# A Complete Bibliography of Publications in *Designs, Codes, and Cryptography*

Nelson H. F. Beebe
University of Utah
Department of Mathematics, 110 LCB
155 S 1400 E RM 233
Salt Lake City, UT 84112-0090
USA

Tel: +1 801 581 5254

E-mail: beebe@math.utah.edu, beebe@acm.org,
beebe@computer.org (Internet)
WWW URL: https://www.math.utah.edu/~beebe/

25 September 2025
Version 2.70

## Title word cross-reference

$(0, 1)$ [628]. $(0, 2)$ [962]. $(0, 2, t)$ [637]. $(0, \alpha)$ [696, 844]. $(1, -1)$ [518]. $(1, 2)$ [1269]. $(15, 8, 4)$ [3362]. $(17, 9)$ [351]. $(17q, 17, 2)$ [364]. $(2)$ [1198]. $(2, 2)$ [1179]. $(2, 2^7)$ [1431]. $(2, 7)$ [1432]. $(2, 8)$ [667, 1133]. $(2, \delta)$ [3251]. $(2, n)$ [904]. $(2, p, p)$ [2430]. $(2, q)$ [1432]. $(2, q^n)$ [1231]. $(255, k)$ [657]. $(25q, 25, 3)$ [364]. $(28, 12, 11)$ [117]. $(2^n)$ [1270]. $(2^n, 2^n)$ [3156]. $(2^q)$ [1452]. $(3, 4)$ [1788, 1872]. $(3, 5*, v)$ [578]. $(3, 8)$ [667]. $(3, L)$ [2484]. $(3, p^3)$ [635]. $(3, t)$ [1550]. $(31, 10, 3)$ [34]. $(36, 16, 12)$ [117]. $(4)$ [659]. $(4, 4)$ [634, 741]. $(4, 8)$ [1133]. $(49, 9, 6)$ [142]. $(5, 2)$ [1138]. $(6, 3)$ [835]. $(6, q)$ [642]. $(64, 2^{37}, 12)$ [236]. $(8, 2)$ [451]. $(96, 20, 4)$ [803]. $(Ck \oplus G, k, 1)$ [251]. $(d, \sigma)$ [2976]. $(\ell, \ell)$ [3202]. $(G, k, 1)$ [251]. $(k)$ [1634]. $(k + s)$ [3301]. $(k, 3)$ [1963]. $(k, k)$ [3455]. $(k, n)$ [478, 1214, 2066, 3442]. $(k, n)^*$ [1982]. $(k, p)$ [425]. $(k^2, k, \lambda)$ [3248]. $(L, G)$ [3440]. $(\lambda + m)K_{v+u} \backslash \lambda K_v$ [1803]. $(m, 40n)$ [2522]. $(m, n)$ [151]. $(m, n, 4, 2)$ [2260]. $(m - 1)/pm$ [167]. $(\mathbf{Z}_v, 4, 1)$ [3229]. $(n, 3)$ [1644]. $(n, 4)$ [1467]. $(n, m)$ [2394, 2556]. $(n, q)$ [636]. $(n \times m, 3, 2, 1)$ [2391]. $(n \times m, k, \lambda, k - 1)$ [3088]. $(\nu, 5, 5)$ [872]. $(\nu, 6, \lambda)$ [901]. $(p^a, p, p^a, p^{a-1})$ [139]. $(p^a, p^a, p^a, 1)$ [605]. $(q)$ [362]. $(q + t, t)$ [637]. $(q, 6, 1)$ [342]. $(Q^{-(5,q)})$ [1643]. $(q^2 + q + 2, q + 2)$ [540]. $(q^2 + q + 8)/2$ [1125]. $(q^2, 2)$ [1541]. $(qm)$ [362]. $(r, \delta)$ [2958, 3192, 3212]. $(r, \lambda) = 1$ [2034]. $(r, t)$ [2604]. $(t, k)$ [1160]. $(t, L)$ [2420]. $(t, m, s)$ [814, 1332]. $(t, n)$ [892, 1153, 1360, 2868]. $(t - 1)$ [1534]. $(t \bmod q)$ [3295]. $(\theta, \delta_\theta)$ [2840]. $(v, \{2, 4\}, 1)$ [245]. $(v, 3, 1)$ [581]. $(v, 4, 1)$ [2859]. $(v, 4, 2, 1)$ [1285]. $(v, 4, \lambda)$ [3057].

$(v, k, 1)$ [1835, 3020]. $(v, k, 2)$ [2283]. $(v, k, 3)$ [2273]. $(v, k, 4)$ [1237, 3433]. $(v, k, k-1)$ [1892, 2346]. $(v, k, k-2, k-1)$ [2525]. $(v, k, \lambda)$ [109]. $(v, K_{1(3)} \cup \{w^*\})$ [1013]. $(x(q+1), x; 2, q)$ [1201]. $(Z/4Z)^3 \times Z/5Z$ [522]. $-1$ [26]. $-2$ [751, 2113, 2120]. 0 [102, 205, 1422, 1995, 2120]. $\{0, 1, 2\}^n$ [101]. 1 [205, 403, 465, 474, 548, 594, 642, 772, 778, 970, 977, 1191, 1329, 1373, 1450, 1457, 1497, 1598, 1670, 1680, 1681, 2079, 2175]. 1/2 [510]. $1/p$ [1609]. 10 [1998]. 1024 [2424, 2425]. 103 [1130]. 12 [980, 1045]. 120 [1805]. 1239 [899]. 13 [1320]. 14 [2126]. $14^1 2^{40} (-4)^{10} (-6)^9$ [1461]. 15 [102, 1944]. 16 [523, 1889]. $19^2$ [980, 1067]. 1 mod $q$ [1252]. 2 [14, 36, 55, 61, 68, 86, 117, 142, 143, 223, 265, 266, 271, 296, 324, 357, 377, 404, 502, 551, 772, 888, 899, 958, 1026, 1037, 1052, 1107, 1182, 1218, 1239, 1347, 1430, 1440, 1463, 1465, 1494, 1507, 1526, 1541, 1549, 1582, 1595, 1623, 1663, 1691, 1749, 1754, 1771, 1834, 1878, 1966, 2008, 2014, 2034, 2101, 2121, 2148, 2160, 2322, 2338, 2391, 2463, 2467, 2515, 2551, 2574, 2652]. $2(2^n - 1)$ [1186]. $2 - (10, 4, 4)$ [602]. $2 - (13, 4, 3)$ [774]. $2 - (22, 8, 4)$ [602]. $2 - (31, 15, 7)$ [1135]. $2 - (35, 17, 8)$ [1135]. $2 - (36, 15, 6)$ [1135]. $2 - (49, 9, 6)$ [617]. $2 - (9, 3, \lambda)$ [593]. $2 - (n^2, 2n, 2n-1)$ [963]. $2 - (v, 405; 40m)$ [2532]. $2 - (v, k, 1)$ [790, 1819]. $2 - (v, k, \lambda)$ [2677, 2779]. 20 [1125]. 23 [1060]. 24 [829, 1848, 2353]. 25 [302, 1167]. 27 [93, 120, 899, 2353]. 28 [290]. 29 [1933]. $2^{2^r} - 1$ [1389]. $2^{2n+1}$ [2566]. $2^{2t}$ [920]. $2^{4e}$ [2088]. $2^e$ [1471]. $2^k$ [1418, 1776]. $2^m + 1$ [2695]. $2^n$ [104, 1182, 1451, 1694]. $2p^m$ [1525, 2454, 2694]. $2p^n$ [1298, 1349]. $2R + 4$ [1061]. $2 \times 2 \times 2 \times 2$ [1546]. $2 \times 2 \times \cdots \times 2$ [3018]. 3 [60, 254, 317, 343, 346, 409, 490, 547, 617, 622, 671, 677, 856, 931, 1012, 1037, 1052, 1099, 1123, 1156, 1158, 1163, 1170, 1182, 1188, 1209, 1218, 1239, 1256, 1274, 1307, 1327, 1344, 1377, 1380, 1423, 1451, 1457, 1563, 1667, 1733, 1791, 1899, 1936, 1960, 1964, 2012, 2024, 2087, 2167, 2213, 2353, 2397, 2424, 2425, 2536]. $3 - (56, 12, 65)$ [833]. 31 [751, 841]. 32 [574, 829, 1291, 1889]. $\{32, 27, 8, 1; 1, 4, 27, 32\}$ [2115]. 324 [541]. 36 [94, 394]. 38 [1402]. 3PDTWh($p$) [994]. 3PTWh($p$) [863]. 4 [514, 547, 577, 595, 623, 741, 835, 863, 994, 1123, 1158, 1218, 1233, 1256, 1364, 1395, 1420, 1422, 1654, 1754, 1803, 1866, 1917, 2160, 2333, 2432, 2463, 2620]. $4(2^n - 1)$ [1506]. $4 - (12, 5, 4)$ [267]. 40 [209, 537, 656, 1284, 1402, 2100]. 41 [366]. 42 [656, 1432, 1667]. 44 [656]. 45 [498]. 49 [118]. $4p$ [2250]. $4p^2$ [2140]. 5 [121, 145, 176, 394, 623, 758, 814, 826, 1233, 1278, 1364, 1808, 1848]. 50 [1742, 1777]. 51 [1044]. $\{52, 35, 16; 1, 4, 28\}$ [1458]. 54 [919]. 56 [833]. 59 [1035]. $5p$ [2974]. 6 [1167, 1218, 1347, 1722, 1878]. 60 [1007, 1742]. 62 [1007]. 64 [306, 422, 943, 1007, 1783, 1881]. 66 [1007]. $\{69, 48, 24; 1, 4, 46\}$ [1458]. 7 [287, 758, 1278]. 72 [306]. 8 [258, 334, 351, 722, 1257, 1274, 1431, 1889, 2267]. $8^4$ [2978]. $8p^3$ [2347]. 9 [573, 1007]. 99 [1374]. 99270589265934370305785861242880 [1314]. $9^4$ [2978]. $[1, q+1, 2q+1, q^2+q+1]_2$ [2642]. [120, 60, 24] [1933]. [207, 4, 165] [485]. [24, 12, 10] [1159]. [28, 7, 12] [90]. [38, 6, 23] [297]. [48, 24, 12] [1401]. [50, 25, 10] [142, 617]. [50, 5, 32] [168]. [52, 26, 10] [1560]. [64, 32, 12] [141]. [69, 5, 45] [105]. $[8 \times 8, 16, 7]_q$ [3096]. [96, 48, 20] [1944]. $[k]^n$ [1470]. $[n, 5, d]_q$ [797]. $[n, k, d]$ [227]. $[q^4 + q^2 - q, 5, q^4 - q^3 + q^2 - 2q; q]$ [41]. $_1$ [832]. $_{22}$ [641]. $_3$ [1225]. $_4$ [671]. $_4[12; 3]$ [820]. $_6$ [1466]. $_8$ [1143]. $_i$ [1522]. $_n$ [1435]. $A$ [478, 874]. $A(n, d, w)$ [968]. $A_6$ [1539]. $A_m$ [3355]. AG(2, $q$) [1538]. AG(3, $q$) [962]. AG(6, 3) [1030]. AG($n, q$) [182]. $\alpha$ [683, 2803]. $\approx 2^{106}$ [1314]. $b$ [1186, 2792, 2989]. $b, c \in \mathbf{F}_q^*$ [2853]. $b_i = 1$ [22]. $\bar{2}$ [1749]. $\beta$ [611]. $BH(n, 6)$ [1947]. mod$2^n$ [1493]. $\mathbf{Z}_4$ [307]. $c$ [111, 1186, 2272, 2629, 2673, 2738, 2821]. $C^*$ [2535]. $c^{n-2}.c^*$ [223]. $c_2$ [1459]. $C_4$ [1227]. $C_\alpha(2, m)$ [2326]. $C_D$ [3077]. $\chi$ [3141]. $\chi^2$ [2037]. $\chi_n$ [3183]. CW(110, 100) [1391]. $D'$

[726, 731, 1719, 1786, 2146, 2437]. $d = 3i - 1$ [22]. $d \neq p$ [3401]. DW$(5, q)$ [1042]. $\ell$ [1750, 2490, 3200]. $\ell_\infty$ [2507]. exp$(G)$ [1047]. $F$ [125]. $F^5$ [653]. $F_q^m$ [742]. $F_2$ [858]. $F_2 + uF_2 + vF_2 + uvF_2$ [1196, 1294]. $F_2^{2m}$ [439]. $F_2^n$ [831]. $F_{2p+1}$ [1822]. $F_2 \times F_2$ [618]. $F_4 + vF_4$ [1991]. $F_5$ [675, 1024, 1051, 1159]. $F_p$ [912]. $F_p, p$ [1809]. $F_p^N$ [922]. $F_q$ [742, 1163]. $F_q[u]/(u^s)$ [834]. $\mathbf{F}_{q^n}$ [83]. $\mathrm{Fi}_{22}$ [978]. $\frac{1}{2}$ [225]. $\frac{1}{n}$ [1595]. $\frac{3^m-1}{2}$ [2467]. $\frac{q^{2m}-1}{q+1}$ [3170]. $\frac{q^m-1}{2}$ [2503]. $G$ [989, 1019, 1047, 2291, 2691, 3157]. $G(1, n, q)$ [909]. $g(x) = x^3 + bx + c$ [2853]. $G^k$ [2863]. $g^t u^1$ [1327]. $g^u m^1$ [743, 1759]. $G_{1,4,2}$ [717]. $\gcd(\lambda, n) = 1$ [3173]. GF(11) [2838]. GF(19) [2838]. GF(23) [2838]. GF$(2^{2m})$ [1654]. GF$(2^{2m+1})$ [1654]. GF$(2^k)$ [315]. GF$(2^q)$ [948]. $GF(4)$ [1308]. GF(5) [485]. GF$(p)$ [75, 2038]. GF$(q)$ [15, 1298, 2125]. GF$(q^s)$ [15]. $GL(n + 1, q)$ [692]. GR$(4, n)$ [1738]. $GR(p^2, m)$ [1406, 2327]. $GS(2, 4, \nu, 2)$ [785]. GS$(3, 4, v, 2)$ [996]. $H$ [995, 1218, 1269, 1973, 2385]. $H(2d + 1, q^2)$ [1658]. $H(n, 2)$ [2111]. $H(q)$ [1221]. $h^u m^1$ [995, 1671]. $h \equiv 0 \bmod 12$ [1671]. $j$ [1422]. $j = 0$ [2774]. $K$ [206, 261, 912, 949, 1214, 1252, 1298, 1394, 1430, 1539, 1614, 1633, 1655, 1694, 2410, 2412, 2677, 2689, 2761, 2767, 2883, 2896, 2944, 3027, 3038, 3301, 3335, 3460]. $k > 2$ [22]. $L$ [988, 3161]. $L(X)$ [3279]. $\lambda$ [244, 352, 989, 1232, 2677]. $\lambda = 1$ [2885]. $\lambda = 2, 4, 8$ [573]. $\lambda = 2^p$ [475]. $\lambda > 1$ [901]. $\langle X^{q^t}, X + \delta X^{q^{2t}}, G(X)\rangle$ [3337]. $\leq k$ [2900]. $M$ [36, 186, 374, 501, 743, 1022, 1111, 1613, 1705, 2229, 3266]. $m + 1$ [2595]. $m > n/2$ [2394]. $M_{13}$ [373]. $Mat_{n,s}(Z_k)$ [721]. $\mathbf{F}_2 + u\mathbf{F}_2 + v\mathbf{F}_2 + uv\mathbf{F}_2 + v^2\mathbf{F}_2 + uv^2\mathbf{F}_2$ [2257]. $\mathbf{F}_2[u]/\langle u^4\rangle$ [2668]. $\mathbf{F}_{2^{2k}}$ [1917]. $\mathbf{F}_{2^k}$ [2041]. $\mathbf{F}_{2^m}$ [2058, 3456]. $\mathbf{F}_{2^n}$ [2049, 2485, 2764, 3213, 3247, 3338]. $\mathbf{F}_{2^r}[u]/\langle u^e\rangle$ [2980]. $\mathbf{F}_2 \times \mathbf{F}_2$ [3307]. $\mathbf{F}_3$ [1730]. $\mathbf{F}_4$ [1561, 2902, 3110, 3307]. $\mathbf{F}_p$ [1919]. $\mathbf{F}_p + u\mathbf{F}_p$ [2332]. $\mathbf{F}_p^n$ [2506]. $\mathbf{F}_q$ [1868, 2503, 2774, 2864, 2911]. $\mathbf{F}_q[u, v]/\langle u^2 - u, v^2 - v, uv - vu\rangle$ [2840]. $\mathbf{F}_q[u]/(u^t)$ [1770]. $\mathbf{F}_q[x]/(x^2)$ [2327]. $\mathbf{F}_{q^2}$ [2036, 2302, 2390, 2853]. $\mathbf{F}_{q^{2n}}$ [2266]. $\mathbf{F}_{q^l}$ [1868]. $\mathbf{F}_{q^m}$ [1959]. $\mathbf{F}_{q^n}$ [2941]. $\mathbf{G}_1$ [3031]. $\mathbf{G}_2$ [3031]. $\mathbf{G}_T$ [3031]. $\mathbf{Q}(\zeta_8)$ [2668]. $\mathbf{Z}$ [2514]. $\mathbf{Z}/N\mathbf{Z} \times |\mathbf{Z}/M\mathbf{Z}$ [1992]. $\mathbf{Z}^n$ [3115]. $\mathbf{Z}_{16}$ [2019]. $\mathbf{Z}_2$ [2202]. $\mathbf{Z}_{2^k}$ [2242, 2622, 3133]. $\mathbf{Z}_{2^m}$ [1806]. $\mathbf{Z}_2^n$ [2067]. $\mathbf{Z}_2\mathbf{Z}_2[u]$ [2253]. $\mathbf{Z}_2\mathbf{Z}_2[u]/\langle u^4\rangle$ [2754]. $\mathbf{Z}_2\mathbf{Z}_4$ [1666, 2175, 2829]. $\mathbf{Z}_4$ [1471, 2116, 2244, 2387, 2445, 2573, 2969, 3109, 3253]. $\mathbf{Z}_4[u]/\langle u^2 - 1\rangle$ [2244]. $\mathbf{Z}_8$ [2019, 2819]. $\mathbf{Z}_m$ [2067, 3037]. $\mathbf{Z}_m^n$ [2555, 2954]. $\mathbf{Z}_p$ [3341]. $\mathbf{Z}_p[u]/\langle u^3\rangle$ [2560]. $\mathbf{Z}_p[u]/\langle u^k\rangle$ [1747]. $\mathbf{Z}_{p^r}$ [2076]. $\mathbf{Z}_{p^s}$ [2788, 3120]. $\mathbf{Z}_p\mathbf{Z}_{p^2}$ [2920]. $\mathbf{Z}_q$ [2146]. $\mathbf{Z}(\mathbf{2^{32} - 1})$ [1771]. $\mathcal{C}$ [2869]. $\mathcal{D}_\prime \cap \mathcal{M}^\#$ [2869]. $\mathcal{GRM}(\in, \Updownarrow)^*$ [1775]. $\mathcal{H}(\ni, \amalg^\in), \amalg$ [1703]. $\mathcal{M}^\#$ [2869]. $\mathcal{Q}^+(\bigtriangledown, \amalg)$ [1931]. $\mathcal{RF}$ [2993]. $\mathcal{S}_c$ [2358]. DW(2n − 1, 2) [2359]. PG$(2, \mathrm{q}^3)$ [1852]. PG$(3, 3)$ [1968]. PG$(4, \mathrm{q})$ [1988, 2483]. PG$(\mathrm{d}, \mathrm{q}^\mathrm{n})$ [2240]. PGL$(2, 2^\mathrm{m})$ [2695]. CENCPP$^*$ [2806]. LWE [2470]. MP [2470]. MD2 [283]. $N$ [23, 143, 261, 501, 646, 783, 3276]. $n - 1$ [2453, 2486]. $n/2$ [3115]. $n = 5p^r$ [1141]. $N = p^r q$ [1715]. $n > 1$ [1231]. $n > 5$ [2910]. $n \equiv 0 \pmod 1 6$ [1170]. $N \equiv 5 \pmod 8$ [2775]. $n \geq 4$ [881]. $NP$ [607]. $\nu$ [145]. $o$ [1865, 3325, 3412]. $O^-(8, 2)$ [300]. $\mathrm{OA}_\lambda(3, 5, v)'s$ [1662]. $\omega$ [3203]. $\overline{3}$ [2024]. $\overline{D}$ [2146]. $P$ [54, 114, 124, 136, 525, 608, 625, 665, 680, 719, 817, 865, 1016, 1124, 1162, 1649, 1807, 1822, 2056, 2278, 2430, 2505, 2553, 2800, 3200]. $p + 1$ [1016]. $p^2$ [1674, 1804, 2259, 2931]. $p^3$ [1804]. $P^4(F_q)P^4(F_q)$ [1107]. $p^e$ [974]. $p^k$ [1406]. $p^n$ [949, 2374, 3429]. $p^{n+1}$ [1361]. $p^r$ [817]. $P_\tau$ [3196]. $p \equiv 1$ [863, 994]. PG$(2, 16)$ [1644]. $PG(2, p)$ [452]. $PG(2, q)$ [1002, 1539, 1751, 1967, 2880]. PG$(2, q^2)$ [1645]. PG$(2, q^3)$ [1636]. $PG(2n, q), n \geq 3$ [786]. $PG(2t + 1, q)$ [421]. PG$(3, 4)$PG$(3, 2)$ [74]. $PG(3, 5)$ [1125]. PG$(3, 7)$ [498]. PG$(3, q)$ [174, 320, 845, 1220, 2718]. $PG(3, q), q \equiv 2(mod 3)$ [1125]. $PG(4, 2)$ [472]. PG$(4, 4)$ [366]. PG$(6, 4)$ [3094]. $PG(9, 2)$

[717]. PG$(m, 2)$ [44]. $PG(n, 2)$ [472, 773, 1000, 1409]. $PG(n, 4)$ [1741]. PG$(n, p^t)$ [1534]. PG$(n, q)$ [528, 909, 1031, 1065, 1411, 2410, 2523, 2761, 3335, 3361]. $PG(n, q), n > 3$ [718]. $PG(n, q), n \geq 3$ [474]. PG$(n, q) \times$ PG$(n, q)$ [1768]. $PG(n, q^3)$ [1252]. $PG(n, q^t)$ [692]. PG$(r, q)$ [2642]. PG$^*$.PG [981]. PGL$(2, 2^f), f$ [13]. $PGL(n + 1, q)$ [692]. $\pm\mathbf{R}^2$ [2830]. $\psi$ [1000]. $P\Sigma L(3, 4)$ [2504]. PSL$(2, 40q)$ [2463]. PSL$(2, 7)$ [1667]. $PSL(2, q)$ [2670, 2996]. $PSL(n + 1, q)$ [692]. PSL$_2(q)$ [879]. PSU$(3, q)$ [2345]. $Q$ [98, 183, 342, 488, 505, 528, 594, 610, 642, 740, 756, 804, 845, 879, 977, 1057, 1058, 1163, 1220, 1221, 1231, 1268, 1411, 1472, 1598, 1643, 1714, 1752, 1815, 1823, 1916, 1974, 2280, 2342, 2370, 2549, 2803, 3018]. $Q(4, q)$ [1532]. $Q(6, q)$ [3180]. $q + 1$ [985]. $q = 19$ [107]. $Q^+(2n + 1, 3)$ [881]. $Q^+(7, q)$ [778]. $Q^{-(5,1)}$ [410]. $Q^-(7, q)$ [1191]. $q^2$ [985]. $q^4 - 2q^2 - 2q + 1 \leq d \leq q^4 - 2q^2 - q$ [797]. $q^m$ [505]. $q^s$ [98]. $R$ [1061, 1330, 2466, 2896, 3191]. $R(1, 7)$ [275]. $R(1, 9)$ [192]. $R(4, 9)$ [192]. $r > \lambda(k - 3)$ [2779]. $R^n$ [628, 812]. $R_3$ [1783]. R$_k$ [1407]. $r \geq 3$ [2642]. $\rightarrow k$ [767]. RM$(3, 7)$ [2183]. $S$ [291, 333, 468, 2469, 2647, 2674, 3003, 3232, 3289, 3301]. $S(2, 4, \frac{3^m-1}{2})$ [2467]. $S(3, 8, 7^m + 1)$ [2802]. $s(u)$ [12]. $S_{1,1,1}(2)S_{1,1,1}(2)$ [1387]. $S_9$ [1143]. $\sigma$ [2520]. SL$(2, 5)$ [232, 980, 1067]. SL$(2, \mathbf{F}_{2^n})$ [1628]. $SL(n + 1, q)$ [692]. SL$_2$ [2011]. SQS(16) [1069]. STS(31) [899]. $sv$ [15]. $T$ [97, 131, 199, 207, 420, 421, 491, 566, 702, 707, 711, 713, 811, 1193, 1627, 1668, 1731, 1732, 1734, 1811, 1916, 1937, 1982, 2095, 2111, 2158, 2241, 2261, 2392, 2469, 2510, 2553, 2647, 2830, 2855, 2858, 3003, 3048, 3211, 3232, 3248, 3289, 3326]. $t + 1$ [3211]. $t - (v, k, \lambda)$ [740]. $t = 3, 4$ [2855]. $T_2(o)$ [683]. $\tau$ [1004, 1290, 2093, 2173, 2733]. **4p** [3388]. **9** [3388]. $\mathbf{F}_2 \times \mathbf{F}_2$ [3040]. $\mathbf{F}_4$ [3040]. $\theta$ [620]. $tR + 1$ [3191]. $tR + \frac{R}{2}$ [2466]. $U(6)$ [55]. $u2^v$ [1017]. $U_3$ [2237]. $U_n(q)$ [1869]. $v$ [15, 585, 1133, 3224]. $v - 1$ [585]. $v = 4(k - \lambda) + 2$ [1695]. $v = r + c - 1$ [822]. $v_k$ [1980]. $\varepsilon$ [3119]. **36** [3216]. $\vec{q}$ [2190]. $v \equiv 0, 1 \pmod 8$ [1133]. $w$ [990]. $W(2n + 1, q)$ [684]. $W_5(q)$ [977]. $w_{\min}/w_{\max} < 1/2$ [2496]. $X$ [1000, 1121, 3279]. $X^\#$ [1000]. $x^{-1} + g(x)$ [1315]. $x^3 g(x^{q-1})$ [2853]. $x^6 + x + a$ [652]. $x^\alpha \bmod N$ [303]. $x^i + ax$ [3247]. $x^{n-1} \in \mathbf{F}_q[x]$ [1875]. $x^r g(x^s)$ [2266]. $x^r h(x^s)$ [2554]. $x^r h\left(x^{q-1}\right)$ [2302]. $x\left(x^s - a\right)^{(q^m-1)/s}$ [2941]. $y^{q^n} - y = \gamma x^{q^h+1} - \alpha$ [1959]. $Z$ [994, 1075, 1238, 1501, 2907]. $Z/(2^{32} - 1)$ [1602]. $Z/2kZ$ [789]. $Z_2 + uZ_2$ [954]. $Z_2 + uZ_2 + u^2 Z_2$ [954]. $Z_2^n$ [959]. $Z_2^s$ [794, 1523]. $Z_{2k}$ [559]. $Z_2 \times Z_4$ [1348]. $Z_2 Z_4$ [1203, 1236, 1842, 2079]. $Z_4$ [343, 346, 375, 401, 622, 658, 869, 1348, 1486, 1559, 2206]. $Z_4^m$ [439]. $Z_4 \times Z_4$ [664]. $Z_8$ [929]. $Z_9$ [929]. $Z_m$ [1108]. $Z_{p^2} \times Z_{p^2} \times \cdots \times Z_{p^2}$ [181]. $Z_{p^3}$ [1120]. $Z_p^k$ [922]. $Z_q$ [1202].

***** [1614]. ***-visual** [1614].

**-Additive** [1666, 2829]. **-adic** [136, 525, 865, 1004, 1290, 1649, 2652, 3403]. **-affine** [2148]. **-Almost** [3119]. **-analog** [2190]. **-Analogs** [740, 1916, 2803]. **-anonymous** [1633, 1634]. **-AONTs** [2430]. **-Arcs** [206, 425, 540, 637, 646, 1430–1432, 1539, 1541, 1644, 1667, 1963, 2412, 3295]. **-Ary** [98, 111, 488, 505, 594, 804, 817, 1016, 1057, 1058, 1268, 1598, 1705, 1714, 1752, 1807, 1815, 1823, 1974, 2278, 2370, 2505, 2549, 2800, 2865, 3018, 3200, 3389]. **-associate** [1000]. **-based** [2470]. **-bases** [1160]. **-bent** [1075, 1501, 2514, 2622]. **-bentness** [2342]. **-BIBDs** [581, 1892]. **-bit** [1889]. **-block-intersection** [1995]. **-Blocking** [474]. **-cap** [1125]. **-caps** [1125]. **-CDMA** [2908]. **-circulant** [3203]. **-clan** [183]. **-Clans** [756]. **-codes** [41, 478, 658, 874, 1457, 2116, 2242, 2291, 2691, 2863, 3109, 3133, 3157, 3440]. **-complementary** [2907]. **-Complete** [607]. **-concurrence** [2167]. **-configurations**

[1130]. **-Consecutive** [3442]. **-construction** [3077]. **-coordinates** [1121]. **-Covering** [713]. **-Coverings** [352]. **-covers** [1111]. **-curves** [2774]. **-Cycle** [36, 176, 1803, 1878]. **-Cyclic** [291, 333, 994, 2175, 2754, 2840]. **-D** [1623, 2391]. **-Deletion-Correcting** [317, 595, 1278, 1754]. **-Derived** [611]. **-Design** [394, 491, 566, 758, 1848]. **-Designs** [55, 61, 97, 109, 207, 245, 296, 334, 343, 346, 502, 620, 622, 623, 671, 702, 707, 711, 740, 811, 970, 1218, 1269, 1344, 1380, 1463, 1668, 1731, 1936, 1937, 2014, 2034, 2095, 2111, 2121, 2213, 2241, 2322, 2385, 2392, 2463, 2467, 2469, 2510, 2515, 2553, 2647, 2830, 2855, 2858, 2859, 3003, 3232, 3289, 3326, 3362, 3455]. **-Difference** [605]. **-differential** [2629, 2673, 2821]. **-dimension** [75, 783]. **-dimensional** [1044, 1347, 1422, 1667, 1786, 2432]. **-disjoint** [3229]. **-double** [2202]. **-Elusive** [2674]. **-error** [912, 949, 1182, 1298, 1394, 1451, 1694]. **-extensions** [1776]. **-factor** [1440]. **-Factors** [403]. **-FCSR** [726]. **-flag** [19]. **-flocks** [683]. **-fold** [1232, 1377, 1732, 2420]. **-form** [3200]. **-frameproof** [2338, 2574]. **-free** [1227]. **-functions** [1627, 2261, 2394, 2556]. **-Galois** [3161]. **-GDDs** [1327, 1420]. **-generalized** [2522]. **-Generator** [548, 1329, 1670, 1973]. **-Geometries** [696, 962, 981]. **-Goethals** [622]. **-Groups** [266, 377, 404, 1037, 1162, 2397]. **-Homogeneous** [199, 465, 731]. **-idempotent** [1052]. **-identifiable** [990]. **-identifying** [1330]. **-input** [501]. **-intersecting** [988, 2101]. **-intersection** [2490]. **-invariant** [1422, 1539, 1667, 2412, 3355]. **-isogenies** [3156, 3202]. **-Kernels** [817]. **-Kneser** [1472]. **-LCD** [2520]. **-level** [68, 1430]. **-lifts** [1783]. **-linear** [401, 742, 922, 1203, 1236, 1559, 1842, 1868, 2079, 2206, 2253, 2689, 2788, 2920, 3120]. **-linearly** [2437]. **-locality** [2604]. **-locally** [2958, 3212]. **-LRCs** [3192]. **-matrices** [1193]. **-MDS** [835]. **-method** [2037]. **-metric** [2093, 2173, 2507, 2733]. **-minihypers** [1201]. **-monomials** [3325, 3412]. **-neighbour** [1966]. **-nest** [980]. **-Nets** [586, 741, 814, 1332, 1960]. **-normal** [2896, 3038]. **-numbers** [3224]. **-optical** [2391]. **-optimal** [2944]. **-output** [501]. **-Overlap** [1681]. **-ovoids** [1111, 2229]. **-Packings** [352, 420, 1872]. **-parent-identifying** [2551]. **-PBDs** [1013]. **-Perfect** [36, 594, 901, 1019, 1450, 1598, 1878, 2079, 2175]. **-periodic** [949, 1017, 1182, 1451, 1694]. **-plateaued** [3301]. **-points** [2803]. **-polynomial** [2553]. **-polynomials** [143, 1865]. **-potent** [2056]. **-Power** [143]. **-primitive** [2896]. **-projectable** [989]. **-publicly** [2868]. **-QC-LDPC** [2484]. **-quasigroups** [1052]. **-Rank** [54, 114, 680, 899, 2353, 2536]. **-Ranks** [124, 665, 719, 1663, 2008]. **-Rectangles** [125]. **-Regular** [468]. **-Reguli** [844]. **-relative** [139]. **-residue** [1811]. **-resolvability** [1269]. **-resolvable** [86, 2469, 2647, 3003, 3232, 3289]. **-rotation** [1834]. **-rotational** [1373]. **-round** [1998, 2012]. **-SEEDs** [1731, 1734]. **-separable** [1749, 2024]. **-sequences** [374, 1750]. **-sequencings** [14]. **-sets** [1655, 2767, 3335]. **-Shift** [131]. **-space** [1534]. **-spaces** [2410, 2761, 2883]. **-splitting** [856, 1012, 2272]. **-spontaneous** [2158]. **-spotty** [1613]. **-Spreads** [421]. **-Steiner** [420]. **-strongly** [3211]. **-subspace** [1252]. **-surjective** [1026]. **-symbol** [2792, 2989]. **-symmetric** [803, 1237]. **-system** [1191]. **-Systems** [186, 642, 778, 977]. **-term** [1156]. **-Threshold** [892, 1360]. **-to-1** [3266]. **-transitive** [23, 1582, 1691]. **-uniform** [1654, 1722, 1866, 1917, 2267, 2333, 2620]. **-variable** [3301]. **-Vectors** [628, 812]. **-Veronese** [2976]. **-vertex** [1395]. **-visual** [1982, 2066]. **-weight** [265, 958, 1163]. **-wise** [1916]. **-XOR** [3460].

**0** [1596]. **0-extendable** [2910].

**1** [1318]. **1-generator** [1281]. **1-Perfect** [817, 1266]. **128** [1317, 1415, 3369]. **128/256** [2214]. **128a** [2762, 3369]. **13** [333]. **160** [2047, 2530]. **162** [555]. **1D** [2193].

**2** [1837]. **2-** [1835, 2273, 2283]. **2-adic** [2864, 3188, 3381]. **2-designs** [2856, 2888, 2922, 3083, 3189, 3235, 3239]. **2-Groups** [504]. **2-pass** [3218]. **2-resolvable** [2855]. **2-subgroups** [3022]. **2-to-1** [3325, 3412]. **2.0** [2569, 2701]. **20004a** [189]. **2013** [2816]. **2017** [2500]. **2022** [2857, 3095]. **224** [2047]. **256** [1998, 2214, 3118]. **256/512** [2214]. **25th** [1902]. **2D** [2193].

**3** [134, 164]. **3-** [3020, 3057]. **3-designs** [2887, 3273, 3358, 3438]. **3-dimensional** [3337]. **3-round** [2720]. **3-spread** [1198]. **381** [3258]. **3G** [2569]. **3rd** [1576].

**4** [120, 1698]. **4-cycle** [1232]. **4-designs** [2670, 3003]. **4-dimensional** [2978]. **4-round** [3197]. **430-cap** [3094].

**5-round** [3073, 3452]. **512** [2214]. **52** [55].

**64** [3276, 3315]. **65th** [1469, 1470].

**70th** [1219].

**8** [189, 2823].

**90k** [55]. **94e** [134, 164]. **95a** [120]. **97f** [189].

**A.** [753]. **Aart** [2875]. **ABE** [2703, 3149]. **abelian** [26, 46, 108, 114, 131, 310, 329, 347, 456, 487, 583, 704, 728, 866, 953, 1037, 1047, 1119, 1156, 1492, 1543, 1591, 1774, 1813, 1886, 2061, 2140, 2347, 2524, 2644, 2755, 2834, 2946, 3269, 3327]. **above** [1127]. **absence** [2728]. **absolute** [2065]. **absolutely** [3002]. **abstract** [2474]. **abundant** [3261]. **accelerate** [3419]. **Access** [560, 893, 1515, 1692, 1729, 1737, 1780, 2017, 2057, 2565, 2899, 2979, 3163, 3442]. **accumulator** [2845]. **Accurate** [1302, 2476]. **Accusation** [1426]. **achievability** [1775]. **Achievement** [276]. **Achieving** [190, 1901, 3223]. **ACORN** [3369]. **ACORN-128** [3369]. **acting** [1952]. **Action** [692, 3237]. **actions** [2061, 2161, 2459, 3333]. **active** [2087]. **actor** [1757]. **adaptive** [2312, 2795, 3271]. **Adaptively** [1901, 2689, 2704, 3027]. **Add** [218]. **adder** [2057]. **addition** [1493, 2870]. **Additive** [398, 561, 659, 1079, 1308, 1561, 1666, 1824, 2055, 2411, 2453, 2527, 2663, 2829, 2902, 3226, 3285, 3359, 3396, 3404, 3462]. **Additivity** [3235]. **adic** [136, 525, 865, 1004, 1290, 1649, 2652, 2864, 3188, 3381, 3403]. **Adjacency** [1227, 1475, 2070]. **adjacent** [1290]. **Admissible** [1695, 3398]. **Admitting** [178, 790, 921, 980, 985, 1067, 1183, 1953, 2077, 2322, 2814]. **Advanced** [1090]. **Advantage** [649, 1884]. **Adventures** [2867]. **adversarial** [2942]. **adversary** [1413, 2970]. **AEAD** [3369]. **AES** [975, 1171, 1333, 1573, 1851, 1989, 1998, 2262, 2476, 3060, 3107, 3118, 3186]. **AES-256** [1998, 3118]. **AES-based** [1851]. **AES-like** [1171, 3060]. **Affine** [17, 58, 151, 166, 295, 325, 344, 408, 422, 461, 487, 525, 591, 674, 677, 696, 852, 947, 1119, 1228, 1258, 1340, 1400, 1418, 1516, 1542, 1607, 1615, 1675, 1709, 1801, 1832, 1835, 2060, 2073, 2123, 2148, 2207, 2289, 2352, 2409, 2547, 2582, 2598, 2728, 2763, 3092, 3193, 3231, 3283, 3294]. **Affine-Invariant** [166, 408, 2073]. **affine-type** [1542]. **AG** [634, 1260, 1467, 1586, 2184, 2300, 2596, 2675, 3387]. **against** [631, 1122, 1272, 1318, 1413, 1635, 1843, 1860, 2047, 2203, 2448, 2461, 2476, 2585, 3049, 3060, 3242, 3435]. **aggregate** [1223, 3271]. **Agreement** [614, 1034]. **aided** [2380, 2634]. **alarms** [1273]. **Algebra** [1169, 1508, 1826, 1828, 2144, 3036]. **Algebraic** [96, 193, 208, 369, 654, 682, 734, 752, 821, 854, 862, 928, 973, 1078, 1116, 1172,

1204, 1271, 1272, 1325, 1454, 1486, 1516, 1572, 1593, 1616, 1682, 1737, 1744, 1843, 1982, 2041, 2042, 2269, 2310, 2330, 2386, 2584, 2618, 2805, 2935, 2983, 3028, 3052, 3093, 3153, 3183, 3201, 3215, 3249, 3255, 3283, 3432]. **Algebraic-Geometric** [193, 208, 2386]. **Algebraic-geometry** [973]. **algebraically** [48]. **Algebras** [47, 390, 470, 1183, 1464, 2301, 2481, 2561, 2655, 3269]. **Algorithm** [285, 503, 575, 584, 660, 678, 857, 987, 998, 1014, 1017, 1097, 1134, 1204, 1293, 1399, 1497, 1763, 1820, 1844, 2037, 2048, 2085, 2363, 2373, 2431, 2433, 2509, 2563, 2617, 2702, 2762, 2782, 2903, 2925, 3019, 3249, 3365, 3398, 3460]. **algorithmic** [2414]. **Algorithms** [165, 882, 1082, 1556, 1999, 2841, 2846, 3113, 3205]. **alignment** [1113, 3225]. **all-but-many** [2662, 3303]. **all-or-nothing** [2749]. **all-to-all** [3207]. **ALLPC** [3450]. **Almost** [161, 210, 273, 325, 406, 495, 542, 828, 1021, 1632, 1677, 1851, 1878, 1909, 1974, 2054, 2078, 2125, 2217, 2255, 2289, 2378, 2416, 2468, 2478, 2533, 3119, 3209, 3303]. **almost-perfect** [2078]. **Alphabet** [365, 524, 835, 1023, 2043, 2800, 3212, 3298]. **alphabet-optimal** [2800, 3212]. **Alphabets** [806, 1974, 2836, 3451]. **also** [15]. **alternant** [3422]. **Alternate** [321]. **Alternating** [670, 767, 1261, 1497, 2227, 2922, 3020, 3057, 3073, 3082, 3143]. **alternative** [1336, 1837]. **Altogether** [175]. **AM** [1623]. **Amalgams** [710]. **ambiguity** [1711]. **AMDS** [3388]. **among** [2155]. **amorphic** [1477]. **amplification** [2423]. **analog** [2190]. **analogies** [2655]. **Analogs** [740, 1916, 2803]. **analyses** [2781, 2813]. **Analysing** [2215]. **Analysis** [303, 437, 670, 867, 1070, 1194, 1393, 1394, 1743, 1982, 2007, 2319, 2422, 2448, 2552, 2701, 2867, 3099, 3106, 3130, 3233, 3242]. **analyzing** [3113]. **András** [1241]. **Andries** [2108]. **anisotropic** [3336]. **Annihilator** [889]. **annihilators** [1925]. **anniversary** [1902]. **Anonymity** [621, 1263, 1521, 2630, 2704]. **Anonymous** [699, 1633, 1634, 1767, 2159, 3005, 3163]. **Answering** [406]. **Antichain** [411]. **Anticode** [2199]. **Anticode-based** [2199]. **Anticodes** [140, 2981]. **antiderivatives** [2506]. **Antipodal** [2931, 3108]. **antiprimitive** [2802]. **antiregularity** [1448]. **Any** [244, 863, 1744, 2276, 3159]. **AONTs** [2430]. **AP** [2738]. **aperiodic** [1798, 3263, 3316]. **APN** [1094, 1205, 1250, 1255, 1306, 1315, 1362, 1654, 1727, 1816, 1930, 2065, 2155, 2418, 2542, 2619, 2639, 2787, 2967, 3002, 3017, 3032, 3324, 3330, 3399]. **APN-like** [2542]. **APN-ness** [2639]. **appearing** [3268]. **Application** [518, 526, 562, 1171, 1279, 1333, 1352, 2287, 2292, 2634, 2713, 2800, 2971, 3033, 3064, 3066, 3091, 3210, 3253, 3267, 3276, 3304, 3323, 3400]. **Applications** [171, 365, 414, 418, 483, 507, 610, 698, 933, 939, 1013, 1097, 1110, 1147, 1240, 1290, 1325, 1428, 1471, 1519, 1576, 1600, 1736, 1737, 1765, 1862, 1887, 1907, 1908, 1962, 1991, 2015, 2028, 2063, 2139, 2217, 2384, 2428, 2429, 2434, 2490, 2539, 2569, 2599, 2675, 2833, 2852, 2863, 2870, 2909, 2916, 2948, 2976, 2992, 3015, 3107, 3123, 3165, 3215, 3393, 3450, 3451]. **Approach** [208, 465, 600, 671, 734, 742, 760, 779, 946, 968, 992, 1122, 1629, 1727, 1750, 1879, 2063, 2441, 2501, 2576, 2583, 2614, 2696, 3079, 3255, 3432, 3436]. **approaching** [3061]. **Approximate** [247, 2887, 3219]. **approximating** [3459]. **approximation** [1426, 2569]. **approximations** [2281, 2824]. **Arakelov** [1693]. **Arasu** [1778]. **Arbitrarily** [491]. **arbitrary** [1023, 1088, 1870, 2095, 2372, 2452, 2618, 2836, 2973, 3056, 3123, 3161, 3250]. **Arbitration** [450, 494, 907, 1732, 2420]. **Arcs** [65, 206, 425, 540, 564, 583, 637, 646, 1231, 1292, 1430–1432, 1538, 1539, 1541, 1644, 1667, 1882, 1963, 1965, 2121, 2350, 2351, 2412, 2427, 2482, 2721, 2881, 3293, 3295]. **Arf** [2330]. **argument** [1867]. **arguments** [1920, 2222, 2663, 3044, 3240]. **Arising** [36, 419, 564, 565, 729, 1015, 1042, 1150, 1322,

1922, 2523, 2804, 3040, 3270, 3434]. **Arithmetic** [435, 444, 590, 672, 1156, 1710, 2954, 2995]. **Arithmetization** [3330]. **Arithmetization-oriented** [3330]. **Armstrong** [1606]. **Array** [757, 2115, 2451, 2798, 2957, 3243]. **Arrays** [22, 25, 29, 279, 372, 586, 597, 644, 698, 713, 730, 761, 819, 822, 896, 900, 915, 967, 986, 1114, 1123, 1199, 1226, 1346, 1379, 1385, 1458, 1481, 1520, 1740, 1817, 1885, 1910, 1946, 1986, 2069, 2104, 2116, 2168, 2225, 2235, 2315, 2426, 2444, 2487, 2499, 2512, 2740, 2862, 2898, 2926, 2933, 3008, 3018, 3054, 3106, 3121]. **Article** [2920]. **Artin** [3220]. **ARX** [3373]. **Ary** [98, 111, 488, 505, 594, 804, 817, 1016, 1057, 1058, 1268, 1598, 1705, 1714, 1752, 1807, 1815, 1823, 1974, 2278, 2370, 2505, 2549, 2800, 2865, 3018, 3200, 3389]. **ASCON** [3175, 3369, 3374]. **ASCON-128a** [3369]. **Aspects** [975, 1277, 1387, 1388]. **assignment** [1780, 2908]. **Assignments** [566]. **Assisted** [747, 1870, 2181, 2264, 2657, 2734, 3011, 3129, 3444]. **Assmus** [379, 380, 486, 671, 2232, 2660, 2810, 3004]. **associate** [1000]. **associated** [1169, 1251, 1259, 1579, 1663, 1953, 2084, 2240, 2515, 2799, 3016, 3020, 3040, 3151]. **Association** [376, 390, 413, 461, 749, 1322, 1477, 1921, 2111, 2232, 2553, 3080, 3270, 3336]. **associative** [1445, 2205]. **assumption** [2308, 2689, 2747]. **assumptions** [1295, 2973, 3055]. **Asymmetric** [1739, 1789, 2295, 2657, 2841]. **Asymptotic** [838, 890, 1178, 1253, 1394, 1612, 1892, 2002, 2178, 2225, 3101, 3226, 3376]. **Asymptotically** [821, 2541, 2936, 3123, 3263, 3316, 3389]. **Asynchronous** [2080]. **Ate** [1522, 2537]. **Attached** [554]. **Attack** [437, 716, 965, 1311, 1333, 1442, 1715, 1728, 1743, 1873, 2139, 2195, 2248, 2254, 2373, 2380, 2433, 2448, 2608, 2634, 2762, 2781, 2782, 2813, 2942, 3024, 3056, 3118, 3197, 3242, 3304, 3352, 3395, 3403]. **Attacks** [159, 519, 760, 836, 1062, 1068, 1272, 1318, 1442, 1572, 1596, 1823, 1843, 1851, 1860, 1896, 1990, 1998, 2003, 2041, 2047, 2090, 2094, 2214, 2243, 2281, 2305, 2383, 2530, 2539, 2543, 2585, 2781, 2786, 2813, 2823, 2867, 2982, 3049, 3052, 3070, 3078, 3107, 3153, 3175, 3186, 3228, 3288, 3313, 3315, 3345, 3369, 3400, 3452]. **Attaining** [797, 2545, 2784, 3173]. **Attribute** [2017, 2251, 2312, 2736, 2795, 2815, 2816, 2899, 2973, 3027, 3074, 3163, 3221, 3257]. **Attribute-based** [2017, 2312, 2736, 2795, 2815, 2816, 2899, 2973, 3074, 3163, 3257]. **attribute-weighted** [3027, 3221]. **attributes** [2795]. **augmentation** [1973]. **Authenticated** [33, 614, 1853, 2151, 2152, 2203, 2471, 2789, 3223]. **Authentication** [25, 33, 38, 52, 91, 112, 133, 149, 159, 160, 169, 293, 301, 332, 337, 338, 450, 494, 733, 856, 891, 907, 936, 1012, 1079, 1142, 1189, 1224, 1321, 1377, 1441, 1521, 1732, 2004, 2272, 2420, 2653, 2752, 2826, 3005, 3271]. **Authentication/Secrecy** [293]. **Authenticators** [309]. **authority** [2501]. **Autocorrelation** [110, 509, 1509, 1525, 1705, 1711, 2261, 2304, 2652, 2864, 3329]. **autoencoders** [1484]. **automata** [2502]. **automatic** [3024, 3373]. **Automorphism** [19, 79, 166, 271, 408, 491, 862, 1007, 1274, 1542, 1582, 1585, 1691, 1777, 1835, 1933, 1952, 1953, 2077, 2079, 2190, 2273, 2504, 2885, 2940, 2996, 3340, 3423]. **Automorphisms** [43, 360, 440, 551, 617, 862, 871, 1060, 1135, 1282, 1605, 1854, 1944, 1962, 1996, 2123, 2805]. **autotopism** [2005]. **auxiliary** [2151, 2152]. **availability** [2199, 2984, 3415]. **Average** [1692, 1825, 2011, 2676, 3038, 3139]. **average-case** [1825]. **averaging** [2942]. **avoid** [77]. **avoidance** [1888]. **Avoided** [119]. **Avoiding** [1011, 1170, 1253, 1386, 1657, 1733, 1760, 1847, 1932, 1955, 2391, 2820, 3428, 3436]. **Ax** [1480]. **azinv** [2846].

**B.** [55]. **bad** [2203]. **Baer**

[399, 457, 1468, 1986, 2356, 2953]. **Bagchi** [55]. **balance** [1619, 1695]. **Balanced** [5, 60, 240, 254, 258, 287, 573, 604, 655, 662, 761, 822, 1028, 1268, 1509, 1843, 1916, 1930, 1936, 1995, 2212, 2320, 2376, 2408, 2416, 2434, 2447, 2464, 2618, 2742, 2775, 3167, 3203, 3260]. **Balancedly** [2708]. **balancing** [2470, 2565, 3366]. **Ball** [1948]. **balls** [1716, 3178]. **Bandersnatch** [3258]. **Barker** [32, 967, 1187, 1993]. **Barlotti** [237]. **Barnes** [948]. **barrier** [3302]. **Bartocci** [1479]. **Base** [888, 923]. **base-transitive** [923]. **Based** [119, 158, 180, 324, 563, 619, 672, 682, 732, 783, 798, 810, 883, 951, 966, 1070, 1142, 1194, 1200, 1207, 1223, 1444, 1501, 1522, 1566, 1594, 1631, 1692, 1724, 1739, 1780, 1787, 1820, 1851, 1864, 1891, 1935, 1981, 2000, 2004, 2009, 2086, 2094, 2114, 2145, 2195, 2204, 2227, 2254, 2256, 2285, 2301, 2303, 2312, 2383, 2398, 2475, 2492, 2502, 2516, 2581, 2609, 2612, 2615, 2638, 2662, 2663, 2712, 2727, 2795, 2796, 2815, 2816, 2845, 2852, 2873, 2909, 2913, 2915, 2926, 2933, 2945, 2965, 2973, 3008, 3015, 3047, 3073, 3098, 3116, 3124, 3172, 3228, 3237, 3246, 3349, 3356, 3357, 3365, 3458]. **based** [1064, 1166, 1443, 1609, 1622, 1682, 1874, 1918, 2017, 2041, 2144, 2199, 2222, 2251, 2340, 2366, 2423, 2470, 2667, 2679, 2703, 2704, 2713, 2736, 2746, 2801, 2899, 2960, 2988, 3055, 3062, 3074, 3085, 3163, 3257, 3263, 3301, 3316, 3428]. **Bases** [50, 83, 295, 831, 923, 932, 1089, 1160, 1372, 1879, 1977, 2224, 2314, 3215]. **Basic** [629, 889, 892, 2632]. **Basis** [357, 535, 562, 1455, 1591, 2128, 2231, 2389]. **Batch** [1893, 1918, 2316, 2398, 2962]. **BBB** [3073]. **BC** [3304]. **BCH** [224, 408, 515, 623, 657, 1093, 1659, 2292, 2429, 2503, 2571, 2741, 2998, 3063, 3114, 3168, 3170, 3222, 3343]. **BCH-like** [1659]. **Be** [119, 725, 2595, 2814, 2929]. **beat** [3284, 3375]. **behavior** [1843]. **behaviour** [1612]. **Beierle** [2485]. **being** [1098]. **BEL** [1927, 2134]. **BEL-configurations** [1927]. **BEL-rank** [2134]. **Belov** [1354]. **Bent** [69, 340, 396, 448, 579, 828, 850, 1075, 1098, 1305, 1306, 1314, 1319, 1322, 1412, 1419, 1500, 1501, 1554, 1702, 1814, 1865, 1903, 2022, 2061, 2067, 2143, 2165, 2170, 2237, 2278, 2290, 2455, 2493, 2505, 2514, 2522, 2546, 2548, 2549, 2556, 2602, 2622, 2682, 2688, 2723, 2730, 2742, 2768, 2790, 2801, 2869, 2894, 2897, 2905, 2934, 2955, 2960, 2963, 2993, 2997, 3064, 3076, 3097, 3101, 3196, 3200, 3270, 3301, 3368, 3397]. **bent-negabent** [2934]. **Bentness** [321, 1850, 2342]. **Bergé** [3446]. **Berlekamp** [263]. **Bernoulli** [2971]. **Bernstein** [2373]. **Best** [88, 620, 2808]. **best-known** [2808]. **better** [1204, 2343, 3315]. **Between** [51, 265, 469, 543, 650, 1166, 1297, 1338, 1379, 1459, 1492, 1516, 1625, 1719, 1919, 1976, 2219, 2491, 2655, 2903]. **Beyond** [1238, 1426, 1620, 1757, 1915, 2321, 2381, 2638, 2806, 3097]. **Beyond-birthday** [2381, 2638]. **beyond-birthday-bound** [2321]. **beyond-birthday-secure** [2806]. **BGV** [3302]. **Bhang** [156]. **Bias** [1083, 2048, 2625, 3153]. **biases** [1873, 2215, 2608]. **BIBD** [364]. **BIBDs** [581, 1278, 1892, 2167, 3376]. **Bijections** [543, 1866, 3409]. **bijective** [3053]. **bijectivity** [1627]. **bijectivity/transitivity** [1627]. **BIKE** [3436]. **bilateral** [3286]. **bilinear** [140, 1282, 2671]. **Binary** [45, 64, 80, 88, 90, 102, 130, 150, 172, 260, 271, 305, 312, 321, 374, 381, 385, 395, 407, 419, 441, 486, 500, 532, 574, 596, 613, 651, 784, 799, 800, 807, 814, 861, 880, 882, 896, 919, 940, 961, 989, 1026, 1059–1061, 1086, 1087, 1099, 1110, 1182, 1266, 1355, 1397, 1402, 1510, 1524, 1525, 1606, 1673, 1745, 1752, 1783, 1877, 1943, 1944, 1973, 2014, 2044, 2100, 2102, 2111, 2190, 2191, 2206, 2234, 2304, 2372, 2374, 2409, 2444, 2453, 2571, 2611, 2678, 2706, 2722, 2729, 2739, 2753, 2757, 2898, 3004, 3144, 3265, 3329, 3405, 3456]. **binary** [316, 938, 1007, 1017, 1092, 1168, 1217, 1258, 1325, 1330, 1394, 1450, 1451, 1589, 1597, 1609, 1694, 1706, 1742, 1827, 1870, 1922, 1925, 1937,

2226, 2250, 2259, 2415, 2496, 2680, 2687, 2694, 2801, 2810, 2860, 2864, 2908, 2923, 3036, 3072, 3077, 3134, 3146, 3340, 3362, 3417, 3429, 3438]. **Binary/Ternary** [260]. **Binomial** [363, 1471, 2750]. **binomials** [1032, 1363, 1846, 2049, 3247, 3325, 3364, 3412]. **Bipartite** [710, 1417, 1440, 1478, 2979, 3054]. **biplane** [1460]. **biplanes** [2564]. **birthday** [1219, 1469, 1470, 1750, 2321, 2381, 2414, 2638, 2806]. **Bit** [868, 1889, 2331, 2460, 2762, 2870]. **bit-vector** [2870]. **Bitcoin** [2428]. **Bits** [725, 997, 3056]. **bivariate** [3015]. **Bivectors** [467]. **BKW** [1763]. **Black** [892, 2210]. **black-box** [2210]. **Blind** [2017, 2815, 3237]. **blindness** [3014]. **Block** [56, 60, 121, 145, 240, 244, 254, 258, 287, 311, 327, 479, 502, 573, 577, 587, 743, 790, 796, 931, 970, 989, 1005, 1070, 1122, 1158, 1228, 1233, 1256, 1278, 1286, 1300, 1333, 1364, 1368, 1380, 1401, 1423, 1497, 1511, 1603, 1759, 1762, 1781, 1859, 1918, 1936, 1992, 1995, 2027, 2089, 2201, 2247, 2297, 2320, 2321, 2373, 2416, 2457, 2463, 2533, 2539, 2543, 2545, 2551, 2646, 2731, 2780, 2820, 2888, 2912, 2992, 3007, 3020, 3037, 3057, 3087, 3118, 3150, 3239, 3245, 3248, 3400]. **block-cipher-based** [1070]. **block-intersection** [56, 1368]. **Block-transitive** [1228, 2888, 3020, 3057, 3248]. **blockcipher** [1781, 2209, 2936]. **Blocking** [226, 245, 452, 474, 534, 667, 718, 759, 881, 886, 1002, 1185, 1220, 1244, 1248, 1409, 1534, 1537, 1650, 2356, 3051, 3361]. **Blocks** [616]. **Blocksize** [662, 3115]. **Blokhuis** [1948, 2875]. **BLS** [3447]. **BLS12** [3258]. **BLS12-381** [3258]. **BLT** [630, 977]. **BLT-property** [977]. **BLT-Sets** [630]. **Boneh** [1106]. **Bonisoli** [2201]. **Book** [100, 2857]. **Boolean** [501, 547, 567, 676, 788, 828, 889, 890, 1098, 1172, 1272, 1319, 1324, 1325, 1418, 1484, 1509, 1516, 1554, 1616, 1656, 1682, 1710, 1834, 1843, 1858, 2004, 2237, 2269, 2342, 2387, 2405, 2422, 2437, 2478, 2496, 2582, 2610, 2618, 2678, 2706, 3030, 3097, 3253, 3263, 3316, 3317]. **Boomerang** [1333, 2559, 2616, 2737, 2808, 2967, 3371, 3450]. **Borel** [1916]. **Bose** [58, 390, 397, 3168]. **Bose-Burton** [397]. **Bound** [20, 41, 54, 59, 64, 108, 227, 276, 547, 558, 591, 620, 668, 712, 797, 955, 961, 993, 1003, 1088, 1127, 1185, 1204, 1253, 1279, 1398, 1414, 1487, 1586, 1618, 1675, 1685, 1748, 1830, 1937, 1949, 2044, 2055, 2087, 2262, 2321, 2327, 2343, 2354, 2396, 2402–2404, 2486, 2545, 2657, 2784, 2838, 2882, 2883, 3010, 3097, 3101, 3173, 3375, 3417]. **Bounded** [903, 2404, 3250]. **Bounding** [1499, 2128, 2731, 2758, 3050]. **Bounds** [80, 129, 150, 211, 257, 293, 308, 316, 335, 338, 349, 353, 418, 468, 473, 478, 480, 494, 501, 507, 556, 576, 603, 648, 651, 657, 806, 885, 941, 946, 968, 991, 1005, 1096, 1109, 1140, 1178, 1265, 1313, 1315, 1332, 1569, 1575, 1578, 1749, 1769, 1775, 1798, 1836, 1877, 1973, 2024, 2032, 2042, 2104, 2110, 2114, 2147, 2158, 2173, 2222, 2271, 2338, 2382, 2405, 2426, 2457, 2606, 2607, 2623, 2745, 2809, 2842, 2932, 3005, 3036, 3067, 3121, 3135, 3207, 3252, 3285, 3359, 3386, 3396, 3421, 3443, 3455, 3462]. **box** [2093, 2210, 2507, 2616]. **Boxes** [428, 601, 939, 1447, 2087, 2558, 2796, 3053, 3242]. **Boyen** [2816]. **Bracken** [2580]. **Braid** [883, 1006]. **branch** [3130]. **branching** [2909]. **BRDs** [1364]. **Breaking** [2684, 2702, 3019, 3249, 3302]. **Brezing** [1522]. **Brickell** [1773]. **bridge** [3053]. **Broadcast** [282, 331, 699, 913, 1151, 2752, 3005, 3163]. **Brouwer** [753, 2108, 2127]. **Bruck** [2, 9]. **Bruen** [54, 107, 1675]. **Bruijn** [59, 123, 138, 1335, 1476, 2162, 2164, 2174, 2372, 2588, 2817, 3143, 3370]. **Buekenhout** [1230, 3292]. **build** [339, 2311, 2851]. **build-up** [2851]. **Building** [383, 392, 1306, 1781, 1926]. **buildings** [1466, 3000]. **built** [3258]. **Bundles** [1080, 1260, 1425, 2848]. **Burnside** [1791]. **burst** [2977, 3360]. **Burton** [397]. **buses**

[1888]. **Bush** [541]. **Bush-Type** [541]. **Butler** [1568]. **Butson** [969, 2335, 2487, 2906]. **butterfly** [2654, 2751]. **byte** [283, 1083]. **bytes** [1083].

**C** [571]. **Caen** [745]. **calculate** [2263]. **Calculation** [836, 1017]. **Calculus** [436, 437]. **Cameron** [320, 1535, 1741, 2188, 2410, 2671, 2761, 2767, 3335]. **Cameron-Liebler** [320, 1741]. **Can** [119, 2337, 3375]. **cancellation** [2681]. **candidates** [2684]. **Cannot** [602, 2595, 2929]. **canonical** [3239, 3392]. **Cap** [366, 634, 1125, 2876, 3094]. **Capability** [246, 1620]. **Capacity** [2110, 3298, 3431]. **Caps** [196, 235, 289, 381, 513, 666, 773, 807, 861, 1030, 1125, 1247, 1687, 2555, 2938]. **cardinality** [2607]. **cards** [1661, 1753]. **Carlet** [2269, 2819]. **Carlitz** [2149]. **carry** [2509]. **Carter** [2653]. **cartesian** [52, 728, 1607, 2547, 2599, 3192, 3264]. **cascade** [2323, 2435, 2975]. **cascaded** [2936]. **Case** [628, 812, 1315, 1825, 2011, 2078, 2479, 3139, 3399]. **cases** [3184]. **CAST** [285, 286]. **CAST-Like** [285]. **Castle** [1576, 1831]. **Cayley** [113, 516, 754, 2035, 2113, 2440, 2587, 2849, 2893, 2948, 3194]. **CCA** [2204, 2312, 2570, 2662, 2690, 3171]. **CCA-secure** [2204, 2312, 2570]. **CCZ** [1305, 1492, 1493, 2211, 2760]. **CCZ-equivalence** [1305, 1493]. **CDMA** [651, 1145, 2794, 2908]. **cells** [1885, 3067]. **cellular** [2502, 2994]. **center** [1347]. **Centers** [184]. **Central** [345, 605]. **Certain** [62, 171, 320, 369, 504, 514, 675, 782, 871, 886, 1296, 1338, 1353, 1549, 1720, 1831, 2352, 2569, 2629, 2675, 2927, 2929, 3256]. **Certificateless** [945, 1624]. **ChaCha** [2608]. **Chain** [107, 336, 367, 654, 783, 999, 1381, 1488, 1541, 1601, 2085, 2520, 2560, 2568, 3189, 3296, 3432, 3445]. **Chain-imprimitive** [3189]. **chains** [2887]. **challenge** [2945]. **challenges** [2899]. **Chan** [1017]. **change** [57, 2999]. **changeable** [2999]. **Changed** [725]. **Channel** [1224, 1573, 2057, 2080, 2289, 3280, 3369]. **channels** [913]. **Character** [234, 483, 543, 815, 825, 944, 1029, 1191, 1243, 1735, 1938, 2032, 2084, 2168, 2541]. **character-theoretic** [1938]. **Characterisation** [182, 787, 1409, 1410, 1636]. **characterised** [3150]. **Characterising** [1988, 2483]. **Characteristic** [84, 268, 324, 438, 612, 652, 719, 790, 884, 932, 1124, 1289, 1363, 1382, 1433, 1494, 1507, 1541, 1549, 1551, 1683, 1776, 1846, 1897, 1905, 2208, 2276, 2372, 2390, 2494, 2540, 2672, 2750, 3086, 3401, 3461]. **Characteristics** [369, 1495, 2562, 2759, 3373]. **Characterization** [44, 310, 321, 386, 389, 461, 477, 644, 782, 845, 850, 961, 981, 1088, 1182, 1221, 1456, 1460, 1503, 1585, 2253, 2460, 2649, 2869, 2876, 3200, 3268]. **Characterizations** [38, 71, 130, 169, 293, 463, 517, 752, 755, 924, 1101, 1519, 2117, 2473, 2554, 2946, 3432]. **Characterizing** [161, 290, 3022]. **Characters** [2, 398, 3123, 3414]. **Chat** [555]. **Cheaters** [77, 126, 361, 560, 1153, 1635]. **Cheating** [847, 1328, 1635]. **Chebychev** [1313, 2105]. **Chebyshev** [3121, 3365]. **Check** [234, 278, 815, 825, 1211, 1276, 1784, 1981, 2636, 2848, 2860, 3280]. **checkable** [3154]. **checksum** [283]. **Chevalley** [234, 1480]. **chip** [1888]. **choice** [966, 1164]. **choices** [1204]. **choosability** [3261]. **Choose** [521]. **Chosen** [159, 2268, 2383, 2585, 3085]. **Chosen-ciphertext** [2383, 2585, 3085]. **Chosen-Content** [159]. **chromatic** [1472]. **Chudnovsky** [2841]. **Chudnovsky-type** [2841]. **Chunming** [2857]. **CI** [2376]. **CI-groups** [2376]. **Cipher** [796, 1068, 1070, 1171, 1333, 1527, 1698, 1849, 2321, 2982, 3118]. **Ciphers** [286, 479, 507, 1122, 1283, 1497, 1572, 1603, 2040–2042, 2226–2228, 2243, 2373, 2492, 2539, 2543, 2731, 2988, 3060, 3073, 3228, 3245, 3373, 3400]. **ciphertext** [1091, 2204, 2268, 2383, 2585, 3085].

**ciphertexts** [1299, 1342, 1767, 1901]. **Circle** [685]. **circuit** [1324, 2460, 2777, 2965]. **circuit-private** [2965]. **circuits** [3250, 3375]. **Circulant** [253, 259, 306, 557, 920, 1155, 1438, 1439, 1579, 1674, 2245, 2475, 2699, 3203, 3255]. **Circular** [3117, 3227]. **CIS** [2579]. **clan** [183]. **Clans** [756]. **clarification** [2625]. **Class** [14, 109, 237, 241, 423, 610, 631, 655, 673, 856, 908, 987, 1012, 1102, 1127, 1181, 1193, 1319, 1321, 1331, 1336, 1344, 1377, 1384, 1410, 1572, 1632, 1670, 1672, 1761, 1861, 1921, 1929, 1954, 2018, 2075, 2086, 2286, 2292, 2304, 2323, 2399, 2503, 2544, 2602, 2642, 2672, 2682, 2687, 2737, 2744, 2747, 2861, 2864, 2892, 2894, 2951, 2967, 2997, 3002, 3017, 3071, 3138, 3168, 3196, 3237, 3323, 3341, 3390, 3391, 3410, 3445]. **class-regular** [1331]. **Classes** [195, 320, 368, 541, 934, 958, 1172, 1424, 1516, 1535, 1741, 1778, 1952, 1958, 2006, 2036, 2082, 2170, 2188, 2230, 2237, 2332, 2496, 2546, 2604, 2673, 2688, 2742, 2905, 2964, 2993, 3089, 3266, 3314, 3344, 3423]. **classic** [2010]. **Classical** [24, 47, 75, 389, 591, 681, 910, 942, 1069, 1191, 1337, 1456, 1642, 1994, 2169, 2612, 3016, 3025, 3333, 3334, 3372]. **Classification** [17, 34, 74, 148, 229, 253, 306, 415, 450, 523, 687, 750, 820, 861, 908, 962, 1045, 1094, 1208, 1318, 1347, 1412, 1546, 1582, 1587, 1639, 1691, 1777, 2140, 2353, 2529, 2560, 2583, 2649, 2788, 2814, 2853, 2958, 3109, 3173, 3216, 3247, 3291]. **classifications** [3325, 3412]. **Classifying** [606, 2550, 2642, 3174]. **Clerck** [1637]. **Client** [190, 2937]. **Client-Independent** [190]. **Clifford** [533, 2635]. **clique** [3380, 3449]. **Cliques** [449, 3239]. **close** [1354, 2354, 3069]. **closest** [1164, 1979, 2182]. **CLR** [2369]. **CLR-cryptosystem** [2369]. **clustering** [1484]. **CM** [1526]. **Co** [855, 2056]. **co-dimension** [2056]. **Co-Orthogonal** [855]. **coboundary** [2715]. **Cocks** [2537]. **coclique** [3140]. **cocycles** [2444]. **Cocyclic** [345, 537, 1284]. **Code** [98, 102, 105, 236, 266, 275, 312, 322, 427, 485, 841, 1064, 1065, 1159, 1264, 1401, 1411, 1495, 1569, 1649, 1653, 1659, 1682, 1744, 1783, 1848, 1933, 1944, 2001, 2062, 2100, 2175, 2183, 2213, 2222, 2326, 2337, 2523, 2609, 2615, 2624, 2653, 2683, 2712, 2814, 2845, 2850, 2852, 2889, 2907, 2913, 2915, 2925, 2931, 2950, 2962, 3085, 3112, 3124, 3127, 3165, 3311, 3356, 3394, 3406, 3448]. **Code-based** [2609, 2712, 2845, 2852, 2913, 2915, 3085, 3124, 3356]. **Codebooks** [1021, 1414, 1565, 1632, 1790, 2541, 2948, 3123]. **coded** [2456]. **Codes** [115, 120, 129, 135, 136, 165, 166, 172, 175, 189, 200, 209, 224, 246, 248, 262, 265, 269, 271, 302, 312, 319, 335, 336, 340, 349, 355–357, 371, 381, 385, 386, 388, 407, 408, 411, 414, 441, 447, 462, 492, 496, 500, 523–525, 527, 529, 537, 542, 548, 551, 555, 556, 558, 561, 574, 577, 582, 603, 617, 618, 648, 653, 656, 687, 693, 721, 733, 742, 763, 770, 789, 797, 824, 826, 835, 839, 865, 869, 874, 880, 897, 1009, 1107, 1676, 1855, 1991, 2074, 2589, 2633, 2714, 2924]. **Codes** [67, 122, 131, 134, 141, 148–150, 164, 167, 180, 191, 193, 204, 211, 219, 227, 253, 256, 259, 260, 297, 306, 308, 313, 316, 317, 327, 329, 338, 344, 350, 360, 375, 391, 395, 401, 415, 418, 419, 450, 467, 468, 478, 480, 482, 488, 494, 505, 507, 510, 515, 526, 539, 559, 562, 604, 623, 640, 654, 659, 664, 669, 675, 703, 714, 724, 727, 729, 737, 764, 768, 772, 784, 794, 800, 806, 809, 829, 830, 833, 834, 837, 852, 854, 855, 871, 875, 884, 885, 887, 2613, 2640, 2646, 3087, 3307, 3355]. **Codes** [133, 152, 159, 168, 198, 208, 210, 212, 214, 229, 250, 310, 325, 333, 362, 368, 369, 377, 384, 389, 413, 423, 424, 440, 473, 486, 506, 532, 594, 595, 598, 619, 622, 646, 668, 671, 673, 723, 771, 799, 817, 821, 827, 856, 954, 998, 1024, 1046, 1161, 1180, 1185, 1257, 1278, 1425, 1577, 1579, 1583, 1709, 1770, 1934, 2075, 2084, 2193, 2223, 2244, 2245, 2276, 2355, 2406, 2431, 2432, 2621, 2648, 2649, 2658, 2664, 2668, 2719, 2721, 2724, 2799, 2811, 2854, 2906, 2925, 2927, 2939, 2966, 2972, 3131, 3187, 3274, 3282, 3285, 3293, 3357, 3451, 3462]. **codes** [62, 64, 66, 75, 79, 916, 919, 934, 946, 955, 973, 1003, 1025, 1048, 1135, 1149, 1184, 1202, 1203,

1262, 1265, 1285, 1291, 1329, 1348, 1349, 1375, 1486, 1508, 1586, 1588, 1591, 1601, 1605, 1606, 1608, 1644, 1670, 1679, 1794, 1842, 1868, 1946, 1961, 1992, 2044, 2116, 2184, 2202, 2206, 2253, 2274, 2279, 2300, 2313, 2343, 2350, 2386, 2413, 2445, 2460, 2468, 2479, 2486, 2526, 2567, 2591, 2596, 2607, 2617, 2641, 2675, 2729, 2754, 2777, 2783, 2788, 2834, 2848, 2866, 3004, 3010, 3040, 3093, 3120, 3133, 3157, 3162, 3185, 3204, 3226, 3259, 3337, 3411, 3418, 3440, 3456]. **codes** [82, 88, 90, 225, 910, 929, 943, 972, 1086, 1088, 1093, 1103, 1118, 1127, 1131, 1143, 1163, 1165, 1183, 1204, 1209, 1281, 1307, 1308, 1345, 1354, 1407, 1504, 1552, 1598, 1623, 1666, 1684, 1691, 1699, 1748, 1749, 1761, 1779, 1815, 1841, 1844, 1924, 1941, 1969, 1973, 2024, 2026, 2031, 2160, 2163, 2221, 2240, 2246, 2257, 2260, 2291, 2293, 2338, 2351, 2421, 2466, 2504, 2515, 2524, 2545, 2547, 2579, 2597, 2676, 2691, 2695, 2698, 2716, 2734, 2757, 2812, 2838, 2901, 2938, 2984, 2993, 3011, 3034, 3110, 3128, 3129, 3132, 3159, 3191, 3201, 3281, 3342, 3354, 3359, 3388, 3391, 3445]. **codes** [31, 41, 80, 295, 907, 918, 927, 951, 961, 989, 1015, 1051, 1072, 1082, 1097, 1112, 1132, 1155, 1236, 1251, 1292, 1355, 1370, 1371, 1389, 1438, 1498, 1528, 1529, 1562, 1580, 1587, 1592, 1617, 1657, 1704, 1731, 1789, 1824, 1828, 1830, 1832, 1853, 1877, 1966, 2029, 2043, 2052–2055, 2057, 2101, 2105, 2142, 2171, 2181, 2254, 2277, 2330, 2379, 2391, 2481, 2490, 2525, 2534, 2540, 2561, 2568, 2576, 2593, 2598, 2678, 2735, 2753, 2758, 2763, 2791, 2819, 2828, 2836, 2837, 2847, 2964, 3059, 3066, 3089, 3100, 3103, 3144, 3168, 3192, 3224, 3251, 3262, 3350, 3434, 3439]. **codes** [20, 35, 40, 72, 89, 91, 142, 307, 343, 908, 911, 917, 930, 942, 1001, 1010, 1016, 1026, 1061, 1066, 1084, 1100, 1110, 1199, 1274, 1381, 1402, 1406, 1421, 1457, 1488, 1489, 1558, 1578, 1584, 1594, 1669, 1673, 1714, 1745, 1746, 1772, 1774, 1783, 1806, 1808, 1821, 1829, 1951, 2019, 2033, 2038, 2069, 2086, 2102, 2141, 2187, 2197, 2201, 2234, 2289, 2370, 2398, 2409, 2440, 2528, 2560, 2571, 2572, 2632, 2674, 2705, 2717, 2722, 2732, 2784, 2825, 2826, 2844, 2849, 2850, 2892, 2893, 2912, 2917, 2977, 3061, 3064, 3081, 3098, 3198, 3203, 3210, 3211, 3236, 3283, 3286, 3287, 3310, 3317, 3324, 3420, 3423]. **codes** [15, 47, 938, 941, 993, 999, 1005, 1057, 1266, 1366, 1377, 1450, 1510, 1559, 1561, 1582, 1593, 1607, 1612, 1689, 1712, 1717, 1726, 1730, 1732, 1733, 1793, 1796, 1847, 1861, 1922, 1932, 1954, 1978, 1987, 1990, 2004, 2015, 2018, 2079, 2114, 2135, 2216, 2233, 2272, 2298, 2324, 2327, 2332, 2393, 2420, 2446, 2473, 2475, 2477, 2480, 2495–2498, 2503, 2520, 2521, 2581, 2587, 2599, 2600, 2605, 2643, 2657, 2709, 2745, 2778, 2800, 2818, 2860, 2863, 2921, 2943, 2974, 3006, 3037, 3039, 3065, 3071, 3072, 3116, 3142, 3177, 3184, 3213, 3222, 3225, 3241, 3243, 3269, 3340, 3344, 3367, 3377, 3379, 3413, 3414, 3417, 3422, 3427, 3432]. **codes** [2, 46, 169, 914, 922, 936, 950, 956, 957, 1011, 1059, 1079, 1108, 1120, 1170, 1173, 1260, 1267, 1320, 1321, 1330, 1378, 1441, 1517, 1523, 1556, 1557, 1585, 1590, 1595, 1646, 1693, 1718, 1723, 1769, 1784, 1813, 1831, 1833, 1836, 1865, 1870, 1881, 1937, 1958, 1974, 1983, 2059, 2076, 2077, 2103, 2154, 2194, 2196, 2217, 2219, 2232, 2264, 2285, 2287, 2314, 2352, 2436, 2462, 2489, 2519, 2550, 2583, 2592, 2627, 2636, 2655, 2741, 2772, 2793, 2810, 2835, 2840, 2923, 2928, 3063, 3108, 3109, 3122, 3161, 3208, 3212, 3215, 3217, 3234, 3238, 3252, 3277, 3362, 3383, 3387, 3390, 3415, 3444]. **codes** [38, 96, 112, 658, 948, 952, 958, 1007, 1023, 1096, 1114, 1145, 1160, 1177, 1210, 1211, 1253, 1332, 1386, 1416, 1426, 1487, 1490, 1503, 1555, 1589, 1716, 1747, 1752, 1756, 1760, 1766, 1795, 1823, 1827, 1839, 1918, 1929, 1943, 2106, 2146, 2199, 2220, 2242, 2258, 2271, 2280, 2284, 2307, 2354, 2365, 2387, 2411, 2429, 2438, 2443, 2453, 2465, 2467, 2484, 2517, 2573, 2577, 2584, 2614, 2659, 2769, 2785, 2805, 2832, 2839, 2843, 2846, 2865, 2874, 2895, 2902, 2918–2920, 2942, 2959, 2969, 2989, 3000, 3023, 3036, 3077, 3088, 3096, 3137, 3150, 3151, 3155, 3170, 3265, 3339, 3343, 3358, 3421, 3438]. **codes** [28, 52, 105, 106, 346, 959, 974, 990, 1012, 1028, 1058, 1060, 1073, 1102, 1109, 1178, 1195, 1196, 1294, 1380, 1420, 1471, 1560, 1597, 1609, 1618,

1620, 1660, 1672, 1685, 1707, 1725, 1742, 1754, 1764, 1777, 1800, 1805, 1807, 1811, 1955, 2006, 2022, 2035, 2068, 2093, 2096, 2153, 2173, 2176, 2230, 2288, 2292, 2309, 2316, 2339, 2375, 2415, 2457, 2507, 2527, 2546, 2574, 2623, 2687, 2700, 2706, 2733, 2792, 2801, 2802, 2829, 2857, 2861, 2871, 2891, 2958, 2971, 2980, 2992, 2998, 3022, 3041, 3086, 3114, 3125, 3134, 3135, 3148, 3160, 3167, 3176, 3181, 3194, 3206, 3209, 3244, 3306, 3312, 3314, 3319, 3321, 3360, 3385, 3386, 3407, 3431, 3437]. **codeword** [1649]. **codewords** [21, 942, 1015, 1210, 1251, 1411, 1709, 2386, 3187, 3342]. **codimension** [102, 2466, 3191]. **Coding** [94, 326, 935, 1018, 1352, 1369, 1474, 1576, 1584, 1708, 1826, 1888, 1913, 1914, 2039, 2189, 2192, 2194, 2198, 2441, 2601, 2827, 2831, 3067, 3079, 3091, 3095, 3185, 3423, 3431, 3446]. **coding-theoretic** [94]. **coefficients** [1350, 1471, 1668, 1710, 1797]. **cofactor** [2305]. **coherent** [2126]. **Cohn** [639, 843, 2442, 2511]. **coincidence** [924]. **coincidences** [918]. **collaborative** [1578]. **collinear** [3424]. **Collinearity** [300, 451]. **Collineation** [8, 232]. **Collineations** [417, 555, 1434, 2148]. **Collision** [766, 1297, 1318, 1596, 1698, 2011, 2089, 2160, 2530, 3119]. **collision-flat** [3119]. **collisions** [1369]. **colluding** [2456]. **collusion** [1342]. **collusion-resistant** [1342]. **color** [1360, 1737, 2401]. **Colored** [453, 777]. **Coloring** [2878]. **colorings** [1366]. **Colouring** [289]. **colourings** [3426]. **column** [2484, 3054, 3255]. **column-orthogonal** [3054]. **Combin** [55]. **Combinational** [2826]. **Combinatorial** [38, 169, 217, 338, 450, 478, 494, 506, 629, 698, 703, 924, 1042, 1073, 1179, 1351, 1428, 1429, 1623, 1629, 1633, 1634, 1661, 1910, 1918, 2059, 2063, 2150, 2179, 2186, 2218, 2219, 2260, 2316, 2398, 2510, 2696, 2766, 2878, 2880, 2918, 2919, 3177, 3207, 3312, 3404, 3436, 3437]. **Combinatorics** [745, 1454, 2287, 2827, 2875]. **Combining** [3050, 3153]. **comes** [1744]. **coming** [2277]. **Comment** [1787]. **Comments** [757, 1328]. **Commitment** [576, 1189]. **commitments** [3250, 3428]. **Common** [1496, 2626, 3332]. **Communication** [446, 859, 2078, 3218, 3375]. **Communication-Computation** [859]. **Communications** [693, 933, 2794]. **Commutative** [442, 793, 1096, 1358, 1427, 1617, 1766, 1828, 2232, 2296, 2301, 2526, 2650, 2851, 3430]. **Compact** [795, 1940, 2171, 2704, 2736, 3027, 3172, 3221]. **Comparing** [1223]. **Comparison** [1823, 1999, 3207]. **compartmented** [2472]. **Compatible** [2833, 3385]. **Complement** [232, 845, 1986, 3370, 3431]. **Complementary** [45, 90, 305, 604, 934, 1765, 2038, 2264, 2288, 2480, 2568, 2680, 2732, 2740, 2798, 2902, 2907, 3025, 3263, 3316, 3367, 3444]. **complementation** [1086, 1779]. **Complete** [34, 122, 125, 180, 400, 403, 564, 607, 627, 646, 746, 773, 807, 861, 887, 1125, 1183, 1231, 1503, 1644, 1963, 1987, 2015, 2068, 2075, 2138, 2149, 2329, 2364, 2477, 2529, 2624, 2633, 2676, 2743, 2764, 2792, 2869, 2942, 2958, 3009, 3264, 3382, 3407]. **completed** [2602, 2682, 2997, 3196]. **Completely** [95, 155, 213, 1215, 1300, 1366, 1588, 1622, 1859, 2002]. **completeness** [2083]. **completion** [9, 1872, 2778]. **completions** [1208]. **Complex** [557, 1339, 1977, 2635, 2955, 3260, 3268]. **complexes** [2293, 3213]. **Complexities** [2224]. **Complexity** [42, 104, 247, 249, 330, 499, 535, 545, 556, 615, 639, 725, 765, 843, 870, 912, 949, 1017, 1077, 1089, 1092, 1182, 1217, 1298, 1302, 1357, 1361, 1372, 1394, 1442, 1451, 1484, 1515, 1524, 1525, 1694, 1763, 1785, 2020, 2025, 2042, 2178, 2243, 2304, 2363, 2374, 2442, 2454, 2652, 2864, 3106, 3171, 3188, 3218, 3265, 3381]. **component** [1829, 3410]. **Components** [885, 2340, 2455, 2556, 3097, 3368]. **Composed** [1564, 1690, 2399, 3305]. **Composite** [939, 1446, 2691, 2753, 3158, 3437].

**Composition** [530, 897, 1092, 1102, 1199, 1721, 2569, 3105]. **compositional** [3084, 3318, 3457]. **compositions** [1365]. **Compressed** [3158]. **Compression** [1765, 1812, 1926, 1935, 2099, 2988]. **compromise** [1757]. **Computation** [4, 678, 686, 859, 953, 1361, 1390, 1827, 1893, 2275, 2537, 2569, 2909, 3106, 3156, 3164, 3169, 3419]. **Computational** [503, 878, 2177, 2180, 3453]. **computations** [1124, 1518]. **Computer** [747, 1826, 1844]. **Computer-Assisted** [747]. **Computing** [313, 563, 1121, 1282, 1776, 1919, 2563, 2600, 3202]. **concatenated** [2834]. **Concatenating** [792]. **Concatenation** [2194, 2801]. **Concept** [629, 1311]. **Concepts** [492, 3322]. **conceptually** [3154]. **Concerning** [43, 202, 565, 1270, 1451]. **concrete** [2665, 3145]. **concurrence** [2167]. **Condition** [227, 336, 1292, 1395, 1649]. **Conditional** [2248, 2634]. **Conditions** [70, 752, 1011, 1181, 2349, 2487, 2728, 2767, 2768, 2898, 3050, 3162]. **Cone** [629]. **cones** [3262]. **Conference** [675, 2877]. **confidentiality** [1630]. **Configuration** [184, 1351, 2126, 2886]. **configurations** [1130, 1154, 1351, 1482, 1633, 1634, 1686, 1927, 1980, 2376, 2628, 2797, 2872]. **conflict** [1011, 1170, 1253, 1657, 1733, 1847, 1932, 1955, 2391]. **conflict-avoiding** [1011, 1170, 1253, 1657, 1733, 1847, 1932, 1955]. **Congruence** [163, 1948, 2744]. **congruences** [2279]. **Congruential** [765, 870, 997, 2286]. **Conic** [840, 886, 1275, 2953]. **Conics** [410, 910, 1663, 1922, 1967, 1988, 2880]. **Conjecture** [26, 208, 291, 333, 382, 520, 720, 1137, 1239, 1325, 1479, 1568, 1911, 2065, 2105, 2124, 2207, 2212, 2267, 2335, 2357, 2441, 2458, 2485, 2878, 3002, 3399]. **Conjectures** [799, 1597, 2249, 2388, 2498]. **conjugacy** [347]. **conjugate** [1052, 2635]. **Conjunctive** [3299]. **connected** [1580]. **Connecting** [2209]. **connection** [2323, 2435, 2963, 2975, 3371]. **Connections** [1719]. **connectivity** [56, 3371]. **Consecutive** [240, 3442]. **consequences** [1206]. **consisting** [1052]. **Consolidation** [2171]. **consta** [2966]. **consta-cyclic** [2966]. **Constacyclic** [1307, 1764, 2135, 2142, 2153, 2216, 2244, 2375, 2534, 2716, 2837, 2925, 3023, 3071, 3222, 3281, 3306, 3367, 3388, 3448, 3451]. **Constant** [129, 356, 423, 424, 440, 897, 961, 1058, 1059, 1102, 1109, 1199, 1253, 1380, 1669, 1714, 1796, 1815, 1958, 2233, 2246, 2409, 2583, 2850, 2870, 2891, 2892, 2912, 2943, 3003, 3099, 3142, 3203, 3265, 3286, 3287, 3386]. **constant-dimension** [2850]. **constant-time** [3099]. **Constant-Weight** [423, 1253, 1714, 1796, 2233]. **constants** [1352, 2809, 3281, 3446]. **constituent** [3339]. **constrained** [66]. **constraint** [2489]. **constraints** [2171, 3186]. **Construct** [266, 1737, 3143]. **Constructed** [675, 703, 731, 813, 926, 1599, 1854, 2224, 2505, 2716, 3234]. **Constructing** [111, 115, 286, 323, 360, 769, 914, 1325, 1508, 1609, 1654, 1682, 1727, 1770, 1806, 2235, 2252, 2394, 2499, 2835, 2855, 2884, 2934, 3006, 3053, 3105, 3123, 3195, 3210, 3301, 3323, 3389, 3393]. **Construction** [37, 41, 52, 91, 133, 135, 181, 221, 236, 280, 296, 304, 327, 351, 354, 369, 375, 506, 536, 605, 662, 664, 740, 776, 804, 823, 889, 896, 897, 917, 945, 952, 971, 1001, 1335, 1360, 1392, 1401, 1414, 1447, 1500, 1501, 1509, 1526, 1616, 1693, 1697, 1732, 1808, 1813, 1945, 2019, 2045, 2051, 2066, 2102, 2137, 2162, 2226, 2247, 2269, 2272, 2319, 2368, 2370, 2390, 2434, 2445, 2478, 2484, 2519, 2577, 2579, 2593, 2618, 2619, 2685, 2686, 2699, 2709, 2719, 2722, 2783, 2791, 2841, 2850, 2851, 2912, 3009, 3061, 3086, 3102, 3127, 3133, 3147, 3152, 3154, 3176, 3256, 3286, 3287, 3377, 3458]. **construction** [63, 1050, 1452, 1544, 1719, 1740, 1804, 1986, 2095, 2153, 2238, 2241, 2422, 2690, 2843, 2960, 2980, 3077, 3145, 3150, 3227, 3267, 3313, 3339, 3383]. **Construction-D** [3127]. **Constructions** [18, 51, 88, 138, 185, 194, 261, 341, 364, 470,

496, 569, 576, 580, 693, 733, 771, 807, 828, 861, 898, 915, 919, 928, 936, 960, 988, 996, 1005, 1020, 1136, 1234, 1305, 1372, 1385, 1481, 1573, 1623, 1677, 1719, 1733, 1734, 1843, 1910, 1917, 1923, 1977, 1980, 1982, 2003, 2024, 2033, 2063, 2135, 2156, 2181, 2217, 2221, 2233, 2246, 2260, 2291, 2302, 2329, 2333, 2339, 2402, 2464, 2472, 2514, 2541, 2548, 2605, 2606, 2656–2658, 2691, 2730, 2798, 2818, 2826, 2891, 2911, 2977, 3005, 3008, 3054, 3074, 3142, 3162, 3171, 3177, 3182, 3211, 3212, 3232, 3236, 3275, 3289, 3327, 3382, 3415, 3417]. **constructions** [99, 948, 1073, 1195, 1569, 1827, 2072, 2146, 2158, 2218, 2223, 2403, 2457, 2469, 2554, 2556, 2616, 2631, 2768, 2907, 2946, 3244, 3386]. **Constructive** [1487, 2225]. **Contactless** [859]. **contacts** [3069]. **contain** [1933, 2453, 2900]. **Contained** [840]. **Containing** [195, 1964, 2429, 2785]. **Content** [159]. **Contents** [802]. **Continuous** [2423]. **contracting** [1303, 3171]. **contraction** [2426]. **contrast** [2144, 2401]. **Contributions** [2875]. **control** [339, 2017, 2899]. **Controllable** [676]. **conversion** [1390]. **Convolutional** [225, 250, 1595, 1992, 2076, 2193, 2194, 2473, 2477, 2621, 2719, 3413, 3439]. **cooling** [3177]. **Coordinate** [447, 3396]. **coordinate-additive** [3396]. **coordinates** [1121, 2279]. **Coprimitive** [1046]. **COPs** [426]. **core** [969, 2899]. **Corrected** [188, 189]. **Correcting** [88, 135, 317, 506, 524, 595, 619, 623, 800, 941, 952, 1073, 1082, 1184, 1278, 1320, 1620, 1659, 1712, 1746, 1754, 2129, 2181, 2355, 2567, 2579, 2675, 2714, 2866, 2977, 3081, 3129, 3135, 3177, 3274, 3360, 3420, 3431, 3444]. **Correction** [120, 164, 246, 555, 1090, 1726, 1888, 2220, 2388, 2403, 2425, 2442, 2682, 2707, 2760, 2761, 2813, 2919, 3275, 3316, 3412, 3462]. **correctors** [3275]. **Correlation** [130, 365, 374, 670, 726, 760, 1304, 1323, 1506, 1603, 1665, 1700, 1874, 1912, 2037, 2137, 2281, 2437, 2451, 2461, 2489, 3030, 3153, 3228, 3435]. **Correlation-Immune** [130, 365, 2437]. **Correlations** [84, 268, 1798, 2824]. **correspond** [1988]. **Correspondence** [265]. **Corresponding** [241, 390, 916, 1588, 3307]. **corruption** [2312]. **corruptions** [2570]. **Coset** [764, 1262, 1588, 1641, 2889]. **cosets** [2230]. **Cospectral** [471]. **cost** [1273, 2774, 3375]. **Costas** [2926]. **coterm** [2270]. **Coulter** [1213]. **counter** [98, 1062]. **counter-attacks** [1062]. **counter-example** [98]. **counterexample** [1451]. **countermeasure** [1573]. **countermeasures** [1743]. **Counting** [330, 857, 885, 1314, 1699, 2087, 2296, 2610, 3104]. **Cover** [694, 712, 1921, 2052, 2054, 2305]. **Cover-Free** [694, 712, 2052, 2054]. **covered** [1751, 2595, 2929]. **Covering** [3, 40, 57, 72, 80, 121, 129, 192, 224, 260, 302, 316, 349, 357, 360, 372, 383, 418, 496, 567, 603, 648, 709, 713, 727, 772, 806, 819, 915, 917, 943, 1026, 1061, 1064, 1123, 1209, 1226, 1307, 1380, 1385, 1562, 1664, 1712, 1740, 1746, 2044, 2168, 2183, 2225, 2315, 2466, 2512, 2825, 2865, 2933, 2957, 3048, 3191, 3418, 3449]. **Coverings** [352, 632, 991, 1577]. **Covers** [292, 353, 589, 746, 1111, 1147, 1444, 1604, 2371, 2419]. **Coxeter** [469, 2876]. **CPM** [2484]. **Cracker** [1950]. **criteria** [1627]. **Criterion** [161, 658, 2028, 2324]. **critical** [2282]. **Critique** [1311]. **Crooked** [1032, 1115]. **Cross** [84, 268, 2489]. **cross-correlation** [2489]. **Cross-Correlations** [84, 268]. **Crossbred** [3398]. **crosscorrelation** [1126, 3113]. **crosstalk** [1888]. **CRT'** [1496]. **cryptanalyses** [1302]. **Cryptanalysis** [285, 445, 601, 1122, 1527, 1551, 1603, 1849, 1862, 1940, 2037, 2042, 2071, 2132, 2285, 2367, 2369, 2380, 2461, 2476, 2500, 2516, 2581, 2609, 2681, 2712, 2816, 2870, 2983, 3060, 3082, 3228, 3245, 3246, 3276, 3356, 3374, 3430]. **Cryptanalytic** [1496, 1999]. **Cryptanalyzing** [966]. **crypto** [2867]. **Cryptocash** [1906]. **cryptocodes** [13]. **cryptocontracts** [1906]. **cryptocurrencies** [1906]. **Cryptogr** [120, 134, 164, 189, 333].

**Cryptographer** [155]. **Cryptographic** [157, 161, 449, 567, 676, 732, 763, 792, 849, 904, 1036, 1214, 1246, 1701, 1737, 1982, 1992, 2340, 2405, 2488, 2796, 2845, 2932, 3015]. **Cryptographically** [1270, 2654, 2751]. **Cryptography** [154, 365, 430, 434, 493, 544, 552, 555, 562, 600, 777, 810, 847, 873, 883, 1006, 1113, 1614, 1708, 1753, 1826, 1915, 1935, 2039, 2066, 2144, 2601, 2909, 3055, 3095]. **Cryptology** [1429, 2589]. **Cryptosystem** [119, 137, 144, 314, 497, 798, 1062, 1095, 1594, 1891, 2301, 2369, 2679, 2681, 3066, 3274, 3436]. **Cryptosystems** [193, 324, 340, 503, 521, 663, 704, 781, 1194, 1505, 1990, 2195, 2268, 2746, 2770, 3403]. **Crypts** [175]. **CRYSTALS** [3427]. **CRYSTALS-Kyber** [3427]. **CSI** [3237]. **CSI-Otter** [3237]. **CSS** [3204]. **CSS-T** [3204]. **cube** [1786, 1820, 2139, 2248, 2380, 2492, 2910]. **cube-attack-like** [2380]. **Cubes** [644]. **Cubic** [65, 370, 710, 1138, 1332, 1440, 1834, 1879, 2083, 2278, 2360, 2602, 2682, 2718, 2886, 2889]. **cubics** [1641]. **Cumulative** [900]. **Cunsheng** [2857]. **Curve** [314, 434, 436, 660, 781, 809, 830, 837, 873, 884, 887, 956, 1100, 1275, 1499, 1518, 1706, 1744, 1904, 1959, 1997, 2029, 2050, 2184, 2236, 2240, 2300, 2386, 2500, 2595, 2929, 3238, 3258, 3401]. **Curve-lifted** [3238]. **Curve25519** [1889]. **Curves** [277, 435, 458, 521, 542, 545, 564, 765, 795, 810, 846, 857, 862, 928, 997, 1009, 1087, 1150, 1188, 1197, 1245, 1282, 1422, 1425, 1522, 1526, 1570, 1604, 1867, 1897, 1899, 1919, 1963, 2020, 2064, 2083, 2099, 2299, 2305, 2325, 2331, 2537, 2589, 2590, 2595, 2613, 2664, 2774, 2929, 2984, 3031, 3043, 3051, 3220, 3230, 3447]. **Cusick** [2212]. **custody** [3169]. **cut** [3024]. **Cycle** [36, 176, 1052, 1232, 1803, 1878, 1995, 2261, 2323, 2324, 2377, 2554, 2603, 2951, 3267, 3410]. **cycle-free** [2324]. **cycles** [1235, 1274, 1287, 1368, 1681, 1721, 2110, 2341, 2578, 2900]. **Cyclic** [11, 15, 31, 43, 81, 136, 167, 196, 213, 238, 302, 358, 369, 385, 441, 505, 525, 561, 577, 612, 654, 665, 695, 719, 731, 742, 780, 819, 852, 854, 863, 869, 954, 969, 1117, 1281, 1288, 1294, 1329, 1349, 1375, 1389, 1406, 1407, 1423, 1508, 1601, 1659, 1670, 1730, 1761, 1762, 1829, 1841, 1857, 1861, 1934, 1954, 1973, 1987, 1990, 2018, 2026, 2055, 2073, 2103, 2135, 2154, 2175, 2197, 2202, 2233, 2246, 2257, 2298, 2351, 2370, 2376, 2431, 2445, 2498, 2560, 2640, 2721, 2724, 2734, 2754, 2778, 2828, 2840, 2860, 2925, 2943, 2966, 2974, 3340, 3342, 3378, 3379, 3417, 3444, 3456]. **cyclic** [55, 96, 98, 291, 333, 958, 994, 1503, 1609, 1618, 1672, 1747, 1807, 1836, 2006, 2220, 2309, 2314, 2375, 2613, 2769, 2772, 2792, 2793, 2802, 2859, 2891, 2989, 3023, 3148, 3217, 3244, 3252, 3265, 3306, 3314, 3339, 3407]. **cyclic-gap** [3265]. **Cyclotomic** [144, 171, 1129, 1361, 1405, 1414, 1477, 1525, 1564, 1565, 1778, 2081, 2230, 2238, 2259, 2374, 2454, 2546, 2694, 2864, 3416, 3429]. **cyclotomy** [1226, 1566]. **cylinder** [2357].

**D** [1595, 1623, 2087, 2391, 3127]. **D.** [2131]. **Damgård** [3313]. **Daniel** [1513]. **dark** [2867]. **data** [1302, 1888, 2243, 2312, 2518, 2696, 2726, 2988, 3078, 3207]. **database** [1633, 1634, 2127]. **databases** [2456]. **Davenport** [1352, 1773]. **Davies** [2319]. **dc** [66]. **dc-constrained** [66]. **DD** [1076]. **DDH** [1216]. **Dealer** [264]. **decades** [1903]. **Decentralized** [2937]. **decimations** [2511]. **deciphering** [1799]. **decisional** [1864, 2308]. **decodability** [1356, 2785]. **Decodable** [386, 935, 2171, 3041]. **Decoding** [87, 165, 211, 295, 903, 911, 1097, 1161, 1346, 1486, 1490, 1556, 1578, 1579, 1620, 1684, 1716, 1723, 1725, 1772, 1828, 1842, 2053, 2100, 2206, 2404, 2617, 2679, 2846, 2913, 2915, 3052, 3098, 3185, 3265, 3280, 3349, 3363, 3395, 3406, 3413, 3439]. **decoding-to-LPN** [3406]. **decomposable** [3140, 3380]. **Decomposing** [3076]. **Decomposition** [354, 1435, 1668, 1986, 2064, 2299, 2711, 2963, 2975, 3069].

**decompositions** [1803, 1863, 3264, 3333]. **Decrease** [725]. **Decreasing** [2449, 3128, 3411]. **Decryption** [796, 3257]. **dedicated** [1219, 2108]. **deep** [1713, 2449]. **DeepBKZ** [2552]. **Defect** [248]. **defective** [3067]. **Defects** [3093]. **deficiency** [1680, 1788]. **defined** [301, 942, 1107, 1592, 1608, 1997]. **Defining** [902, 1591, 2332]. **definition** [3145]. **definitions** [2384]. **degenerate** [1107, 3025]. **Degree** [143, 547, 701, 909, 1107, 1315, 1332, 1447, 1776, 1812, 2529, 2746, 2793, 2807, 2935, 2939, 3180, 3256, 3331, 3399, 3422]. **degrees** [1507, 2537, 3100, 3158, 3441]. **Dehon** [207]. **Delandtsheer** [2888]. **delegation** [2518]. **Deletion** [135, 317, 506, 595, 952, 1073, 1278, 1754, 2567, 2579, 2866]. **Deletion-Correcting** [135, 506, 1073]. **deletions** [2977, 3135, 3360]. **Deligne** [2613]. **Delsarte** [7, 79, 219, 620, 1323, 1480, 2986, 3380]. **Delsarte-Goethals** [79, 219]. **Dembowski** [1343, 1540]. **demerit** [3329]. **Demi** [1794]. **Demi-matroids** [1794]. **deniable** [2752]. **Denniston** [2350]. **Densest** [326]. **Densities** [3100]. **density** [249, 965, 1211, 2848, 3038, 3199]. **Denting** [137]. **Deoxys** [3304]. **Dependence** [629]. **Dependent** [601, 1441]. **depth** [1874]. **depths** [2650]. **Derivation** [960, 1114, 2188]. **derivations** [1605, 2012]. **Derivative** [3306]. **Derivatives** [2963]. **Derived** [232, 288, 611, 885, 1211, 1524, 2020, 2385, 2496, 2923, 3203, 3253]. **DES-like** [340, 939]. **Desarguesian** [24, 201, 348, 495, 679, 697, 1015, 1248, 1537, 1675, 2427]. **descendants** [3306]. **Descent** [791]. **described** [48]. **Description** [732, 1149, 2961]. **Design** [48, 119, 135, 182, 286, 394, 491, 566, 602, 691, 758, 803, 939, 978, 1277, 1312, 1388, 1648, 1848, 2007, 2465, 2655, 2770, 2908, 3080, 3140, 3239, 3260, 3347, 3380]. **Design-theoretic** [1277, 1388, 2655]. **Designed** [173, 188, 837, 884, 2429, 2598, 3168]. **Designer** [3277]. **Designing** [792, 2796, 2817, 3196]. **Designs** [30, 55, 116, 121, 127, 175, 194, 198, 201, 207, 235, 238, 240–242, 244, 245, 254, 258, 267, 287, 296, 311, 323, 334, 356, 371, 376, 389, 392, 402, 409, 414, 440, 456, 464, 475, 490, 502, 516, 520, 541, 554, 555, 559, 573, 577–580, 587, 591, 593, 597, 604, 616, 617, 620, 622–624, 631, 646, 658, 659, 671, 677, 702, 703, 706, 707, 711, 740, 743, 774, 776, 782, 790, 820, 833, 851, 872, 879, 901, 970, 1025, 1259, 1340, 1482, 1835, 1953, 2027, 2111, 2533, 2743, 2858, 2888, 3189, 3334, 3433]. **designs** [5, 20, 39, 56, 60, 89, 109, 117, 142, 343, 907, 926, 934, 937, 947, 963, 964, 979, 1040, 1053, 1071, 1084, 1128, 1135, 1137, 1143, 1148, 1222, 1228, 1234, 1331, 1334, 1344, 1400, 1404, 1429, 1456, 1463, 1511, 1621, 1638, 1668, 1673, 1695, 1731, 1745, 1762, 1819, 1854, 1882, 1916, 1936, 1937, 1941, 1952, 1972, 1995, 2014, 2054, 2059, 2133, 2179, 2189, 2191, 2207, 2213, 2247, 2265, 2273, 2297, 2320, 2385, 2400, 2416, 2439, 2459, 2464, 2504, 2515, 2670, 2677, 2678, 2699, 2708, 2830, 2856, 2885, 2911, 3020, 3083, 3207, 3235, 3239, 3248, 3323, 3354, 3404, 3455]. **designs** [17, 34, 57, 61, 63, 71, 78, 97, 346, 811, 931, 1028, 1177, 1218, 1237, 1256, 1269, 1286, 1300, 1380, 1423, 1483, 1619, 1633, 1634, 1759, 1859, 1863, 1918, 1996, 2034, 2095, 2121, 2157, 2158, 2219, 2241, 2283, 2322, 2392, 2463, 2467, 2469, 2510, 2532, 2553, 2647, 2766, 2769, 2779, 2780, 2839, 2855, 2857, 2859, 2887, 2922, 3003, 3007, 3016, 3057, 3119, 3148, 3232, 3273, 3289, 3312, 3326, 3358, 3362, 3438]. **detectable** [1635]. **detecting** [1379, 3271]. **Detection** [361, 560, 1090, 1153, 1328, 2584, 3328]. **determinantal** [3151]. **Determination** [809, 838, 887, 1872, 2220, 2633, 3088]. **determine** [2982]. **determining** [1538]. **Deterministic** [716]. **Development** [154]. **DFT** [330, 742]. **Diagonal** [402, 2881, 2994]. **diagonalization** [1967]. **Diagonally** [1857]. **Diagram** [23, 2339, 3065, 3141]. **diameter** [22, 1457, 1459, 1542, 2424, 2425]. **diamond**

[3298]. **diassociative** [1960]. **diatomic** [2739]. **Dickson** [213, 870, 2605]. **Difference** [6, 10, 26, 27, 29, 70, 85, 103, 108, 114, 115, 139, 171, 181, 185, 195, 202, 241, 251, 252, 255, 266, 294, 304, 318, 341, 342, 347, 377, 398, 404, 439, 448, 487, 504, 522, 546, 569, 605, 609, 612, 665, 719, 731, 780, 803, 819, 864, 898, 1011, 1021, 1076, 1119, 1123, 1141, 1147, 1151, 1176, 1233, 1239, 1288, 1404, 1507, 1677, 1680, 1735, 1738, 1778, 1822, 1847, 1930, 1962, 2063, 2080, 2138, 2140, 2145, 2161, 2252, 2255, 2320, 2328, 2346, 2347, 2368, 2378, 2391, 2434, 2447, 2644, 2719, 2723, 2735, 2755, 2926, 2985, 3173, 3182, 3195, 3229, 3320, 3371, 3372, 3459]. **difference** [46, 63, 345, 983, 1037, 1104, 1162, 1268, 1286, 1544, 1632, 1697, 1804, 1856, 1907, 1985, 2238, 2309, 2397, 2584, 2713, 2833, 2871, 2897, 3117, 3227, 3385]. **difference-balanced** [1268]. **Difference-based** [2713, 2926]. **differences** [3322]. **Different** [155, 3281]. **Differential** [285, 428, 601, 1596, 1849, 1862, 2047, 2094, 2263, 2394, 2461, 2476, 2562, 2608, 2629, 2634, 2672, 2673, 2821, 2870, 2967, 3017, 3060, 3066, 3107, 3130, 3276, 3341, 3353, 3373, 3393, 3400, 3430, 3448, 3452]. **differential-linear** [1862]. **Differentially** [1654, 1722, 1866, 1917, 2267, 2333, 2620]. **differentials** [2262, 2731]. **differentiation** [2139]. **Diffie** [433, 1175, 1383, 2308, 2336]. **diffusion** [1303, 1696, 2028, 2051, 2306]. **digit** [940, 1164, 1276, 1290, 1981, 2739, 3146]. **Digital** [359, 519, 575, 619, 660, 1134, 1293, 2433, 3349, 3392]. **Digraph** [2625]. **digraphs** [2814]. **Dihedral** [27, 203, 609, 864, 2561, 2793]. **dihedrants** [925]. **Dillon** [1778]. **Dillon-Player** [1778]. **Dimension** [75, 312, 350, 388, 403, 466, 488, 514, 532, 783, 799, 826, 998, 1094, 1109, 1188, 1314, 1558, 1768, 1808, 1958, 1990, 2056, 2246, 2850, 2891, 2910, 2912, 2943, 2950, 3089, 3142, 3286, 3287, 3362]. **Dimensional** [19, 63, 457, 984, 1044, 1195, 1250, 1255, 1347, 1420, 1422, 1424, 1667, 1786, 1795, 1953, 1994, 2030, 2322, 2421, 2432, 2598, 2798, 2843, 2978, 3063, 3093, 3269, 3337, 3365, 3385]. **Dimensions** [125, 326, 967, 1359, 1597, 2882, 3161]. **Ding** [2250, 2857]. **Diophantine** [703, 1505]. **Direct** [946, 1992, 2045, 2072, 2639, 2909]. **Directed** [145, 420, 1278, 1308, 2631]. **directions** [1538, 3193]. **Dirt** [156]. **Discrete** [4, 158, 324, 432, 436, 553, 584, 615, 1166, 1173, 1200, 1518, 1651, 1711, 1793, 1900, 1904, 1905, 2363, 2404, 2506, 2563, 2875, 3068, 3205, 3254, 3455]. **Disjoint** [273, 341, 715, 898, 971, 1064, 1327, 1731, 1907, 2346, 3114, 3206, 3229, 3372]. **disjunctive** [2053]. **Disparity** [256]. **Dispelling** [2781, 2813]. **displacements** [1434]. **Distance** [3, 22, 150, 211, 308, 316, 363, 369, 468, 482, 515, 657, 721, 746, 748, 772, 809, 837, 844, 882, 884, 887, 903, 911, 925, 1066, 1118, 1264, 1267, 1313, 1348, 1457–1459, 1552, 1588, 1618, 1659, 1769, 1827, 1836, 1969, 1973, 2096, 2103, 2105, 2112, 2113, 2115, 2135, 2141, 2196, 2233, 2258, 2330, 2404, 2424, 2425, 2429, 2453, 2486, 2527, 2598, 2640, 2758, 2778, 2818, 2862, 2984, 3010, 3121, 3134, 3168, 3252, 3328, 3359, 3388]. **Distance-Increasing** [882]. **Distance-Preserving** [369]. **Distance-Regular** [748, 844, 1457–1459, 2113, 2115, 2424, 2425]. **Distance-transitive** [925]. **Distances** [385, 918, 1587, 1929, 2165, 3168]. **Distillation** [649]. **distinct** [341, 1197, 2279]. **distinctness** [1602, 1771]. **distinguisher** [2586, 3284, 3422]. **distinguishers** [1415, 2492, 3393, 3450]. **distinguishing** [2243, 2530]. **Distorting** [1071]. **Distributed** [893, 1511, 3351]. **Distributing** [796]. **Distribution** [99, 132, 222, 247, 282, 331, 363, 428, 538, 685, 691, 765, 1166, 1262, 1323, 1350, 1443, 1517, 1694, 1787, 1807, 1861, 1915, 1954, 2056, 2176, 2395, 2446, 2641, 2792, 2828, 3178, 3331, 3371, 3394]. **Distributions** [219, 427, 515, 721, 764, 938, 1339, 1366, 1672, 1730, 2216, 2640, 2698, 2928, 2989].

**disturbance** [1318]. **Divisibility** [1428, 1494, 2222]. **Divisible** [78, 85, 194, 235, 255, 356, 384, 440, 580, 587, 743, 931, 937, 964, 1040, 1099, 1380, 1621, 1648, 1738, 1759, 1762, 1952, 2247, 2297, 2400, 2439, 3140, 3184, 3347, 3380, 3459]. **Division** [986, 2558]. **divisor** [2550, 2793]. **Divisors** [529]. **DLP** [2010]. **DNA** [1991, 2257, 2579, 2863, 3282, 3437]. **Do** [1427, 1458, 2526]. **Dobbertin** [1074]. **does** [1933]. **Dom** [745]. **domain** [1726, 2381]. **domain-preserving** [2381]. **domains** [1985]. **Doob** [1978, 2411]. **Double** [253, 259, 292, 306, 580, 589, 623, 761, 822, 1655, 2089, 2202, 2245, 2828]. **Double-Error-Correcting** [623]. **Doubly** [17, 141, 191, 581, 611, 833, 1266, 1320, 1673, 1691, 1731, 1745, 1755, 1848, 1937, 2133, 2566, 2656, 3147]. **Doubly-Even** [141, 191, 833, 1731]. **doubly-shortened** [1266]. **Dowling** [2282]. **Doyen** [2888]. **dp** [3401]. **DR** [1892]. **DRBG** [3233]. **dropbox** [2312]. **dropout** [2699]. **DS** [651]. **DS-CDMA** [651]. **DSA** [2448]. **duadic** [3072]. **Dual** [83, 89, 142, 209, 253, 259, 271, 306, 308, 415, 500, 523, 526, 527, 535, 551, 574, 617, 618, 657, 696, 703, 727, 829, 833, 839, 893, 919, 929, 942, 943, 964, 1001, 1040, 1051, 1132, 1155, 1159, 1255, 1274, 1291, 1355, 1370, 1371, 1381, 1389, 1411, 1412, 1419, 1433, 1438, 1549, 1552, 1601, 1666, 1673, 1691, 1731, 1745, 1755, 1770, 1783, 1806, 1848, 1938, 1941, 1944, 1961, 1964, 2000, 2142, 2234, 2245, 2291, 2343, 2386, 2445, 2540, 2593, 2596, 2668, 2676, 2691, 2717, 2753, 2757, 2763, 2825, 2838, 2927, 2931, 2972, 3110, 3162, 3201, 3210, 3236]. **dual** [3, 24, 1007, 1060, 1065, 1120, 1250, 1402, 1436, 1496, 1523, 1560, 1582, 1742, 1764, 1777, 1805, 1937, 1994, 2019, 2071, 2100, 2109, 2264, 2307, 2358, 2429, 2480, 2493, 2560, 2659, 2683, 2897, 2902, 2950, 2955, 2960, 2980, 3006, 3076, 3086, 3150, 3234, 3241]. **dual-bent** [2897]. **dual-containing** [2429]. **Duality** [1203, 1396, 1419, 1598, 1656, 1983, 2287, 2517, 2524, 2591]. **dualization** [1489]. **Duals** [92, 515, 1789, 2018, 2182, 2288, 2599, 2901, 2923, 2993, 3170, 3343, 3444]. **duplication** [3206, 3431]. **duplication-correcting** [3431]. **duplication-free** [3206]. **Dynamic** [762, 950, 957, 2845, 2930, 3366]. **dynamical** [1403]. **Dynamics** [3126].

**EA** [1296, 1492]. **EA-equivalence** [1296]. **each** [757, 1252]. **EAQMDS** [2716]. **Eastman** [639, 843, 2442, 2511]. **ECDSA** [766, 859, 3056]. **eCK** [1757]. **Eckardt** [2886]. **Ed** [380]. **Edge** [1086, 1779]. **edition** [2857]. **Editor** [2107, 2200]. **Editorial** [1, 378, 405, 429, 1074, 1301, 1485, 1531, 1576, 1637, 1708, 1876, 1902, 1957, 2039, 2601, 2827, 3042, 3095]. **edits** [3167]. **Edward** [379]. **Effective** [1935]. **Efficiency** [503, 1151, 2275, 2470, 2937]. **Efficient** [359, 435, 614, 672, 932, 953, 1034, 1091, 1124, 1142, 1200, 1207, 1216, 1413, 1743, 1827, 1939, 1982, 2145, 2340, 2395, 2472, 2528, 2697, 2727, 2765, 2824, 2909, 2939, 2987, 3046, 3156, 3166, 3169, 3205, 3243, 3274, 3351, 3370]. **efficiently** [1750]. **Egalitarian** [2726]. **EGFN** [2028]. **Eggs** [2956]. **Egyptologist** [155]. **Eigenbasis** [757]. **Eigenspaces** [390]. **Eigenvalue** [751, 2113]. **Eigenvalues** [728, 748, 1462, 1478, 2120, 2124, 2879]. **eight** [1314, 2537, 2818]. **Eisenstein** [1758, 2849]. **elation** [3174]. **elations** [921]. **element** [1089]. **Elements** [95, 524, 590, 640, 739, 801, 831, 932, 1150, 1488, 1718, 1933, 1976, 2002, 2804, 2896, 3038]. **Elephant** [2684]. **eleven** [1460]. **Elliptic** [314, 397, 434, 436, 521, 545, 660, 765, 781, 810, 846, 873, 997, 1024, 1087, 1197, 1282, 1422, 1518, 1706, 1867, 1904, 1919, 2020, 2050, 2099, 2236, 2305, 2325, 2500, 2590, 2664, 2774, 3043, 3230, 3258]. **eluded** [1890]. **Elusive** [2674]. **embeddable** [2157]. **Embedded** [696, 962, 1075, 2931]. **Embedding** [243, 403, 425, 944, 1042, 1044, 1221, 1435, 1503, 2537, 3405]. **Embeddings** [387, 922,

931, 1467, 1550, 1768, 1816, 2359, 2504]. **emission** [2158, 2532]. **emphasis** [1176]. **empty** [1885]. **enciphering** [2702]. **Enclosings** [1232]. **Encoding** [596, 1800, 2197, 2703, 3050, 3265]. **encodings** [2180, 2251, 2590]. **encrypt** [1891, 2310]. **encrypted** [1864, 2319]. **Encryption** [282, 285, 331, 796, 836, 1090, 1091, 1166, 1207, 1295, 1299, 1519, 1622, 1625, 1729, 1739, 1901, 1942, 1975, 1979, 2000, 2017, 2136, 2145, 2177, 2180, 2204, 2210, 2251, 2303, 2310–2312, 2340, 2366, 2417, 2423, 2470, 2475, 2501, 2570, 2615, 2665, 2725, 2727, 2736, 2752, 2765, 2806, 2815, 2816, 2873, 2899, 2937, 2945, 2952, 3005, 3019, 3029, 3074, 3145, 3154, 3163, 3223, 3257, 3357, 3365, 3403]. **encryptions** [3085]. **endomorphism** [2236]. **endowed** [2436]. **energies** [2607]. **enforcing** [2899]. **Enhanced** [1858]. **enlargement** [2597]. **ensemble** [3280]. **Entanglement** [1870, 2181, 2264, 2657, 2734, 3011, 3129, 3444]. **Entanglement-assisted** [1870, 2181, 2264, 2657, 2734, 3011, 3129, 3444]. **Entry** [1966]. **Entry-faithful** [1966]. **Enumerating** [1161, 2557]. **Enumeration** [225, 327, 574, 593, 702, 1230, 1329, 1421, 1810, 1881, 2445, 2980, 3086]. **enumerative** [2287]. **Enumerator** [362, 658, 1934, 2006, 2220, 2377, 2889, 3407]. **Enumerators** [259, 407, 414, 764, 1613, 1839, 1987, 2015, 2068, 2075, 2676, 2972, 3122]. **ephemeral** [1757]. **ephemeral-key** [1757]. **Epimorphisms** [463]. **Equal** [547, 572, 2120, 3206]. **equal-length** [3206]. **equality** [2725]. **Equation** [171, 263, 442]. **Equations** [703, 1078, 1085, 1324, 1505, 1668, 1720, 1956, 2150, 2286, 3397]. **equi** [1011, 1847, 2391]. **equi-difference** [1011, 1847, 2391]. **Equiangular** [1977, 2400, 2708]. **Equidistant** [1199, 2844, 3379]. **Equilateral** [466]. **Equiorthogonal** [299]. **equipped** [3271]. **equitable** [1008, 1144, 1748, 1857]. **Equivalence** [58, 368, 1086, 1122, 1279, 1296, 1305, 1362, 1379, 1418, 1492, 1493, 1495, 1516, 2021, 2172, 2211, 2431, 2491, 2527, 2582, 2688, 2760, 2793, 2854, 2925, 3112, 3120, 3165, 3281, 3292, 3311, 3392, 3416]. **Equivalences** [2155]. **equivalency** [2550]. **Equivalent** [225, 650, 2473, 2558, 3325, 3412]. **Erasure** [1082, 1725, 1726, 2398, 3280, 3413]. **erasures** [1772, 2714]. **Erdos** [1476, 1642, 1658, 1819, 2345, 2878]. **Errata** [1003]. **Erratum** [134, 333, 1293, 1634, 1707, 1745, 1746, 1760]. **Error** [88, 246, 363, 524, 619, 623, 678, 800, 903, 912, 941, 949, 1005, 1058, 1077, 1082, 1090, 1182, 1298, 1320, 1394, 1451, 1620, 1659, 1694, 1712, 1725, 1726, 1746, 1888, 2129, 2158, 2181, 2532, 2594, 2675, 3081, 3129, 3139, 3177, 3274, 3280, 3420, 3444]. **error-block** [1005]. **Error-Correcting** [524, 619, 1620, 1712, 1746, 2129, 2675, 3081, 3129, 3177, 3274, 3420, 3444]. **error-erasure** [1725]. **errors** [1184, 1712, 1746, 1772, 2355, 3206]. **Escrow** [549]. **essay** [1436]. **Establishing** [1151]. **Establishment** [154]. **eSTARK** [3240]. **estimate** [2405]. **Estimates** [483, 1302, 2932, 3112, 3139]. **estimating** [1352]. **Estimation** [312, 3302]. **Ethereum** [3169]. **ETRU** [1758]. **Euclidean** [2313, 2379]. **Euclidian** [503]. **Eurocrypt'98** [445]. **evaluating** [104]. **Evaluation** [927, 973, 1183, 1504, 1592, 1679, 1845, 1891, 1989, 2086, 2632, 2683, 2746, 3060, 3103, 3153, 3434]. **evaluators** [2765]. **Even** [141, 145, 191, 205, 209, 253, 415, 523, 633, 642, 697, 829, 833, 869, 879, 884, 1221, 1309, 1411, 1507, 1537, 1551, 1673, 1683, 1691, 1731, 1745, 1848, 1937, 1943, 1955, 1990, 2012, 2445, 2618, 2661, 2750, 3073, 3086, 3291]. **even-Mansour-based** [3073]. **Every** [491, 1098, 1455, 1468]. **Evolving** [3453]. **Exact** [648, 1339, 1522, 1692, 1720]. **exactly** [2175]. **example** [98]. **examples** [1639]. **exceeding** [3417]. **Exceptional** [470, 1928, 3002, 3266, 3399]. **exceptionality**

[3032]. **excess** [1463]. **Exchange** [163, 1521, 1853, 2151, 2152, 2203, 2471, 2789, 3218, 3246]. **exchanges** [33]. **Executing** [859]. **exist** [1458, 2430, 2526, 2858, 3326]. **Existence** [45, 60, 142, 191, 227, 244, 254, 291, 317, 320, 333, 342, 536, 541, 572, 581, 595, 722, 780, 785, 811, 863, 895, 901, 994, 1013, 1049, 1055, 1105, 1133, 1181, 1218, 1278, 1338, 1354, 1364, 1370, 1373, 1520, 1541, 1553, 1569, 1644, 1662, 1680, 1892, 1936, 2002, 2347, 2349, 2385, 2392, 2487, 2614, 2748, 2767, 2780, 2859, 3162, 3227, 3229, 3335, 3376]. **Exists** [491, 1159, 2126]. **expander** [2505]. **expansion** [1091, 1478]. **expansions** [1290, 1350]. **Expected** [1217]. **experimental** [1122, 2713]. **Experiments** [173, 188]. **expiration** [1884]. **explication** [53]. **Explicit** [37, 143, 928, 1020, 1405, 1875, 2081, 2314, 2472, 2997, 3236, 3327]. **Exploiting** [2215, 3099, 3284]. **exponent** [108, 1599, 1715, 1791, 1804, 3070]. **Exponential** [20, 1494, 2415]. **Exponentially** [851, 1222]. **Exponentiation** [162, 303, 511, 878, 932, 1235, 2774]. **exponents** [2282, 2580]. **expressive** [2736]. **Extendability** [768, 1958, 1965]. **extendable** [2468, 2910, 3209]. **Extended** [383, 503, 1264, 1271, 1589, 1783, 1920, 1941, 2000, 2003, 2314, 2315, 2351, 2630, 2721, 2814, 2860, 2889, 3030, 3122, 3148, 3263, 3316, 3419]. **Extending** [1773, 1970, 2104, 2647, 3240]. **Extension** [184, 391, 408, 1163, 1336, 1378, 1507, 1578, 1812, 2043, 2195, 2207, 2379, 2499, 2681, 2836]. **Extensions** [213, 666, 1488, 1776, 1809, 1879, 1942, 1995, 2002, 2187, 2269, 2557, 2613, 2787]. **extensive** [2824]. **exterior** [3262]. **External** [750, 898, 1922, 2138, 2238, 2328, 2584, 2953, 3117, 3225, 3227, 3372]. **extractable** [2782]. **extraction** [2331, 3166]. **extractor** [2308, 2666]. **Extractors** [1087, 2789, 2930]. **extraspecial** [1804]. **Extremal** [141, 142, 191, 253, 259, 306, 307, 375, 415, 527, 551, 617, 618, 656, 727, 829, 833, 943, 1132, 1291, 1402, 1449, 1457, 1582, 1644, 1673, 1691, 1731, 1734, 1745, 1783, 1805, 1848, 1933, 1937, 2019, 2100, 2234, 2972, 3016, 3109, 3160]. **extreme** [1026]. **Extremely** [2940, 3035].

**F** [379]. **Faber** [2878]. **faces** [3014]. **factor** [1440, 2994]. **Factoring** [431, 1091, 1628, 1853]. **factorisations** [1033]. **Factorization** [42, 1382, 1875, 2399, 3305]. **factorizations** [2081, 2364]. **Factorized** [178]. **Factors** [111, 123, 403, 549, 1405, 1564, 3329]. **faithful** [1966, 2061]. **False** [1273, 1756, 1823]. **Families** [115, 252, 294, 342, 346, 471, 546, 694, 706, 712, 898, 928, 992, 1020, 1147, 1154, 1186, 1197, 1233, 1326, 1528, 1537, 1575, 1588, 1592, 1615, 1685, 1703, 1738, 1790, 1801, 1880, 1907, 2060, 2063, 2138, 2212, 2213, 2225, 2238, 2320, 2328, 2346, 2394, 2447, 2505, 2573, 2584, 2659, 2741, 2744, 2771, 2997, 2998, 3023, 3072, 3117, 3144, 3190, 3227, 3229, 3268, 3273, 3297, 3343, 3354, 3359, 3372]. **Family** [178, 251, 255, 343, 383, 404, 509, 612, 647, 773, 814, 1093, 1115, 1186, 1231, 1307, 1331, 1506, 1574, 1615, 1676, 1706, 1802, 1807, 1931, 1945, 2068, 2208, 2309, 2397, 2487, 2535, 2705, 2716, 2802, 2969, 3096, 3298, 3301, 3388, 3416, 3429]. **Fano** [1208, 2190, 2348, 2803]. **Farfalle** [3082]. **Fast** [162, 165, 760, 911, 1272, 1490, 1581, 1843, 2226, 2569, 2736, 3031, 3091, 3153, 3185, 3223, 3258, 3402, 3416]. **faster** [1837, 1883, 2610]. **Fault** [1393, 3345]. **Faults** [781]. **Faure** [2254]. **FCSR** [726, 1126, 1168, 2231]. **FCSRs** [2226]. **FE** [2697, 3027, 3221]. **Feedback** [682, 1287, 1581, 1740, 2041, 2070, 2509]. **feet** [3292]. **Feistel** [876, 1283, 1303, 1491, 2003, 2461, 2543, 2638, 2685, 3073, 3082, 3171, 3450]. **Feng** [1272, 1830, 2269, 2277, 2330]. **Fermat** [1524]. **Ferrers** [2339, 3065]. **Few** [1445, 1538, 1735, 1818, 2106, 2205, 2332, 2546, 2706, 2879, 2993, 3391]. **FHE** [1845, 2965]. **fiber** [2984]. **Fibonacci** [2491]. **Fibrations**

[756]. **fibre** [1604]. **Field** [400, 640, 791, 801, 960, 1150, 1573, 1684, 1812, 1910, 1997, 2014, 2191, 2477, 2597, 2681, 2773, 3092, 3258, 3419]. **Fields** [4, 37, 55, 95, 143, 144, 163, 213, 215, 277, 324, 408, 476, 493, 590, 625, 686, 736, 739, 928, 930, 932, 1124, 1155, 1336, 1363, 1365, 1371, 1428, 1446, 1494, 1526, 1530, 1582, 1604, 1612, 1677, 1718, 1761, 1775, 1776, 1820, 1822, 1836, 1863, 1905, 1908, 2002, 2083, 2091, 2102, 2123, 2139, 2163, 2276, 2360, 2365, 2409, 2494, 2495, 2529, 2540, 2575, 2603, 2629, 2698, 2714, 2741, 2772, 2804, 2811, 2822, 2837, 2838, 2841, 2858, 2896, 2928, 2995, 3038, 3040, 3051, 3126, 3132, 3164, 3215, 3254, 3256, 3285, 3291, 3307, 3327, 3331, 3346, 3364, 3398, 3416, 3425, 3462]. **fields** [1078, 1178, 1276, 1405, 1564, 1690, 1764, 1792, 1797, 1839, 1886, 1956, 1976, 2032, 2081, 2238, 2673, 2738, 2748, 2750, 2821, 2905, 3084, 3318, 3457, 3461]. **Fields*** [850]. **Figueroa** [2961]. **fill** [2744]. **filter** [1858, 2396]. **filtered** [2725]. **Filtering** [330]. **Finding** [968, 1014, 1399, 1750, 1883, 2552, 3230]. **fine** [2017]. **fine-grained** [2017]. **Fingerprinting** [784, 1023, 1054, 1173, 2074, 2217, 2942]. **Finite** [37, 143, 213, 215, 365, 367, 387, 400, 417, 476, 525, 555, 588, 625, 626, 681, 686, 708, 728, 736, 739, 755, 801, 850, 852, 909, 955, 1003, 1038, 1043, 1103, 1150, 1185, 1198, 1247, 1254, 1265, 1370, 1371, 1399, 1446, 1455, 1531, 1548, 1592, 1601, 1604, 1617, 1637, 1642, 1663, 1677, 1761, 1776, 1794, 1820, 1880, 1910, 1957, 1981, 1997, 2061, 2083, 2163, 2239, 2290, 2296, 2317, 2344, 2360, 2419, 2526, 2529, 2540, 2568, 2603, 2698, 2804, 2811, 2822, 2837, 2838, 2841, 2858, 2875, 2896, 2996, 3051, 3126, 3164, 3256, 3285, 3290, 3291, 3327, 3333, 3398, 3445, 3462]. **finite** [24, 55, 95, 97, 301, 928, 932, 982, 999, 1078, 1124, 1156, 1181, 1211, 1217, 1229, 1276, 1363, 1365, 1381, 1405, 1421, 1428, 1444, 1492, 1530, 1564, 1612, 1690, 1764, 1792, 1836, 1850, 1854, 1863, 1886, 1905, 1908, 1927, 1956, 1976, 2032, 2081, 2085, 2091, 2123, 2134, 2139, 2148, 2238, 2365, 2409, 2494, 2495, 2520, 2521, 2629, 2650, 2673, 2710, 2738, 2741, 2748, 2750, 2755, 2772, 2821, 2905, 2921, 2928, 2940, 2946, 2956, 2995, 3007, 3038, 3084, 3092, 3193, 3296, 3299, 3308, 3318, 3331, 3334, 3364, 3425, 3432, 3457, 3459, 3461]. **First** [165, 1083, 2744, 3122, 3181]. **first-order** [3122, 3181]. **Five** [220, 244, 311, 350, 488, 640, 676, 1094, 1385, 1859, 1921, 1954, 2018, 2213, 2537, 2741, 2755, 2807]. **five-weight** [1954, 2213]. **Fix** [122]. **Fix-Free** [122]. **Fixed** [551, 1182, 1867, 2680, 3001, 3178, 3298]. **fixed-length** [3178]. **fixes** [2867]. **fixing** [1215]. **Flag** [19, 387, 422, 457, 674, 981, 1237, 1261, 1953, 2034, 2273, 2283, 2463, 2533, 2670, 2677, 2724, 2745, 2779, 2922, 3083, 3189, 3377, 3433]. **Flag-Transitive** [422, 457, 981, 1237, 1261, 1953, 2034, 2273, 2283, 2463, 2533, 2670, 2677, 2779, 2922, 3083, 3189, 3433]. **Flags** [715, 1460, 2192, 2289, 2596]. **flash** [1584]. **Flat** [1000, 1096, 3119]. **Flats** [750, 792]. **Flaw** [902]. **FlexAEAD** [2786]. **flexible** [2765, 2908]. **Flock** [661, 1512]. **Flocks** [206, 239, 410, 683]. **Flying** [156]. **Flystel** [3384]. **fold** [1232, 1377, 1409, 1732, 1921, 2420]. **Folded** [644, 3098]. **Forbidden** [628, 751, 812, 1154, 1482, 2817]. **Forcing** [200]. **Foreword** [153, 1826, 2589]. **Foreword-Special** [2589]. **forgery** [1851]. **ForkSKINNY** [3400]. **Form** [39, 268, 298, 2302, 2325, 2554, 2853, 2941, 3200, 3247, 3279, 3397]. **Formal** [157, 2781, 2813, 3145]. **Formally** [89, 253, 415, 500, 523, 829, 1132, 1355, 1666, 2291, 3006, 3241]. **Forms** [140, 402, 1107, 1319, 1350, 1433, 1549, 1899, 2668, 2671, 3392]. **formula** [1522, 1523]. **formulae** [1536]. **Formulas** [388]. **Forrelation** [3113]. **forward** [1443, 1757, 1787, 3218]. **Four** [5, 524, 554, 572, 587, 722, 738, 743, 800, 915, 1052, 1300, 1357, 1380, 1488, 1565, 1730, 1759,

1903, 1936, 2230, 2233, 2307, 2496, 2504, 2776, 2809, 3241, 3331]. **Four-Error-Correcting** [800]. **Four-Weight** [554]. **Fourier** [1632, 1711, 1824, 2061, 2290]. **Fourier-reflexive** [1824]. **Fourth** [536, 3059, 3394]. **fourth-order** [3394]. **Fractal** [12]. **fraction** [2509]. **Fractional** [1359, 1683, 3160, 3285, 3462]. **Frame** [2320, 2385]. **frame-derived** [2385]. **frameproof** [950, 957, 1685, 1877, 1974, 2217, 2338, 2574, 3421]. **Frames** [426, 580, 995, 1671, 2400, 2708]. **framework** [1075, 2252, 2414, 2548, 2669, 2801, 2869, 3024, 3373, 3393, 3402, 3409]. **Frameworks** [479]. **Frank** [1637]. **Franklin** [1106]. **Free** [95, 122, 174, 456, 599, 694, 712, 714, 754, 1227, 1488, 2052, 2054, 2296, 2324, 2526, 2530, 2555, 3061, 3079, 3206, 3296, 3364]. **French** [3370]. **Frequency** [299, 924, 1199, 1334, 1367, 1566, 1665, 1700, 1798, 2082, 2137, 2156, 2334, 2402, 2403, 2645, 3328]. **frequency-hopping** [924, 1566, 1665, 2082]. **friendly** [1526, 3031, 3302, 3447]. **Frobenius** [448, 955, 1003, 1188, 1265, 1350, 1617, 1794, 2296, 2481, 2526, 2921]. **Fu** [961]. **Full** [841, 1721, 1743, 1767, 2280, 2365, 2474, 2529, 2648, 2712, 2824, 2906, 2999, 3039, 3218, 3223]. **full-rank** [3039]. **full-time** [2712]. **fullrank** [2023]. **Fully** [696, 1342, 1610, 2845, 3348]. **Function** [12, 163, 324, 493, 501, 509, 545, 547, 930, 1178, 1192, 1246, 1326, 1572, 1596, 1696, 1866, 1895, 2023, 2102, 2488, 2597, 2771, 2932, 2960, 3092, 3132, 3215, 3324, 3338, 3346, 3353]. **Functional** [1251, 1608, 2136, 2180, 2462, 2665, 2937, 3029, 3250]. **functionality** [3271]. **Functions** [69, 130, 148, 161, 237, 279, 284, 321, 340, 365, 396, 448, 567, 579, 613, 676, 731, 739, 788, 792, 805, 828, 849, 850, 874, 876, 889–891, 1019, 1075, 1094, 1098, 1115, 1171, 1172, 1205, 1255, 1277, 1305, 1306, 1362, 1388, 1418, 1442, 1500, 1501, 1516, 1627, 1710, 1722, 1809, 1834, 1858, 1903, 1926, 1930, 2056, 2061, 2065, 2161, 2211, 2212, 2237, 2274, 2290, 2295, 2342, 2390, 2394, 2447, 2529, 2542, 2582, 2619, 2620, 2639, 2688, 2723, 2730, 2760, 2787, 2817, 2862, 2867, 2894, 2910, 2935, 2993, 3002, 3032, 3097, 3138, 3197, 3253, 3266, 3323]. **functions** [1008, 1070, 1080, 1081, 1105, 1250, 1272, 1314, 1319, 1322, 1325, 1412, 1419, 1427, 1502, 1509, 1554, 1616, 1656, 1682, 1702, 1727, 1782, 1814, 1822, 1839, 1843, 1850, 1856, 1865, 1909, 2011, 2067, 2106, 2143, 2155, 2165, 2170, 2261, 2267, 2269, 2278, 2314, 2336, 2387, 2405, 2408, 2418, 2422, 2434, 2437, 2455, 2478, 2493, 2496, 2505, 2506, 2510, 2514, 2522, 2546, 2548, 2549, 2569, 2602, 2610, 2618, 2622, 2662, 2682, 2697, 2706, 2728, 2738, 2747, 2821, 2830, 2869, 2897, 2905, 2923, 2934, 2946, 2960, 2963, 2967, 2997, 3017, 3030, 3064, 3076, 3101, 3119, 3196, 3200, 3224, 3263, 3270, 3301, 3316, 3317, 3351, 3368, 3397, 3457]. **functions** [113, 1792, 1893, 2022, 2518, 2556, 2673, 2742, 2768]. **fundamental** [183]. **Further** [72, 1067, 1172, 1233, 1353, 1427, 1520, 1771, 1897, 1959, 2269, 2455, 2458, 2491, 2625, 2842, 2923, 2960, 3053, 3191, 3353, 3461]. **fusion** [1477]. **Future** [432]. **Fuzzy** [848, 2308, 2666, 3166]. **FWT** [3245].

**Gabidulin** [137, 1490, 1716, 1725, 1726, 2195, 2196, 2254, 2276, 2284, 2285, 2785]. **Gabidulin-based** [2195]. **Gács** [1241]. **Gain** [326]. **Galbraith** [2363, 2630]. **Galois** [16, 185, 236, 319, 569, 633, 874, 936, 1001, 1240, 1375, 1376, 1507, 1738, 1914, 1985, 2002, 2142, 2491, 2495, 2636, 2756, 2828, 2837, 2980, 3086, 3123, 3161, 3267, 3401, 3410]. **games** [1017, 2650]. **Gap** [427, 1639, 3265]. **gapless** [2852]. **Gaps** [770, 1976, 3132, 3346]. **garbled** [3375]. **Garcia** [3127]. **Gauss** [932, 1372, 1565, 2086, 2224]. **Gaussian** [1426, 2452, 2849, 2971]. **GBRDs** [1364, 1563]. **GDDs** [1327, 1420]. **GDRPs** [1102]. **Geil** [1586]. **General** [270, 354, 416, 560, 580, 610, 779, 783, 787, 893, 1214, 1360, 1413, 1631, 1737, 1780, 1901, 1981, 2051, 2456, 2548, 2669, 2687, 2695, 2801, 2815, 2869, 2969, 3009, 3024, 3351, 3365, 3409, 3451]. **Generalised**

[345, 900, 1139, 1723, 2013, 2812, 2966, 3082]. **generalising** [2139]. **Generalization** [58, 207, 561, 853, 1156, 1175, 1343, 1497, 1499, 1583, 2016, 2059, 2118, 2146, 2212, 2240, 2431, 2791, 2925, 3332, 3430]. **Generalizations** [516, 1179, 1351, 2348, 3322]. **Generalized** [29, 60, 254, 263, 274, 319, 456, 463, 517, 531, 565, 582, 645, 655, 666, 741, 785, 821, 827, 866, 875, 942, 951, 996, 1008, 1028, 1043, 1044, 1057, 1072, 1100, 1105, 1110, 1116, 1144, 1174, 1179, 1202, 1234, 1280, 1329, 1341, 1361, 1378, 1392, 1491, 1512, 1525, 1550, 1557, 1558, 1565, 1566, 1707, 1709, 1784, 1811, 1814, 1831, 1948, 1979, 2027, 2067, 2143, 2169, 2170, 2276, 2328, 2336, 2374, 2414, 2417, 2444, 2454, 2515, 2522, 2539, 2547, 2561, 2576, 2619, 2648, 2694, 2710, 2717, 2788, 2912, 2914, 2929, 2996, 3056, 3059, 3071, 3120, 3174, 3203, 3215, 3267, 3286, 3397, 3400, 3423, 3440]. **generalized** [24, 28, 948, 952, 1436, 1448, 1554, 1569, 1624, 1655, 1661, 1750, 1943, 2259, 2415, 2685, 2805, 2861, 2864, 3155, 3181, 3188, 3353, 3383, 3387, 3429]. **generalizing** [2991]. **generated** [75, 910, 1065, 1171, 1403, 2894, 2903]. **Generating** [706, 846, 1006, 1465, 1526]. **Generation** [225, 309, 327, 1318, 1721, 2815, 3370]. **Generator** [362, 499, 508, 548, 670, 997, 1108, 1203, 1281, 1329, 1670, 1682, 1784, 1858, 1973, 2236, 2286, 2550, 3028]. **Generators** [684, 765, 767, 870, 881, 1036, 1142, 1216, 1444, 1530, 1811, 2538, 2793, 2968, 3001]. **Generic** [766, 945, 1184, 1923, 2063, 2090, 2514, 2690, 2752, 2756, 2987, 3029, 3074, 3145, 3154, 3458]. **genericity** [2196]. **Gentry** [1845]. **genus** [1425, 1526, 1899, 2064]. **Geometric** [84, 92, 148, 193, 208, 262, 388, 556, 586, 650, 669, 968, 1222, 1277, 1388, 1448, 1454, 1456, 1584, 1753, 1879, 1996, 2033, 2252, 2354, 2386, 2459, 2583, 2614, 2773, 2871, 2961, 3088, 3187]. **Geometrical** [463, 2871, 2882]. **Geometries** [16, 23, 58, 75, 223, 233, 387, 443, 462, 626, 641, 696, 962, 981, 1038, 1039, 1048, 1211, 1240, 1437, 1489, 1531, 1637, 1880, 1914, 1957, 2249, 2344, 2388, 3290]. **Geometrisable** [300, 451]. **Geometry** [52, 170, 183, 301, 700, 821, 973, 978, 1029, 1204, 1429, 1593, 1693, 1716, 2330, 2462, 2474, 2710, 2805, 2875, 3201, 3215, 3295, 3299, 3362, 3418]. **Germain** [1822]. **GF** [362, 659, 1198, 1270, 1452]. **GFS** [2028]. **GGS** [2300]. **GIFT** [2539, 3315]. **GIFT-64** [3315]. **Gilbert** [2343, 2586]. **girth** [1257, 2484]. **girth-8** [2484]. **Giulietti** [2386]. **Giuseppe** [216]. **Given** [360, 1447, 1475, 2607, 3159]. **giving** [3051]. **GK** [2184]. **Gleason** [1174, 1419]. **Gleason-type** [1419]. **global** [1178]. **GLS** [1422]. **gluing** [3202]. **GLV** [1422, 3447]. **GMW** [238, 3188]. **GOB** [907]. **Godsil** [2122]. **Goethals** [79, 219, 401, 622, 1323]. **Golay** [1309, 1310, 2172, 2335, 3018]. **Gold** [1145, 1341, 2314, 2910, 3399]. **Goldreich** [3028]. **Golomb** [2903]. **Gong** [2652, 3188]. **Good** [167, 616, 821, 1509, 1789, 1843, 1844, 1874, 2181, 2438, 2692, 2707, 2796, 2799, 2807, 2864, 3222, 3275]. **Goppa** [211, 312, 441, 482, 532, 556, 770, 799, 1183, 1589, 2044, 2860, 2950, 3010, 3066]. **Gorenstein** [3224]. **Gowers** [2237]. **GPT** [1062, 1594]. **Graham** [1568]. **Grain** [1801, 2060, 2651, 2762, 3369]. **GRAIN-128-AEAD** [3369]. **Grain-128a** [2762]. **Grain-like** [2060, 2651]. **grained** [2017]. **Gram** [2449]. **Graph** [116, 123, 300, 403, 451, 747, 752, 1063, 1190, 1257, 1259, 1264, 1308, 1459–1461, 1510, 1515, 2007, 2115, 2130, 2165, 2185, 2324, 2424, 2425, 2757, 2847, 3069, 3140, 3347, 3380, 3432]. **Graph-theoretic** [2007]. **graphical** [3016]. **Graphs** [11, 22, 56, 113, 124, 140, 179, 180, 292, 395, 459, 464, 465, 471, 589, 710, 746, 748, 751, 754, 885, 916, 983, 1033, 1048, 1169, 1227, 1368, 1440, 1457, 1458, 1462, 1472, 1475, 1478, 1529, 1542, 1562, 1579, 1580, 1588, 1646, 1648, 1689, 1779, 1921, 1930, 1946, 1962, 1978, 1995, 2008, 2035, 2070, 2109, 2112, 2113, 2120, 2122, 2127, 2169, 2185, 2362, 2364, 2411, 2440, 2443, 2497,

2505, 2587, 2631, 2671, 2674, 2780, 2849, 2879, 2893, 2917, 2948, 3016, 3054, 3061, 3140, 3160, 3194, 3239, 3264, 3336, 3347, 3380, 3405, 3449]. **Grassl** [2966]. **Grassman** [140]. **Grassmann** [1221, 1961, 2122, 2352]. **Grassmannian** [717, 750, 909, 1345, 1716, 2218, 2735]. **Gravity** [184]. **Gray** [1676, 2101, 2116, 2819, 2829]. **Greater** [547]. **Greedy** [200, 204, 668, 2432, 2637]. **Greismer** [227]. **Grey** [20]. **Grey-Rankin** [20]. **grid** [1158, 3069]. **Grids** [761, 822, 3259]. **Griesmer** [41, 276, 558, 723, 797, 993, 1088, 1127, 1185, 1354, 1808, 1965, 2327, 2354, 2614, 2784, 3285, 3462]. **GRM** [427]. **Gröbner** [295, 3079]. **Gröbner-free** [3079]. **Groebner** [1591]. **Grøstl** [1596]. **Grøstl-0** [1596]. **Groth** [2310]. **Group** [19, 47, 78, 194, 232, 235, 310, 332, 356, 491, 526, 543, 580, 587, 624, 728, 732, 743, 790, 813, 824, 862, 866, 871, 879, 931, 964, 978, 1096, 1112, 1149, 1171, 1215, 1218, 1380, 1401, 1519, 1542, 1543, 1585, 1621, 1645, 1759, 1762, 1766, 1813, 1835, 1869, 1898, 1933, 2000, 2130, 2161, 2190, 2247, 2288, 2291, 2297, 2318, 2322, 2345, 2395, 2398, 2400, 2439, 2459, 2487, 2504, 2561, 2568, 2667, 2691, 2695, 2844, 2845, 2921, 2930, 2933, 2987, 2996, 3029, 3150, 3237, 3269, 3271, 3321, 3333, 3350]. **group-based** [2933]. **Group-Divisible** [587]. **group-invariant** [2487]. **Group-Type** [587]. **Groups** [8, 18, 27, 79, 97, 114, 131, 166, 177, 178, 189, 195, 203, 234, 266, 272, 310, 344, 377, 404, 408, 456, 469, 490, 504, 533, 583, 609, 677, 692, 695, 704, 741, 766, 780, 824, 864, 923, 1037, 1047, 1143, 1156, 1162, 1166, 1229, 1337, 1370, 1399, 1444, 1492, 1563, 1582, 1631, 1647, 1691, 1697, 1767, 1791, 1804, 1850, 1854, 1952, 1953, 1981, 2061, 2077, 2079, 2140, 2180, 2205, 2235, 2251, 2255, 2273, 2290, 2347, 2376, 2378, 2397, 2409, 2524, 2533, 2635, 2670, 2703, 2755, 2832, 2881, 2922, 2940, 2946, 2992, 3020, 3035, 3282, 3308, 3327, 3340, 3351, 3423, 3438, 3459]. **groups** [1261]. **grows** [1222]. **Growth** [518, 998, 2957]. **GRS** [3081, 3159, 3390]. **Guess** [2982]. **Guess-and-determine** [2982]. **Guessing** [3315]. **Guest** [378, 429, 1876, 2827, 3042]. **gum1** [587]. **Guruswami** [1204, 1723]. **GWhD** [1133].

**H** [1034, 1435, 2131]. **Hadamard** [108, 203, 212, 238, 272, 274, 298, 345, 409, 504, 541, 557, 706, 741, 851, 877, 926, 969, 983, 1084, 1104, 1135, 1145, 1146, 1176, 1234, 1284, 1291, 1392, 1439, 1464, 1585, 1697, 1738, 1947, 2206, 2280, 2335, 2437, 2487, 2648, 2788, 2839, 2927, 2955, 3113, 3120, 3190, 3216, 3219, 3268]. **Haemers** [2124]. **Halevi** [1845]. **half** [1308, 1856]. **half-rate** [1308]. **Hall** [2797]. **Halved** [644]. **halves** [3375]. **Halving** [13, 1518]. **Hamada** [558, 993, 1137, 1456, 2207]. **Hamilton** [1368]. **Hamiltonicity** [1995]. **Hamming** [152, 319, 539, 606, 721, 875, 918, 922, 1057, 1100, 1386, 1529, 1569, 1665, 1700, 1711, 1760, 1783, 1798, 1816, 1831, 1833, 2086, 2111, 2137, 2173, 2437, 2451, 2547, 2592, 2674, 2678, 2698, 2814, 2862, 3122, 3278, 3378]. **Hamming-autocorrelation** [1711]. **Hanani** [1815]. **Hand** [1085]. **Hanfried** [170, 1567]. **Hans** [1074]. **hard** [3015]. **Hardness** [1791, 2679, 3112]. **hardware** [2226]. **Harmonic** [407, 2990, 3122, 3136]. **Harn** [1328]. **Hash** [113, 783, 849, 928, 992, 1020, 1070, 1154, 1246, 1442, 1574, 1575, 1596, 1685, 1880, 1895, 2011, 2225, 2256, 2295, 2488, 2667, 2771, 2852, 3119, 3313]. **hash-based** [2667]. **Hashing** [112, 262, 816, 1297, 2050, 2089, 2774, 3435]. **Hasse** [2055]. **Having** [128, 351, 362, 369, 967, 995, 1007, 1081, 1274, 1340, 1671, 2793, 3094, 3376]. **HC** [1317, 1415]. **HC-128** [1317, 1415]. **Head** [3349]. **Healing** [691]. **Heffter** [1885, 3454]. **Helleseth** [558, 2250, 3353]. **Hellman** [433, 1175, 1273, 1383, 2308, 2336]. **hemisystem** [1139]. **Hemisystems** [1512, 1652, 1802, 2013, 2904]. **herding**

[1442]. **Hermitian** [21, 28, 290, 400, 570, 627, 755, 759, 809, 830, 837, 860, 884, 887, 956, 1041, 1100, 1101, 1107, 1136, 1244, 1251, 1267, 1275, 1453, 1557, 1570, 1578, 1590, 1608, 1652, 1802, 1855, 1964, 2013, 2109, 2141, 2258, 2298, 2313, 2595, 2597, 2643, 2722, 2791, 2904, 2929, 2959, 2972, 3011, 3151, 3159, 3162, 3210, 3401]. **Hermitian-lifted** [2643]. **Heuristic** [1828]. **Hexagon** [709]. **Hexagons** [827]. **HFE** [1551]. **HIBE** [1767, 2727]. **hidden** [1299, 2286, 2500, 3163]. **Hiding** [449, 2180, 3026]. **Hierarchical** [1625, 2000, 2303, 2366, 2624, 2689, 2727, 2949, 3283, 3299]. **Hierarchies** [106, 336, 3344]. **Hierarchy** [724, 2964, 3411]. **Higgledy** [1972]. **Higgledy-piggledy** [1972]. **High** [997, 1150, 1509, 1616, 1843, 1889, 2025, 2199, 2408, 2598, 2804, 2824, 3275]. **high-order** [997]. **High-speed** [1889]. **Higher** [63, 527, 839, 1332, 1425, 2030, 2139, 2421, 2630, 3093]. **higher-dimensional** [63]. **Highly** [25, 891, 1447, 1782, 2744, 3158]. **Hilbert** [3441]. **history** [1905]. **hit** [1334, 1700, 1798, 2137, 2156]. **Hjelmslev** [1489, 1541, 2349]. **HMOLS** [572]. **Hoffman** [3140]. **Høholdt** [3091]. **hole** [995, 1671]. **Holes** [176, 572]. **holey** [1123, 1158, 1762]. **Homage** [170]. **Homogeneous** [199, 465, 579, 731, 1033, 1467, 1550, 1938, 2359]. **homology** [1645, 1650]. **Homomorphic** [1519, 1610, 1887, 1989, 2011, 2268, 2295, 2384, 2711, 2765, 3357, 3402]. **homomorphisms** [1898]. **Honor** [1470, 1637, 1876]. **honoring** [1469]. **Honour** [571, 2589]. **hopping** [924, 1334, 1367, 1566, 1665, 1700, 1798, 2080, 2082, 2137, 2156, 2402, 2403]. **HOPs** [426]. **horizontal** [2193]. **Howell** [2027]. **HQC** [3274]. **Huff** [2325]. **Hughes** [984, 1513]. **hull** [1497, 2843, 3063, 3159, 3269]. **Hulls** [1580, 1603, 2479, 2495, 2835, 3006, 3125, 3161, 3217, 3241, 3310]. **hybrid** [1207]. **hyper** [1319]. **hyper-bent** [1319]. **Hyperbolic** [708, 756, 845, 1254, 1533, 2483]. **hyperboloids** [3075]. **Hyperconics** [438]. **hypercube** [1064, 1484, 2130, 3332]. **Hypercubes** [299, 1546, 1547, 3075, 3090]. **Hypercubic** [623]. **Hyperelliptic** [503, 795, 1897, 1899, 2064, 2299]. **Hypergraph** [402, 1799]. **Hypergraphical** [419]. **hypergraphs** [1476, 2878, 3160]. **hyperoval** [2358]. **Hyperovals** [206, 318, 679, 1249, 1250, 1255, 1453, 1479, 1703, 1755, 1971, 1994, 3300]. **Hyperplane** [19, 512]. **Hyperplanes** [628, 812, 1042, 1065, 1411, 1467, 1550, 1964, 2483, 2523, 3094]. **hypersurfaces** [2811, 3220]. **hypotheses** [3058]. **hypothesis** [1122].

**IBE** [1106, 1939, 2159, 2585, 2630, 2689, 2704, 3149, 3303, 3348]. **IBE/ABE** [3149]. **ID** [1207]. **ID-based** [1207]. **Ideal** [509, 530, 672, 1103, 1152, 1698, 1845, 2132, 2317, 2711, 2949, 3124]. **ideals** [47]. **Idempotent** [1052, 1811, 2056, 2375, 2550]. **Idempotents** [1081, 1398, 2216]. **identical** [3410]. **identifiable** [990, 2074]. **Identification** [607, 1153]. **Identify** [126]. **Identifying** [539, 671, 914, 1140, 1330, 1577, 2271, 2551, 2623]. **identities** [1110, 1824]. **Identity** [622, 1114, 1166, 1443, 1739, 1787, 2000, 2145, 2204, 2303, 2366, 2423, 2727, 2945, 3055]. **Identity-based** [1166, 1443, 1739, 1787, 2145, 2204, 2303, 2366, 2423, 2727, 2945, 3055]. **II** [169, 237, 307, 371, 375, 559, 588, 654, 664, 789, 825, 1310, 1388, 1401, 1455, 1672, 2289, 2439, 3004, 3109, 3136, 3187]. **Im** [3375]. **Image** [98, 505, 2819, 2890, 3092]. **Images** [609, 1360, 1737, 2116, 2244, 2829]. **Imaginary** [663, 1839]. **Imai** [445]. **Immune** [130, 365, 2437]. **Immunity** [889, 1116, 1172, 1271, 1272, 1325, 1516, 1616, 1682, 1843, 1925, 2269, 2618, 3028]. **immunity-resiliency** [3028]. **imperfect** [2666]. **implementations** [3099]. **implemented** [2058]. **Implementing** [1422, 2127]. **implications** [3028]. **implies** [2854]. **Impossibility**

[171, 1190, 1519, 2417, 3166]. **impossible** [1122, 1333, 2047, 2262, 2461, 2476, 2731, 2870, 3107, 3393, 3400]. **impossible-differential** [2047, 2870]. **imprimitive** [1045, 2677, 2888, 3189]. **Improved** [312, 544, 941, 945, 1054, 1097, 1178, 1184, 1299, 1415, 1575, 1661, 1728, 1949, 2028, 2050, 2147, 2210, 2214, 2285, 2338, 2363, 2402, 2403, 2530, 2623, 2720, 2746, 2823, 2838, 2912, 2937, 2968, 3006, 3049, 3118, 3121, 3135, 3153, 3241, 3288, 3315, 3360, 3369, 3450]. **Improvement** [9, 620, 1173, 1830, 2842]. **Improvements** [473, 480, 558, 875, 1185, 3443]. **Improving** [1929, 2037, 2041, 2047, 2104, 3010]. **inactive** [3242]. **Incidence** [49, 54, 147, 228, 233, 402, 417, 518, 555, 680, 1065, 1254, 1437, 1545, 1580, 1663, 2362, 2523, 2718]. **Incomplete** [66, 244, 258, 287, 354, 573, 1995, 2320, 2416, 2464]. **Increasing** [882, 1775]. **Incremental** [2952]. **Indecomposable** [707]. **Independence** [1108, 1131]. **Independent** [101, 190, 279, 1259, 2281, 2437]. **Index** [121, 244, 836, 1859, 2032, 2307, 2377, 2842, 3003]. **Indicator** [3224]. **Indicators** [792]. **indifferentiability** [1070, 1949, 2012, 2720, 3152]. **Indifferentiable** [1926, 2774]. **indistinguishable** [2590]. **Individual** [3068, 3419]. **Indivisible** [1157]. **induced** [1970]. **Inequalities** [7, 40, 730, 1714]. **Inequality** [326]. **inequivalent** [2284, 2511]. **inextendable** [1046]. **Inferring** [997]. **Infinite** [187, 217, 343, 346, 541, 706, 1231, 1676, 1703, 2014, 2213, 2394, 2802, 2997, 3003, 3144, 3273, 3298, 3359, 3416]. **infinitely** [1809]. **infinity** [985, 1592]. **inflection** [1009]. **Information** [146, 257, 430, 649, 1591, 1692, 2038, 2382, 2456, 2604, 2626, 2766, 3166, 3351, 3439]. **Information-set** [3439]. **information-theoretic** [2766, 3166, 3351]. **Inherited** [232]. **inhomogeneous** [2106]. **initial** [2768]. **injections** [1474]. **Inner** [876, 1295, 1619, 1625, 1695, 1901, 2789, 3217]. **Inner-product** [1295, 1901, 2789]. **input** [501, 3026]. **input-size** [3026]. **inputs** [2151, 2152]. **Insecurity** [660]. **inserting** [2912]. **insertions** [1713, 2449, 3135]. **insights** [3070, 3276]. **instance** [3158]. **instances** [3205]. **instantiation** [2665]. **instantiations** [3145, 3458]. **insulation** [2366, 2727]. **Integer** [162, 431, 549, 1164, 1784, 1885, 2379, 2971]. **Integers** [865, 888, 940, 1004, 1758, 2739, 2849, 3146]. **Integral** [2123, 2759, 3285, 3462]. **integrated** [1923]. **integrations** [3459]. **Interactive** [222, 576, 663, 808, 1166, 1443, 1724, 1787, 2275, 2384, 2868, 2939, 3271]. **interconnection** [48]. **interference** [3225]. **Interlacing** [748]. **interleaved** [1578, 1620, 1705, 1725, 2652, 2679, 3185, 3188]. **interleaving** [1874, 2137, 2250]. **Internal** [528, 840, 1596, 3452]. **International** [1576]. **Interpolation** [263, 553, 1678, 1725, 1728, 2336, 3091, 3098]. **Interpolation-based** [3098]. **Intersecting** [585, 680, 988, 1252, 2101, 2513, 2883, 3291]. **Intersection** [22, 56, 351, 464, 502, 616, 644, 702, 880, 963, 970, 1031, 1101, 1275, 1286, 1368, 1386, 1404, 1458, 1459, 1641, 1675, 1760, 1995, 2084, 2115, 2490, 2882, 2937, 3026, 3094, 3331]. **intersections** [3309]. **Intractability** [563]. **intriguing** [960, 2239]. **intrinsical** [1149]. **Introducing** [3113, 3387]. **Introduction** [281, 384]. **Invariant** [166, 408, 525, 788, 789, 1052, 1143, 1289, 1397, 1422, 1432, 1495, 1539, 1667, 1743, 1821, 2029, 2073, 2318, 2412, 2487, 2603, 2661, 3100, 3242, 3355]. **Invariants** [533, 579, 1545, 2635, 2880, 2981]. **inverse** [1866, 3092, 3338]. **inverses** [2580, 2941, 3084, 3318, 3457]. **Inversion** [562, 975, 987, 1867, 2058, 2286]. **Inversions** [873]. **inversive** [1970, 2286, 2776]. **invertible** [2012]. **investigating** [2756]. **Investigation** [1148, 1852, 3324, 3353]. **Involutions** [2227, 3327]. **Involutory** [1452, 2333, 2686]. **involving** [3138]. **IPE**

[2159]. **IPP** [771, 2528, 3211]. **irreducibility** [2065, 3002, 3305]. **Irreducible** [37, 736, 858, 1336, 1365, 1440, 1503, 1641, 1797, 1934, 2044, 2092, 2216, 2220, 2370, 2792, 2822, 2860, 2916, 2989, 3023, 3105, 3256, 3407, 3414, 3425]. **irrepressible** [1932]. **ISD** [3356]. **iso** [3201, 3233]. **iso-dual** [3201]. **Isodual** [764, 2577, 3234, 3358]. **Isogenies** [1886, 1919, 2987, 3045, 3156, 3158, 3202]. **isogeny** [3237, 3428]. **isogeny-based** [3237, 3428]. **Isometric** [922]. **isometries** [1821]. **Isometry** [2596]. **Isometry-dual** [2596]. **isomorphic** [1002, 1039, 1440, 2544]. **Isomorphism** [2777, 3165, 3311, 3409]. **Isomorphisms** [469, 1338, 1841]. **isoperimetric** [2362]. **isotopic** [2619, 3104]. **isotopisms** [2205]. **Issue** [153, 1219, 1469, 1637, 1708, 1876, 1902, 2039, 2108, 2189, 2344, 2589, 3042]. **iterated** [303, 2935]. **Iterations** [547]. **iterative** [1844, 2085]. **Ito** [382, 2335]. **Itoh** [562, 987, 2058]. **IV** [854].

**J** [55, 1514]. **Jaap** [455]. **Jacobi** [371, 1985, 2668, 2831, 2849, 3122, 3123, 3181]. **Jacobian** [2064]. **Jacques** [2361]. **Jamison** [16]. **Jennifer** [3277]. **JH** [1949]. **Johnson** [64, 1033, 1109, 1646, 1689, 2553, 2847, 3449]. **joining** [3267]. **joint** [1620, 2025, 2676]. **Jordan** [470]. **Julin** [88]. **jump** [1704]. **Jumps** [631]. **Jungnickel** [520]. **Jungnickel-Tonchev** [520]. **junta** [2882]. **Just** [2936].

**Kai** [3317]. **Kai-Uwe** [3317]. **Kakeya** [1639]. **Kaleidoscopes** [2348]. **Kalyna** [2214]. **Kalyna-128** [2214]. **Kalyna-128/256** [2214]. **Kalyna-256** [2214]. **Kalyna-256/512** [2214]. **Kantor** [178, 512]. **Karystinos** [651]. **Karystinos-Pados** [651]. **Kasami** [393, 413, 2580, 2639]. **Katz** [1480]. **KDM** [3074]. **Keccak** [2380, 3452]. **KEM** [3124]. **Kendall** [2093, 2171, 2173, 2733]. **Kerdock** [346, 413, 951, 1881]. **Kernel** [598, 1236, 2280, 2920, 3172]. **Kernels** [152, 817, 2026]. **Key** [33, 77, 99, 119, 132, 137, 144, 154, 163, 193, 222, 263, 282, 331, 338, 430, 442, 445, 497, 568, 601, 607, 614, 663, 685, 691, 704, 762, 798, 883, 966, 1034, 1062, 1083, 1091, 1122, 1166, 1200, 1263, 1297, 1311, 1333, 1441, 1443, 1497, 1505, 1511, 1521, 1622, 1629, 1696, 1728, 1743, 1757, 1787, 1853, 1891, 1915, 1975, 1990, 2007, 2012, 2048, 2089, 2094, 2151, 2152, 2203, 2209, 2227, 2254, 2268, 2312, 2366, 2384, 2395, 2471, 2539, 2586, 2725, 2727, 2786, 2789, 2815, 2823, 2873, 2965, 2988, 3058, 3073, 3074, 3082, 3085, 3218, 3246, 3257, 3288, 3365, 3403, 3435]. **Key** [3277]. **key-alternating** [1497, 3073, 3082]. **Key-Dependent** [601, 1441]. **Key-Exchange** [163]. **key-generation** [2815]. **Key-homomorphic** [2384]. **key-insulation** [2366, 2727]. **key-policy** [2312]. **key-recovery** [2823]. **Keyak** [2248]. **keyed** [2268, 2380]. **keyed-homomorphic** [2268]. **Keys** [832, 1006, 1864, 1901, 1940, 2295, 2303, 2516, 3019, 3249, 3378, 3436]. **keyspace** [2759]. **kinds** [2631]. **Kirkman** [446, 578, 581, 971, 995, 1049, 1050, 1212, 1671, 2072, 2166, 2294, 2744, 3012, 3179, 3426]. **Klein** [1800, 2763, 3297]. **Kleinfeld** [984]. **Kloosterman** [401, 622, 1099, 1316]. **Kløve** [2105]. **KM** [2427]. **KM-arcs** [2427]. **Kneser** [1472]. **Knot** [3420]. **Knowledge** [270, 1898, 2384, 2663, 2913, 2915, 2930, 3042, 3045–3047]. **Known** [308, 505, 660, 1929, 2094, 2333, 2586, 2620, 2808, 3056]. **known-key** [2094, 2586]. **Knuth** [984]. **Ko** [1642, 1658, 1819, 2345]. **Koblitz** [435, 2331]. **Koetter** [678]. **Köhler** [11]. **Korchmáros** [2386]. **Korkin** [535]. **Kötter** [1678, 3091]. **KPD** [578]. **Kranz** [2485]. **Krawtchouk** [3144]. **Kronecker** [1599]. **Kummer** [1604, 2187]. **Kung** [2016]. **Kyber** [3427].

**L** [585]. **L-Intersecting** [585]. **labeling** [2565]. **Lagrangian** [1345]. **Laguerre**

[3174]. **Lai** [1283, 2090, 3013, 3152, 3197]. **Lam** [2250]. **Lambda** [475]. **Lambda-Designs** [475]. **Lander** [1239]. **Language** [157]. **languages** [2310]. **Large** [18, 128, 273, 381, 412, 471, 491, 513, 585, 806, 811, 971, 988, 1050, 1077, 1212, 1227, 1231, 1506, 1532, 1643, 2036, 2072, 2077, 2096, 2125, 2141, 2162, 2166, 2191, 2297, 2504, 2693, 2798, 2858, 2862, 2891, 2954, 3008, 3012, 3142, 3159, 3415]. **larger** [3063]. **Largest** [366, 634, 1615, 1642, 1819]. **Last** [81, 838, 2531]. **latency** [3053]. **Latin** [58, 460, 638, 705, 722, 746, 894, 895, 905, 926, 1037, 1157, 1169, 1631, 2005, 2119, 2371, 2502, 2557, 2994, 3090, 3443]. **Lattice** [326, 519, 716, 1465, 1622, 1718, 1883, 2231, 2448, 2508, 2552, 2663, 2704, 2809, 2909, 2916, 2949, 3115, 3116, 3127, 3403, 3427, 3458]. **Lattice-based** [1622, 2663, 2704, 2909, 3116, 3458]. **Lattices** [535, 948, 1096, 1324, 1719, 1825, 1845, 1853, 1855, 2009, 2132, 2146, 2182, 2287, 2404, 2452, 2531, 2655, 2795, 2987, 3040, 3149, 3303, 3307]. **layer** [3328]. **layers** [2051, 2306]. **LBlock** [3450]. **LBlock-s** [3450]. **LCD** [2298, 2313, 2520, 2526, 2561, 2571, 2599, 2649, 2709, 2722, 2729, 2959, 3034, 3064, 3208, 3209, 3321, 3350]. **LCP** [2921]. **LCZ** [1384]. **LDPC** [714, 910, 942, 956, 2484, 2719]. **leader** [2889]. **Leakage** [2159, 2251, 2423, 2471, 2690, 2789, 3055, 3149]. **Leakage-resilient** [2251, 2423, 2690, 2789, 3055, 3149]. **leakages** [3435]. **Leander** [2485, 2580]. **learning** [1791]. **Least** [104, 751, 2113]. **Lee** [911, 1161, 1165, 1471, 1583, 1613, 1769, 2379, 2770, 3199]. **Leech** [1465]. **left** [1432, 1813]. **Legendre** [550, 912, 1785, 2680]. **Lehmer** [2131]. **Lemma** [698, 793, 1471]. **Lempel** [639, 843, 2442, 2511]. **Length** [102, 122, 209, 224, 229, 302, 537, 551, 574, 595, 826, 833, 841, 869, 919, 943, 972, 985, 1016, 1047, 1052, 1059, 1061, 1126, 1127, 1170, 1186, 1278, 1309, 1310, 1320, 1349, 1389, 1406, 1522, 1525, 1541, 1586, 1657, 1733, 1749, 1754, 1775, 1777, 1783, 1805, 1848, 1881, 1955, 1993, 2024, 2085, 2089, 2100, 2234, 2262, 2338, 2445, 2460, 2467, 2503, 2578, 2646, 2680, 2695, 2731, 2777, 2974, 3109, 3159, 3170, 3178, 3206, 3211, 3319, 3383, 3388, 3389, 3394]. **lengthened** [3081]. **Lengths** [306, 523, 656, 829, 1007, 1402, 1742, 2449, 2653, 2753, 3184]. **Lenz** [170, 237, 1567]. **Lenz-Barlotti** [237]. **less** [1284, 3315]. **level** [68, 509, 1430, 3243]. **Levels** [552, 730]. **Levenshtein** [1059, 3178]. **LEX** [1527]. **Lexicodes** [804, 1688, 2317]. **Lexicographic** [230]. **LFSR** [3228]. **LFSR-based** [3228]. **LFSRs** [2372]. **Li** [2212]. **Liao** [1272]. **Lie** [1229]. **Liebler** [320, 1535, 1741, 2188, 2410, 2671, 2761, 2767, 3335]. **lies** [1468]. **Life** [170]. **Lifted** [1716, 2001, 2393, 2643, 3185, 3238, 3354]. **Lifting** [937, 3201]. **lifts** [1783]. **LIGA** [2679]. **Ligero** [3044]. **Light** [2109]. **lightweight** [2485, 2686, 3044]. **Like** [285, 340, 939, 1171, 1363, 1659, 1849, 2060, 2069, 2079, 2323, 2380, 2542, 2622, 2651, 3060, 3111, 3158]. **limit** [249, 1462]. **Limitations** [3356, 3406]. **limited** [1059, 1712, 1746]. **limited-magnitude** [1712, 1746]. **limits** [3207]. **Lin** [1328, 3027]. **Lin17** [2665]. **Line** [19, 75, 320, 714, 786, 886, 985, 1045, 1215, 1242, 1408, 1535, 1640, 1741, 1818, 2188, 2395, 2419, 2718, 2940]. **line-oval** [1215]. **line-primitive** [2940]. **line-transitive** [1045]. **line/off** [2395]. **Linear** [15, 229, 243, 246, 249, 269, 280, 285, 301, 313, 319, 330, 336, 357, 362, 369, 381, 386, 389, 391, 401, 418, 447, 467, 473, 477, 479, 480, 488, 499, 510, 545, 548, 558, 568, 586, 588, 603, 615, 639, 671, 674, 680, 725, 729, 734, 737, 757, 765, 768, 794, 804, 826, 834, 843, 870, 912, 998, 1154, 1161, 1180, 1196, 1209, 1603, 1605, 1633, 1634, 1647, 1712, 1737, 1871, 1913, 2022, 2075, 2106, 2293, 2327, 2350, 2354, 2430, 2431, 2454, 2479, 2480, 2490, 2497, 2515, 2521, 2546, 2568, 2732, 2769, 2857, 2864, 3106, 3151, 3213, 3253, 3293, 3367]. **linear** [19, 35, 49, 64, 742, 946, 949, 955, 972, 989, 992,

993, 997, 1003, 1005, 1017, 1025, 1057, 1086, 1088, 1127, 1163, 1182, 1185, 1203, 1236, 1242, 1262, 1287, 1361, 1378, 1401, 1489, 1506, 1508, 1524, 1525, 1530, 1559, 1587, 1631, 1649, 1669, 1717, 1780, 1820, 1828, 1842, 1862, 1865, 1868, 1969, 1982, 2015, 2020, 2021, 2033, 2037, 2062, 2079, 2085, 2086, 2092, 2102, 2206, 2240, 2253, 2279, 2304, 2332, 2370, 2374, 2409, 2436, 2468, 2481, 2495, 2496, 2569, 2572, 2689, 2695, 2705, 2773, 2784, 2788, 2800, 2819, 2836, 2854, 2878, 2894, 2986, 3035, 3120, 3153, 3245, 3262, 3324, 3344, 3354, 3392]. **linear** [104, 922, 974, 1045, 1077, 1085, 1114, 1122, 1160, 1208, 1298, 1330, 1367, 1394, 1451, 1497, 1517, 1534, 1574, 1585, 1653, 1660, 1694, 1740, 1746, 1750, 1785, 1810, 1864, 1870, 1929, 2041, 2068, 2077, 2144, 2219, 2230, 2264, 2309, 2322, 2337, 2415, 2442, 2461, 2467, 2517, 2539, 2687, 2706, 2801, 2824, 2835, 2843, 2895, 2920, 2923, 2940, 3096, 3125, 3212]. **Linear-Algebraic** [369]. **linear/coset** [1262]. **Linearity** [200, 230, 805, 1168, 2773, 2788, 2819, 3100]. **linearized** [1014, 1720, 2901, 3098, 3185, 3215, 3279]. **Linearly** [288, 1887, 2157, 2437, 2558]. **Lines** [400, 909, 1167, 1254, 1376, 1470, 1751, 1977, 2603, 2931, 3238, 3259, 3361]. **Ling** [1789]. **link** [2219]. **Linked** [2439, 3195]. **links** [2416]. **Lipschitz** [2849]. **List** [689, 1097, 1204, 1356, 1684, 1716, 1725, 2053, 2679, 2785]. **list-decoding** [2053]. **Littlewood** [2567]. **Lizard** [2762]. **LLL** [1713, 1845, 2449]. **LMR** [3208]. **Local** [160, 448, 465, 698, 793, 1086, 1598, 1779, 2382, 3084, 3238]. **locality** [2198, 2604, 2613, 2624, 2692, 2707, 2772, 2895, 3387]. **Locally** [459, 2199, 2599, 2600, 2605, 2714, 2800, 2958, 2967, 2984, 3134, 3198, 3208, 3212, 3251, 3283, 3339, 3415, 3445]. **locally-APN** [2967]. **locating** [2594]. **lock** [2311]. **log** [1166, 1900]. **Logarithm** [158, 324, 436, 553, 584, 615, 1200, 1518, 1904, 2404, 3068, 3205, 3419]. **logarithmic** [1229, 1337, 1869]. **Logarithms** [4, 432, 1905, 2363, 2563]. **logspace** [3221]. **Loidreau** [2254, 2615]. **Long** [381, 1630, 1635, 1769, 2460, 3267]. **long-period** [3267]. **Longest** [2588]. **look** [3058]. **Looking** [609]. **loop** [1522, 1960]. **loops** [2]. **lose** [3395]. **lossy** [2662]. **Lovász** [698, 2878]. **Low** [586, 857, 965, 1089, 1211, 1334, 1372, 1399, 1506, 1700, 1705, 1709, 1798, 1888, 2042, 2137, 2156, 2394, 2620, 2636, 2673, 2692, 2707, 2939, 3030, 3053, 3177, 3180, 3265, 3342]. **low-complexity** [3265]. **low-degree** [2939]. **Low-density** [965, 1211]. **Low-hit-zone** [1700, 2137, 2156]. **low-latency** [3053]. **Low-Memory** [857, 1399]. **low-power** [1888, 3177]. **Low-rank** [2636]. **Low-weight** [3342]. **Lower** [59, 335, 349, 353, 501, 556, 668, 941, 968, 991, 1313, 1769, 1798, 2044, 2110, 2426, 2486, 3005, 3101, 3375, 3417, 3443]. **LowMC** [2983]. **LowMS** [3124]. **LP** [2171]. **LPN** [3406]. **LRC** [2692, 2707]. **LRCs** [2604, 2944, 3192]. **LRW1** [2936]. **LTF** [3303]. **LTV** [1989]. **Luby** [876, 2720]. **Lucas** [1890, 3139]. **Lusztig** [2613]. **LWC** [2684]. **LWE** [1763, 2178, 2747, 2965, 3348].

**M** [586, 641, 1469, 2168, 3158]. **m-sequences** [2168]. **M-SIDH** [3158]. **MAC** [1851, 2256, 3272]. **machines** [48, 2973]. **MacWilliams** [1110, 1114, 1419, 1656, 1824, 2043, 2836]. **Maekawa** [558]. **Magliveras** [1219]. **magnitude** [1712, 1746, 2652]. **Main** [208]. **maintain** [66]. **Maiorana** [2602, 2682, 2687, 2997, 3196]. **make** [2062]. **Maliciously** [2965]. **malleable** [1622, 2210, 3117]. **MANETs** [694]. **Manickam** [2249, 2388]. **manipulation** [2584]. **Mansour** [2012, 2661, 3073]. **Mantin** [2215, 2625]. **Many** [399, 458, 725, 851, 1604, 1809, 2337, 2662, 2714, 3303]. **map** [1119, 1676, 1900, 2116]. **Mapping** [2174, 3448]. **Mappings** [23, 882, 896, 1270, 1296, 1358, 1492, 2149]. **maps** [87, 1935, 2004, 2132, 2629, 2665, 2737,

2890, 3126, 3138, 3183, 3253]. **marginals** [2680]. **Marialuisa** [1514]. **marking** [1470]. **Markov** [2887]. **Martinet** [3446]. **Mask** [763, 3153]. **masked** [1530]. **masking** [3053]. **Mass** [1523]. **Massey** [1283, 2090, 3013, 3152, 3197]. **master** [3074]. **master-key** [3074]. **matchings** [1847, 3054]. **Mates** [894, 895]. **Mathematics** [430, 2875, 3042]. **Mathon** [1431]. **Matrices** [49, 54, 128, 147, 202, 203, 205, 272, 274, 278, 298, 345, 351, 382, 402, 409, 417, 518, 555, 557, 655, 675, 702, 706, 741, 769, 813, 877, 920, 926, 935, 969, 1035, 1108, 1123, 1135, 1146, 1193, 1203, 1227, 1234, 1284, 1289, 1291, 1374, 1392, 1438, 1439, 1452, 1475, 1580, 1663, 1668, 1674, 1680, 1738, 1784, 1822, 1840, 1941, 1947, 2045, 2124, 2318, 2335, 2437, 2475, 2487, 2577, 2680, 2685, 2686, 2691, 2753, 2755, 2839, 2877, 2918, 2919, 2927, 2955, 3151, 3190, 3203, 3216, 3219, 3268]. **Matrix** [228, 362, 541, 680, 824, 1065, 1382, 1599, 1617, 1682, 1727, 2450, 2518, 2593, 2718, 3150, 3234, 3280, 3402]. **matroid** [1609, 2626]. **Matroids** [215, 530, 647, 1396, 1794, 2282, 2406, 2637, 2715, 2911, 2949, 2990, 3136]. **Matsui** [1497, 3050]. **Matsumoto** [445, 1586]. **matter** [2867]. **Matthews** [1213]. **Mattson** [486, 671, 2232, 2660, 2810, 3004]. **Mattson-Type** [671]. **Maximal** [73, 76, 101, 239, 249, 425, 467, 472, 495, 498, 529, 635, 636, 638, 663, 667, 722, 786, 959, 1030, 1116, 1126, 1188, 1244, 1245, 1403, 1532, 1541, 1640, 1680, 1882, 2121, 2184, 2350, 2351, 2401, 2525, 2556, 2575, 2595, 2645, 2651, 2721, 2929, 3090, 3208, 3368, 3416]. **maximality** [1180, 2119]. **Maximally** [396, 2783]. **Maximum** [247, 279, 446, 501, 721, 775, 889, 1066, 1198, 1259, 1348, 1475, 1658, 1847, 1969, 2135, 2160, 2196, 2269, 2429, 2455, 2460, 2527, 2777, 3097, 3137, 3239, 3254, 3319]. **MaxMinMax** [1956]. **McEliece** [137, 193, 1095, 1480, 1940, 1990, 2770, 3066]. **McFarland** [26, 2602, 2682, 2687, 2997, 3196]. **McKay** [2122]. **McLaughlin** [1510]. **MDC** [1698, 1837]. **MDC-2** [1837]. **MDC-4** [1698]. **MDP** [2477]. **MDS** [208, 210, 310, 542, 646, 835, 1001, 1024, 1103, 1292, 1303, 1371, 1452, 2043, 2045, 2051, 2076, 2096, 2141, 2193, 2221, 2264, 2313, 2456, 2465, 2519, 2540, 2658, 2664, 2685, 2686, 2709, 2717, 2734, 2818, 2874, 2938, 2966, 2974, 3011, 3161, 3243, 3285, 3462]. **mean** [2112, 2932]. **mean-regular** [2112]. **Meet** [684, 1998, 2003, 2214, 2567, 3024, 3118, 3186, 3352]. **Meet-in-the-middle** [1998, 2003, 2214, 3024, 3118, 3186, 3352]. **Meeting** [20, 41, 227, 558, 651, 961, 993, 1088, 1414, 1576, 1748]. **meets** [2873]. **Membership** [699, 798, 3031, 3046]. **memoriam** [1241]. **memories** [1584]. **Memory** [857, 1074, 1399, 2827, 3067, 3078, 3317]. **Memoryless** [1369]. **Mendelsohn** [311, 516, 901]. **Menon** [29, 70, 195]. **Merkle** [3313]. **Meshulam** [1156]. **Mesner** [390]. **Mesner-Algebras** [390]. **Message** [158, 1224, 1413, 1441, 1775, 2197, 2243, 2612, 2653, 3271, 3313]. **messages** [1441, 3062]. **Meta** [749]. **Meta-Thin** [749]. **Meter** [156]. **Metering** [734, 779]. **Method** [16, 115, 769, 791, 1360, 1422, 1682, 1806, 2037, 2064, 2087, 2263, 2618, 2713, 2730, 2746, 2756, 2835, 2855, 2968, 2980, 3006, 3050, 3084, 3105, 3210, 3267, 3301, 3413, 3450]. **Methodology** [119, 1862]. **Methods** [282, 2145, 2225, 2934, 2960]. **Metric** [149, 721, 834, 1612, 1769, 1983, 2093, 2173, 2176, 2194, 2223, 2274, 2285, 2339, 2406, 2436, 2457, 2507, 2517, 2576, 2583, 2591, 2592, 2615, 2617, 2621, 2627, 2679, 2733, 2770, 2785, 2992, 3037, 3065, 3087, 3100, 3108, 3112, 3124, 3278, 3396, 3418]. **Metrical** [2493]. **metrics** [1165, 3396]. **Meyer** [314, 2319]. **Meyer-Müller** [314]. **Micro** [783]. **Micro-payment** [783]. **microcontrollers** [1889]. **middle** [1998, 2003, 2214, 3024, 3118, 3186, 3352]. **Miklós** [2249, 2388]. **MILP** [2380, 2634, 2713, 3153]. **MILP-aided**

[2380, 2634]. **MILP-based** [2713]. **Minihypers** [558, 610, 635, 737, 993, 1088, 1111, 1201, 1410]. **Minimal** [205, 224, 367, 534, 667, 738, 902, 1002, 1152, 1164, 1210, 1220, 1229, 1337, 1357, 1382, 1534, 1761, 1813, 1869, 2165, 2450, 2496, 2509, 2572, 2633, 2641, 2651, 2687, 2801, 2811, 2993, 3055, 3077, 3144, 3261, 3432]. **Minimization** [535]. **minimizing** [3424]. **Minimum** [150, 211, 316, 322, 385, 388, 468, 482, 582, 675, 709, 737, 743, 772, 809, 826, 837, 887, 972, 1061, 1264, 1267, 1522, 1587, 1618, 1659, 1751, 1768, 1769, 1827, 1836, 1929, 1973, 2096, 2098, 2103, 2141, 2314, 2386, 2437, 2453, 2531, 2598, 2758, 2818, 2895, 2931, 2984, 3010, 3134, 3417]. **Minimum-Weight** [582]. **Minkowski** [132, 2404]. **Minors** [518]. **MinRank** [3052]. **missing** [997, 3003, 3184]. **mission** [1122]. **MISTY1** [1860]. **mix** [1008, 1105, 2991]. **Mixed** [260, 443, 730, 979, 1772, 3155, 3287, 3385, 3441, 3451]. **mixers** [3255]. **mixture** [3060]. **MJH** [1837]. **MNT** [846]. **Möbius** [2715]. **mod** [863, 994, 1465]. **mode** [1949]. **model** [945, 1106, 1200, 1622, 1698, 1858, 1894, 1939, 2312, 2321, 2366, 2396, 2781, 2789, 2796, 2813, 2870, 3029, 3154]. **modeling** [3153]. **Models** [554, 782, 867, 1464, 1595, 2281, 3374]. **Moderate** [2848]. **Moderate-density** [2848]. **modes** [2380]. **Modifications** [119]. **Modified** [767, 1234, 1341, 1392, 1594, 1989, 3102, 3246]. **Modular** [136, 303, 590, 1108, 1150, 1602, 2286, 2508, 2866, 2870, 3046]. **modulation** [2093, 2507]. **Module** [213, 1825, 2836]. **modules** [2296, 3296]. **Moduli** [868, 3303]. **moduli-PRF** [3303]. **Modulo** [61, 608, 625, 974, 1163, 1235, 1471, 1771]. **modulus** [1715, 2452]. **Moisio** [2415]. **MOLS** [1621, 2104, 2947]. **Moments** [363, 1262, 1517, 3329]. **monochrome** [1737]. **Monomial** [1479, 1841, 2599, 3165, 3192]. **Monomial-Cartesian** [2599, 3192]. **monomials** [1792, 3325, 3412]. **monotone** [1729, 2846]. **Montgomery** [119, 315]. **Morgan** [2458]. **MORUS** [2367]. **Mosaics** [2179, 2766, 3119]. **most** [970, 1045, 1152, 1635, 2190, 2415, 2513, 3341]. **MPC** [2965, 3349]. **MPC-in-the-Head** [3349]. **MQV** [1034]. **MR** [55, 120, 134, 164, 189]. **MRD** [816, 2240, 2453, 3065, 3096, 3262, 3337, 3377]. **MST** [832, 1225]. **MUB** [3268]. **Mullen** [2458]. **Muller** [40, 72, 165, 275, 314, 467, 507, 529, 582, 948, 1064, 1072, 1097, 1202, 1210, 1498, 1682, 1707, 1709, 2183, 2421, 2446, 2515, 2627, 2633, 3059, 3122, 3155, 3181, 3224, 3310, 3394]. **Muller-type** [3224]. **Mullin** [571]. **Multi** [446, 478, 735, 1200, 1390, 1551, 1574, 1723, 1736, 2184, 2187, 2194, 2209, 2231, 2321, 2396, 2428, 2501, 2570, 2698, 2868, 2937, 2945, 2965, 2977, 3026, 3169, 3345, 3360, 3365]. **multi-authority** [2501]. **multi-challenge** [2945]. **multi-client** [2937]. **multi-dimensional** [3365]. **multi-HFE** [1551]. **multi-key** [2209, 2965]. **multi-linear** [1574]. **Multi-party** [1390, 3026, 3169]. **multi-permutation** [2977, 3360]. **Multi-point** [2187]. **multi-prime** [3345]. **Multi-Receiver** [478]. **multi-secret** [1736, 2868]. **multi-sequences** [2231]. **multi-shot** [2194]. **multi-signature** [1200]. **multi-signatures** [2428]. **Multi-trial** [1723]. **multi-twisted** [2698]. **Multi-User** [446, 735, 2321, 2396, 2570]. **multicast** [1913]. **Multicovering** [507, 1651]. **Multidimensional** [765, 1146, 2037, 2473, 3106]. **multilength** [2833, 3385]. **Multilevel** [948, 1146, 1584, 3286]. **multilinear** [2132, 2665]. **Multimedia** [2074, 2528, 2942, 3211]. **multipartite** [2364, 2970]. **multiparty** [2275, 2384]. **Multiple** [80, 520, 718, 867, 991, 1085, 1185, 1247, 1248, 1537, 1848, 2057, 2099, 2538, 2968, 3019, 3163, 3225, 3249]. **Multiplication**

[315, 444, 1290, 1647, 2485, 2841, 3382, 3402, 3416, 3447]. **Multiplications** [873, 1984]. **Multiplicative** [398, 987, 1976, 2042, 2663, 2970, 3338]. **multiplicity** [2693]. **multiplied** [1130]. **multiplier** [26, 43, 1911]. **multipliers** [6, 2484]. **Multiply** [232]. **Multiround** [337]. **Multisecret** [221, 823]. **Multisequences** [1077, 2025]. **Multiset** [2316]. **multisets** [1248, 1483, 2084]. **multishot** [3185]. **multivariable** [999, 1561, 1868]. **Multivariate** [1505, 2939, 3176, 3228]. **must** [2453]. **Mutually** [273, 638, 722, 926, 1631, 1731, 1840, 1977, 2119, 2334, 2502, 2557, 2645, 2907, 3114, 3443]. **myths** [2781, 2813].

**n** [1614, 2738]. **Naive** [1686]. **Naor** [545, 2336]. **narrow** [2503, 2741]. **narrow-sense** [2503, 2741]. **National** [154]. **NAXOS** [1034]. **NC** [2747]. **Near** [403, 774, 818, 829, 1024, 1132, 1183, 1369, 1435, 1487, 1632, 2030, 2117, 2138, 2229, 2404, 2664, 2874, 2938, 2972]. **near-** [2530]. **near-collisions** [1369]. **Near-complete** [2138]. **Near-Extremal** [829, 1132, 2972]. **Near-MDS** [1024, 2664, 2874, 2938]. **near-optimal** [1632]. **Nearly** [182, 1049, 1414, 1717, 1790, 2407, 2775]. **Necessary** [70, 227, 1011, 1181, 2477, 2487]. **nega** [2740, 3113]. **nega-crosscorrelation** [3113]. **nega-Forrelation** [3113]. **nega-Hadamard** [3113]. **negabent** [2934, 3322]. **negacirculant** [2307]. **Negacyclic** [1381, 1486, 2026, 2292, 2998, 3129, 3170, 3343]. **negaperiodic** [2172]. **negative** [1037, 1756]. **negligible** [1083]. **neighbor** [2757]. **neighbors** [943]. **Neighbour** [1529, 1646, 1689, 1966, 2812]. **Neighbour-transitive** [1646, 1689, 2812]. **neighbourhood** [1081]. **Ness** [2639, 3353]. **nest** [980, 1067]. **Nested** [352, 569, 1520, 2048, 3283]. **nesting** [3376]. **Net** [124]. **Nets** [2, 18, 65, 82, 233, 565, 586, 599, 679, 701, 741, 814, 946, 1055, 1332, 1960, 2880]. **Network** [632, 1744, 1913, 2062, 2189, 2192, 2194, 3185, 3298]. **networks** [48, 1303, 1491, 1511, 1629, 2638, 3082, 3225, 3298]. **Neumaier** [2118, 2879]. **neural** [3312]. **neutralization** [3275]. **never** [3425]. **Newton** [458]. **Next** [2633]. **Next-to-Minimal** [2633]. **NFSR** [1615, 1801, 2492, 2728, 2746, 2975]. **NFSR-based** [2492, 2746]. **NFSRs** [2323, 2435, 2491, 2544, 2756, 2975, 3267, 3409, 3410]. **Niederreiter** [1594]. **Nielsen** [3091]. **Niho** [853, 2688]. **nilpotency** [2793]. **nilpotent** [3308]. **nilpotents** [2793]. **Nine** [151]. **NLFSRs** [1721]. **NMDS** [1644, 2717, 3089, 3236]. **no** [55, 120, 134, 164, 189, 333, 967, 1156, 1159, 1718]. **noise** [2942, 3302]. **noisy** [2057, 2665]. **Nomura** [1464]. **Non** [130, 222, 246, 284, 316, 320, 385, 451, 486, 491, 576, 663, 682, 704, 705, 716, 721, 722, 754, 780, 805, 808, 1002, 1039, 1083, 1088, 1107, 1162, 1166, 1251, 1290, 1331, 1338, 1354, 1410, 1443, 1477, 1488, 1543, 1622, 1640, 1644, 1659, 1680, 1724, 1729, 1773, 1787, 1813, 1969, 1986, 1997, 2012, 2034, 2126, 2210, 2240, 2273, 2275, 2301, 2322, 2347, 2362, 2365, 2384, 2427, 2481, 2483, 2524, 2526, 2611, 2767, 2780, 2851, 2860, 2868, 2918, 2919, 2947, 3025, 3030, 3077, 3104, 3117, 3137, 3227, 3239, 3262, 3270, 3296, 3319, 3333, 3335, 3372, 3383]. **Non-Abelian** [704, 1543, 1813, 2524]. **non-adjacent** [1290]. **non-amorphic** [1477]. **Non-Binary** [130, 316, 385, 486, 2611, 2860]. **Non-canonical** [3239]. **Non-Cayley** [754]. **Non-Collinearity** [451]. **non-commutative** [2301]. **non-cyclic** [1659]. **non-degenerate** [1107, 3025]. **non-Desarguesian** [2427]. **Non-Deterministic** [716]. **non-disjoint** [3372]. **Non-Existence** [320, 722, 780, 1338, 1354, 1644, 1680, 2347, 2767, 2780, 3227, 3335]. **Non-free** [1488, 2526, 3296]. **non-full-rank**

[2365]. **Non-Hamming** [721]. **non-incidence** [2362]. **Non-Interactive** [222, 576, 663, 808, 1166, 1443, 1724, 1787, 2275, 2384, 2868]. **non-invertible** [2012]. **Non-isomorphic** [1002, 1039]. **non-isotopic** [3104]. **Non-linear** [1969, 2240, 3262]. **Non-linearity** [805]. **non-malleable** [1622, 2210, 3117]. **Non-Maximal** [663]. **non-monotone** [1729]. **non-negligible** [1083]. **non-orthogonal** [3030]. **non-overlapping** [3137, 3319, 3383]. **non-perfect** [1773]. **Non-Polynomial** [705]. **non-prime-power** [1986]. **Non-Primes** [682]. **Non-repudiation** [808]. **non-Schurian** [2126]. **non-singular** [1251, 1640, 2483]. **Non-special** [1997]. **non-spreading** [3333]. **Non-surjective** [284]. **Non-symmetric** [2034, 2273, 2322]. **non-trivial** [2947]. **Non-Uniform** [246]. **non-unital** [2851, 2918, 2919, 3077]. **non-weakly** [3270]. **non-weighted** [1088, 1410]. **Nonabelian** [18, 803, 2255, 2378]. **nonadaptive** [2398]. **nonassociativity** [2575]. **nonbinary** [1335, 2114, 2222]. **Nonces** [660]. **nonclassical** [1139]. **nondegenerate** [106]. **nonelementary** [1037]. **Nonexistence** [32, 62, 64, 168, 297, 350, 485, 488, 797, 1132, 1391, 1587, 1704, 1814, 2067, 2170, 2522, 2733, 2784, 3397]. **Nonfactorizable** [1547]. **nonintersecting** [3075]. **Nonisomorphic** [125]. **Nonlinear** [152, 330, 396, 870, 891, 1019, 1036, 1080, 1092, 1447, 1782, 1792, 1827, 2025, 2161, 2306, 2890]. **Nonlinearity** [501, 788, 890, 1306, 1509, 1616, 1843, 1850, 2056, 2405, 2408, 2478, 2808, 3275]. **Nonsingular** [1254, 1546–1548, 2756, 3075]. **Nonsymmetric** [61, 1464]. **Nontrivial** [3326]. **Nontrusting** [149]. **nonuniform** [1380]. **nonweight** [225]. **nonzeros** [1730]. **Norm** [590, 1718, 2237, 3128, 3397, 3411]. **norm-trace** [3128, 3411]. **Normal** [39, 50, 178, 213, 275, 277, 298, 1089, 1350, 1372, 1570, 1879, 1899, 2002, 2224, 2240, 2389, 2748, 2896, 3038]. **normalized** [1394]. **Normalizers** [695]. **Note** [10, 32, 55, 85, 218, 305, 504, 586, 646, 758, 1055, 1126, 1225, 1258, 1406, 1470, 1570, 1606, 1690, 2013, 2107, 2152, 2200, 2255, 2326, 2438, 2660, 2751, 2810, 3004, 3095, 3219, 3289, 3384]. **Notes** [843, 1192, 1250, 1633]. **Nothing** [484, 2749]. **Notions** [1326, 1397]. **Novel** [2690, 2971, 3460]. **NQR** [355]. **NTRU** [716, 1238, 1758, 3019, 3249]. **NTT** [3302]. **NTT-friendly** [3302]. **Nuclei** [226, 528]. **nucleus** [984]. **Null** [212, 1059]. **Nullstellensatz** [2878]. **Number** [20, 81, 205, 215, 291, 333, 351, 547, 591, 616, 831, 838, 870, 888, 905, 1002, 1036, 1120, 1197, 1206, 1222, 1400, 1444, 1459, 1472, 1499, 1530, 1604, 1684, 1718, 1720, 1751, 1897, 2087, 2092, 2277, 2281, 2284, 2286, 2362, 2455, 2500, 2533, 2536, 2556, 2618, 2822, 2865, 2922, 2952, 2957, 3001, 3097, 3101, 3104, 3130, 3220, 3368, 3419, 3424]. **number-theoretic** [291, 333]. **Numbers** [464, 502, 525, 754, 963, 970, 1040, 1101, 1286, 1986, 3224, 3449]. **numerical** [1184]. **Nyberg** [3097].

**OAs** [1379]. **obfuscation** [1864]. **Obituary** [1513, 1514, 1567, 2361, 3021]. **oblivious** [1280, 2017]. **Observations** [409, 849, 1317, 3130]. **obtain** [2862]. **Obtained** [149, 980, 1067, 1186, 3077, 3103]. **Obtaining** [1034]. **occasion** [1219]. **octagon** [1044]. **Octonion** [470]. **Odd** [13, 268, 357, 500, 528, 845, 977, 1047, 1125, 1135, 1220, 1231, 1310, 1355, 1359, 1363, 1433, 1507, 1541, 1551, 1643, 1657, 1703, 1733, 1755, 1776, 1777, 1797, 1809, 1818, 1993, 2110, 2208, 2390, 2478, 2494, 2540, 3256, 3370]. **odd-points** [1818]. **oddly** [2445]. **ODPC** [1775]. **OFB** [3233]. **off** [859, 1297, 3028]. **off-line** [2395]. **officer** [94]. **Offord** [2567]. **Oil** [3441]. **OLE** [3047]. **OLE-based** [3047]. **on-chip** [1888]. **On-line** [1408, 2395]. **on-line/off-line** [2395]. **O'Nan** [1171]. **One** [616, 662, 783, 803, 831, 924, 930, 973, 1119,

1127, 1320, 1521, 1660, 1788, 1800, 1856, 2174, 2175, 2364, 2489, 2609, 2748, 2774, 2843, 2923, 3061, 3178, 3214, 3269, 3407]. **one-and-half** [1856]. **one-coincidence** [924]. **one-dimensional** [2843, 3269]. **one-error-correcting** [1320]. **one-factorizations** [2364]. **One-point** [930, 973, 1800]. **one-time** [2609]. **One-way** [783, 1521]. **one-weight** [1660, 3407]. **ones** [2012]. **online** [3223]. **only** [1121]. **OOCs** [1424, 2833]. **Open** [1245, 1873, 1895, 2799]. **opening** [2383, 2585, 2945, 3145, 3348]. **operations** [1610]. **operator** [2655]. **opposite** [2174]. **OPPTS** [1623]. **Optical** [115, 577, 1195, 1285, 1420, 1623, 1795, 2160, 2260, 2391, 2489, 2525, 3385]. **optima** [2986]. **Optimal** [31, 35, 50, 115, 229, 269, 335, 350, 352, 450, 467, 500, 510, 577, 640, 653, 777, 823, 828, 856, 888, 897, 904, 919, 966, 1089, 1127, 1158, 1170, 1214, 1268, 1285, 1288, 1336, 1357, 1380, 1424, 1516, 1611, 1623, 1657, 1692, 1700, 1780, 1790, 1795, 1815, 1829, 1843, 1847, 1872, 1888, 1918, 1936, 1955, 2033, 2058, 2082, 2089, 2097, 2137, 2193, 2260, 2272, 2304, 2382, 2391, 2402, 2403, 2407, 2409, 2489, 2498, 2537, 2541, 2572, 2605, 2649, 2692, 2707, 2729, 2752, 2778, 2807, 2892, 2944, 2958, 2959, 2981, 3005, 3016, 3065, 3134, 3146, 3149, 3177, 3192, 3198, 3203, 3251, 3312, 3377, 3385, 3389]. **optimal** [105, 990, 1012, 1073, 1102, 1186, 1195, 1272, 1320, 1325, 1367, 1379, 1560, 1616, 1632, 1665, 1682, 1733, 2156, 2250, 2339, 2478, 2584, 2604, 2618, 2652, 2775, 2800, 2936, 2942, 2969, 3077, 3088, 3123, 3212, 3218, 3263, 3314, 3316, 3339, 3386]. **optimally** [2468, 3209]. **optimization** [1417]. **optimized** [3111]. **Optimizing** [3447]. **Optimum** [1172, 1766]. **oracle** [1106, 1894, 1939, 2396, 2939]. **oracles** [1095]. **Orbit** [11, 824, 985, 1503, 1941, 2197, 2640, 2724, 3379]. **orbits** [97, 303]. **Order** [93, 118, 120, 151, 165, 223, 226, 230, 247, 271, 370, 422, 460, 467, 534, 536, 541, 551, 585, 617, 633, 697, 722, 739, 741, 754, 801, 840, 980, 985, 997, 1007, 1035, 1047, 1060, 1067, 1097, 1135, 1150, 1167, 1179, 1239, 1274, 1284, 1291, 1359, 1374, 1376, 1475, 1537, 1550, 1563, 1565, 1621, 1650, 1767, 1777, 1804, 1816, 1820, 1933, 1943, 1944, 2046, 2088, 2139, 2140, 2180, 2183, 2190, 2251, 2347, 2422, 2441, 2446, 2703, 2776, 2804, 2931, 2947, 2978, 3083, 3122, 3174, 3181, 3216, 3275, 3291, 3370, 3394, 3401]. **Ordered** [586, 1114]. **Ordering** [447, 1799]. **Orders** [6, 663, 672, 1439, 1683, 2566, 2744, 3230, 3281]. **ordinary** [2774]. **orientable** [3389]. **orientations** [3230]. **oriented** [1287, 3330]. **Orthogonal** [14, 58, 115, 173, 188, 204, 279, 292, 460, 559, 577, 586, 589, 638, 703, 722, 730, 833, 855, 894, 895, 926, 986, 1008, 1069, 1112, 1114, 1144, 1186, 1195, 1230, 1254, 1285, 1420, 1520, 1552, 1623, 1631, 1717, 1795, 1946, 1986, 2116, 2119, 2141, 2160, 2260, 2265, 2334, 2364, 2391, 2444, 2489, 2502, 2525, 2531, 2557, 2561, 2645, 2675, 2708, 2791, 2794, 2837, 2871, 2898, 2907, 2908, 2918, 2919, 2980, 3008, 3011, 3030, 3054, 3064, 3086, 3088, 3133, 3209, 3254, 3260, 3308, 3385, 3443]. **Orthogonality** [669, 2069, 3336]. **orthomorphisms** [3308]. **osculating** [1744]. **Ostrom** [358, 1540]. **Other** [55, 428, 757, 1227, 3311]. **Ott** [54]. **Otter** [3237]. **output** [501, 1083, 1572, 2728, 3351]. **outsourced** [1893]. **Oval** [201, 697, 1215]. **Ovals** [583, 679, 683, 701, 708, 3174]. **Overbeck** [2195]. **Overlap** [1681]. **overlapping** [3137, 3319, 3383]. **overlarge** [3179]. **Ovoidal** [1244]. **Ovoids** [512, 681, 715, 842, 1041, 1111, 1244, 1254, 1532, 1643, 2229, 2721, 3180, 3332].

**p** [2738, 3242, 3401, 3403]. **P-SPN** [3242]. **packet** [3328]. **packetization** [3243]. **Packing** [81, 311, 578, 597, 819, 838, 1555, 2833, 3069, 3199, 3385]. **Packings** [145, 326, 352, 420, 775, 959, 1158, 1288, 1300, 1815, 1872, 1968, 2218, 2606, 2871, 3261]. **Pados** [651]. **Paillier** [1724]. **Paillier-based** [1724]. **pair** [1327, 2135, 2180, 2221, 2568, 2680, 2703, 2818,

2974, 2994, 3081, 3188, 3308, 3352, 3386, 3388]. **pair-of-tweaks** [3352]. **pair-weight** [3386]. **paired** [2735]. **Pairing** [810, 953, 1223, 1522, 1526, 1867, 2537, 2662, 2899, 3031]. **pairing-based** [1223, 2899]. **pairing-friendly** [1526, 3031]. **pairings** [1121, 1282, 1739, 3447]. **pairings-friendly** [3447]. **Pairs** [55, 352, 482, 918, 1187, 1309, 1310, 2129, 2172, 2335, 2490, 2594, 2732, 2748, 2775, 2798, 2947, 3367]. **Pairwise** [5, 240, 1002, 2464, 2883]. **Paley** [459, 502, 983, 1162, 1543, 1778]. **palindromic** [3431]. **paper** [1833]. **Pappus** [1351, 2797]. **PAPR** [3030]. **Parabolic** [842, 1532]. **paradigm** [3349]. **Parallel** [444, 716, 987, 2850, 3272, 3287]. **Parallelisms** [489, 1788]. **Parameter** [730, 757, 966, 1204, 2160, 2531, 2984]. **Parameters** [64, 182, 334, 521, 591, 612, 731, 795, 916, 1222, 1266, 1306, 1340, 1354, 1400, 1450, 1526, 1695, 1704, 1942, 1980, 2538, 2632, 2704, 2888, 2968, 3016, 3072, 3088, 3096, 3148, 3222, 3398]. **parametrization** [2085]. **Parasites** [119]. **parent** [990, 1140, 2074, 2271, 2551, 2623]. **parent-identifying** [1140, 2271, 2623]. **Parity** [278, 596, 1211, 1784, 2636, 2848, 2860, 3255, 3280]. **parity-check** [1211, 2636, 2848, 2860, 3280]. **Part** [463]. **Partial** [73, 76, 103, 181, 185, 186, 206, 239, 348, 421, 448, 462, 472, 495, 498, 549, 569, 635, 636, 667, 681, 786, 913, 959, 1037, 1041, 1162, 1167, 1198, 1244, 1473, 1532, 1544, 1632, 1640, 1643, 1700, 1702, 1804, 1891, 1962, 1985, 1996, 2137, 2140, 2143, 2147, 2206, 2249, 2252, 2347, 2371, 2388, 2397, 2459, 2475, 2519, 2565, 2723, 2812, 2820, 2873, 2894, 2897, 3090, 3272, 3408]. **Partially** [69, 660, 969, 1932, 1936, 2542, 3067, 3237]. **Partially-bent** [69]. **Participants** [220, 689, 1152, 1515]. **Particular** [610, 1176, 1410, 1958]. **Parties** [149]. **Partition** [1288, 1571, 1938, 2098, 2499, 2991]. **partition-type** [1288]. **partitionable** [426]. **Partitioned** [254, 2063, 2447]. **Partitioning** [235, 592, 2759]. **partitionings** [2743]. **Partitions** [173, 188, 443, 457, 979, 1022, 1043, 1053, 1145, 1181, 1449, 1824, 2622, 2790, 3231, 3294, 3332]. **party** [1390, 2289, 3026, 3169]. **pass** [1891, 3218]. **PASS-Encrypt** [1891]. **password** [1884]. **Past** [432]. **path** [2949, 3264]. **pattern** [2160, 2260, 2489]. **Patterns** [99, 132, 331, 685, 868]. **Patterson** [1081, 3102]. **Pay** [783]. **Pay-Word** [783]. **payment** [783]. **PBDs** [1013]. **PBIBDs** [2832]. **PEKS** [1923]. **Pellikaan** [2589]. **Pencils** [438]. **Pentanomials** [858, 986, 3461]. **Perfect** [29, 36, 51, 87, 102, 111, 123, 126, 131, 135, 146, 160, 220, 249, 311, 317, 368, 389, 406, 423, 424, 457, 492, 506, 516, 594, 595, 598, 687, 733, 817, 841, 880, 892, 901, 908, 911, 959, 992, 1016, 1019, 1020, 1073, 1093, 1110, 1161, 1266, 1268, 1278, 1307, 1320, 1366, 1377, 1450, 1598, 1692, 1732, 1754, 1757, 1773, 1792, 1793, 1878, 1880, 1909, 1978, 1999, 2035, 2078, 2079, 2144, 2175, 2225, 2365, 2411, 2420, 2440, 2487, 2512, 2587, 2733, 2814, 2826, 2849, 2865, 2893, 2933, 2944, 2957, 3022, 3039, 3155, 3194, 3218]. **perfectly** [1413, 2408, 2890]. **period** [104, 1298, 1361, 1403, 1506, 2250, 2259, 2374, 2454, 2651, 2694, 2775, 3267, 3429]. **Periodic** [45, 305, 949, 1017, 1077, 1092, 1182, 1451, 1694, 1765, 1925, 3106]. **Periodicity** [726]. **periods** [932, 1372, 1565, 2224, 3410]. **PERK** [3172]. **Perkel** [747]. **Permanent** [781, 1382, 1536]. **Permutation** [344, 693, 896, 917, 923, 1059, 1199, 1326, 1346, 1370, 1416, 1481, 1555, 1579, 1772, 1821, 1842, 2036, 2049, 2091, 2104, 2105, 2171, 2173, 2206, 2235, 2266, 2302, 2315, 2319, 2329, 2381, 2390, 2426, 2438, 2457, 2486, 2494, 2499, 2529, 2638, 2733, 2764, 2808, 2844, 2853, 2862, 2915, 2941, 2951, 2977, 2992, 3009, 3084, 3121, 3138, 3217, 3247, 3318, 3324, 3360, 3456, 3457, 3461]. **permutation-based** [2638]. **Permutations** [23, 199, 340, 876, 882, 896, 939, 1276, 1296,

1313, 1654, 1816, 1900, 1917, 2198, 2263, 2333, 2554, 2559, 2578, 2603, 2620, 2654, 2661, 2672, 2750, 2751, 2806, 3278, 3330, 3341, 3382, 3424]. **permutators** [2396]. **permuted** [3172]. **permuting** [1866]. **perpendicular** [25]. **Personal** [155]. **perspectives** [1208]. **Perturbation** [3366]. **Perturbation-resilient** [3366]. **PG** [635, 636, 667, 1138, 1231, 1431, 1432, 1467, 1788, 2412]. **PGV** [1926]. **phantom** [2562]. **Phase** [2794]. **Phased** [2335]. **physical** [3328]. **physical-layer** [3328]. **Picard** [857]. **Piecewise** [828]. **Pierce** [1174]. **piggledy** [1972]. **piggybacking** [2465]. **Pinch** [2537]. **Piotrowski** [187]. **PIR** [2646]. **Pixels** [552, 892]. **PKC** [2500]. **PKE** [1923, 2256, 2662, 2690, 3116]. **places** [3346]. **plain** [1200]. **Plaintext** [159, 3154]. **Planar** [6, 237, 243, 697, 1427, 1792, 1846, 1909, 1928]. **Plane** [458, 540, 564, 852, 862, 910, 927, 980, 1592, 1641, 1960, 1970, 2083, 2190, 2776, 2803, 2961, 3051, 3193]. **Planes** [6, 8, 93, 118, 120, 132, 147, 151, 201, 226, 232, 237, 348, 370, 387, 417, 422, 438, 457, 555, 592, 611, 632, 633, 674, 697, 708, 728, 921, 985, 1015, 1067, 1117, 1167, 1213, 1220, 1248, 1376, 1468, 1479, 1537, 1540, 1541, 1559, 1642, 1650, 1663, 2121, 2148, 2427, 2441, 2797, 2931, 2956, 3174, 3291, 3300]. **Plateaued** [1500, 1856, 2155, 2278, 2548, 2549, 2946, 3275, 3301]. **Play** [373]. **Player** [774, 1778]. **Pless** [2827, 2839]. **plexes** [1157]. **Plotkin** [1748, 2969]. **Plotkin-optimal** [2969]. **Plücker** [1503]. **PLWE** [3416]. **PLWE-RLWE** [3416]. **PN** [1205, 1809]. **Point** [75, 322, 565, 684, 809, 837, 857, 884, 887, 930, 973, 1045, 1100, 1252, 1267, 1339, 1460, 1518, 1788, 1800, 1812, 1835, 1952, 1953, 2050, 2099, 2184, 2187, 2273, 2283, 2299, 2513, 2590, 2677, 2718, 2820, 2883, 2886, 2888, 3003, 3351, 3446]. **point-distributions** [1339]. **point-imprimitive** [1045, 2677, 2888]. **point-line** [75, 2718]. **Point-missing** [3003]. **point-primitive** [1835, 1953, 2273]. **point-quasiprimitive** [2283]. **point-transitive** [1788]. **Points** [290, 394, 458, 551, 566, 770, 840, 1009, 1065, 1252, 1254, 1289, 1411, 1462, 1499, 1604, 1751, 1818, 1897, 1922, 1959, 1997, 2126, 2353, 2474, 2523, 2595, 2610, 2628, 2803, 2929, 2931, 2953, 3001, 3080, 3220, 3336]. **pointsets** [1988]. **Polar** [186, 390, 397, 446, 681, 700, 960, 1041, 1249, 1433, 1434, 1453, 1549, 1642, 1964, 1994, 2109, 2419, 2971, 3326, 3332–3334, 3336]. **Polarities** [242, 1137, 1213, 1466]. **polarity** [1227, 1638]. **polarizing** [1599]. **policies** [1884]. **Policy** [2009, 2312]. **Policy-based** [2009]. **Polly** [1950]. **polycirculant** [2577]. **Polycyclic** [2799, 2829]. **Polygon** [403, 458, 1435]. **Polygons** [463, 818, 1043, 2117, 2229]. **Polyhedra** [233]. **polymatroid** [2576]. **Polynomial** [42, 148, 416, 444, 553, 608, 705, 831, 909, 966, 1148, 1319, 1403, 1678, 1713, 1728, 2220, 2254, 2261, 2286, 2336, 2404, 2449, 2518, 2542, 2553, 2939, 2964, 3015, 3019, 3091, 3126, 3146, 3176, 3241, 3279, 3303, 3363, 3365]. **polynomial-based** [3015]. **polynomial-reconstruction** [966]. **Polynomial-time** [42, 2254, 2449]. **Polynomials** [37, 143, 213, 371, 503, 625, 719, 736, 870, 932, 1014, 1079, 1258, 1287, 1297, 1315, 1336, 1365, 1405, 1428, 1446, 1494, 1540, 1564, 1605, 1690, 1797, 1865, 1891, 1928, 1945, 2032, 2036, 2065, 2081, 2091, 2154, 2266, 2270, 2302, 2329, 2372, 2390, 2399, 2605, 2692, 2707, 2715, 2764, 2807, 2822, 2825, 2831, 2853, 2924, 2941, 2951, 2990, 3002, 3009, 3084, 3105, 3122, 3136, 3144, 3181, 3256, 3273, 3318, 3331, 3355, 3364, 3434, 3456, 3457]. **Polytopes** [233]. **pomset** [2223, 3037]. **popular** [2616]. **popularity** [2726]. **ports** [2626]. **poset** [1066, 3087]. **posets** [2572, 2814]. **positions** [3056]. **positive** [1823]. **possessing** [3410]. **possibility** [3375]. **Possible** [620, 889, 1439]. **Post** [2563, 2667, 2669, 3013, 3274]. **post-processing** [2563]. **Post-quantum** [2667, 2669, 3013, 3274]. **potent** [2056].

**potentials** [3455]. **PotLLL** [1713]. **Pott** [406]. **Power** [125, 143, 342, 499, 531, 805, 1239, 1296, 1507, 1722, 1888, 1900, 1986, 2136, 2166, 2211, 2267, 2594, 2672, 2673, 2737, 2760, 2821, 2935, 3017, 3177, 3302, 3448]. **power-of-two** [3302]. **Powerful** [115, 1635]. **Powerline** [693]. **powers** [2677]. **Practical** [649, 663, 1122, 1224, 1860, 2310, 2470, 2782, 2786, 2930, 3070, 3395]. **Practical-time** [1860]. **practice** [2899]. **pre** [3459]. **pre-difference** [3459]. **precise** [2824]. **Predicate** [2251, 2501, 3145]. **predicates** [2815]. **Predicting** [1530, 2538, 2968]. **Predistribution** [338, 568, 1511, 1629, 2007]. **Preface** [197, 231, 454, 571, 688, 744, 976, 1056, 1429, 1454, 1469, 2108, 2189, 2344]. **prefer** [2174, 3214]. **prefer-one** [2174, 3214]. **prefer-opposite** [2174]. **preference** [2817, 2903]. **prefix** [3041]. **Preimage** [1698, 3175, 3452]. **Preliminary** [299]. **Preparata** [64, 343, 414, 1264, 2079]. **Preparata-like** [2079]. **Prescribed** [739, 868, 918, 1118, 1502, 1587, 1797, 1996, 2748]. **presemifields** [983, 1080, 2358]. **Presence** [781, 1441]. **PRESENT** [1849]. **PRESENT-like** [1849]. **preserved** [1779]. **Preserving** [369, 543, 871, 1887, 2381, 2696]. **PRF** [3303]. **PRFs** [2381]. **primality** [1890]. **primals** [44]. **primary** [1830, 2763]. **Prime** [4, 42, 125, 226, 277, 342, 531, 811, 840, 863, 994, 1125, 1135, 1235, 1289, 1304, 1376, 1382, 1496, 1526, 1541, 1563, 1767, 1775, 1777, 1797, 1986, 2166, 2180, 2251, 2441, 2533, 2677, 2703, 2775, 2922, 3083, 3345, 3401]. **prime-order** [2251, 2703]. **Primes** [682, 1822, 2430]. **Primitive** [224, 490, 641, 790, 932, 1237, 1287, 1602, 1771, 1835, 1879, 1953, 2002, 2088, 2216, 2273, 2375, 2389, 2429, 2479, 2571, 2741, 2748, 2896, 2940, 3035, 3148, 3438]. **Primitives** [732, 1263, 3145]. **principal** [1103, 2317]. **PRINTcipher** [1743]. **Privacy** [2518, 2696]. **Privacy-preserving** [2696]. **Private** [2303, 2456, 2965, 3026, 3062, 3070]. **Probabilistic** [1014, 2448, 3381]. **Probabilities** [903, 1426, 1756, 1823]. **Probability** [363, 1058, 1297, 1302, 2477, 3280]. **Problem** [94, 158, 263, 436, 518, 584, 607, 632, 753, 798, 880, 1018, 1113, 1175, 1194, 1383, 1639, 1651, 1661, 1864, 1900, 1904, 1956, 2150, 2182, 2231, 2286, 2299, 2414, 2500, 2567, 2866, 2913, 2963, 3015, 3052, 3112, 3172, 3205, 3349, 3363, 3460]. **problem-based** [1194]. **Problems** [217, 1245, 1791, 1838, 1895, 2873, 3165, 3311]. **Procedure** [286]. **procedures** [1090]. **processing** [2563]. **produced** [997]. **Product** [376, 666, 668, 724, 1295, 1399, 1528, 1544, 1599, 1617, 1625, 1901, 1992, 2534, 2789, 3217, 3234]. **products** [10, 1564, 1604, 1690, 2984, 3264, 3279, 3305, 3414]. **Professor** [3021]. **Profile** [249, 870, 2020, 2408]. **profiles** [1653]. **program** [2986]. **programmable** [2295]. **programming** [946, 955, 1003, 1780, 2413, 3036]. **programs** [2909]. **progress** [1233, 1373, 1904, 3002]. **progression** [1156, 2555]. **progression-free** [2555]. **progressions** [2954, 2995]. **progressive** [998]. **projectable** [989]. **projection** [1358, 1945, 2100]. **Projections** [476, 2193, 2825]. **Projective** [6, 8, 106, 147, 151, 196, 201, 243, 265, 381, 387, 390, 417, 438, 443, 529, 534, 540, 542, 555, 582, 632, 728, 807, 909, 910, 916, 975, 981, 1015, 1117, 1128, 1130, 1185, 1242, 1247, 1340, 1397, 1430, 1479, 1489, 1537, 1541, 1642, 1663, 1667, 1709, 1728, 1880, 1945, 1953, 1960, 2121, 2322, 2349, 2393, 2419, 2421, 2427, 2441, 2462, 2466, 2481, 2521, 2633, 2695, 2705, 2848, 2884, 2923, 2931, 2956, 3039, 3131, 3187, 3224, 3310]. **Proof** [7, 393, 486, 520, 584, 720, 747, 751, 799, 1448, 1479, 1553, 2105, 2256, 2485, 2639, 2720, 2852, 3043, 3169]. **Proofs** [1597, 1898, 2310, 2913, 2939, 3046]. **Propagation** [161]. **propelinear** [2280, 2648, 2906]. **Proper** [1160, 1674]. **Properties** [12, 261, 377, 428, 508, 676, 726, 892, 1036, 1042, 1168, 1172, 1269, 1329, 1509,

1700, 1734, 1992, 2128, 2163, 2165, 2228, 2261, 2451, 2493, 2534, 2556, 2694, 2749, 2796, 2899, 2900, 2926, 2962, 3041, 3081, 3183, 3353, 3423]. **Property** [218, 256, 700, 977, 990, 1268, 1623, 1626, 1874, 2028, 2074, 2558, 2644, 2758, 2836, 3033, 3196, 3226]. **proportion** [3025]. **Proposing** [2713]. **Protect** [631]. **Protecting** [2518]. **Protocol** [157, 433, 614, 649, 1034, 1753, 2395, 2915, 3246]. **protocols** [1142, 1521, 3047]. **Provable** [1122, 1624, 2461, 2476, 3115]. **provably** [3196]. **Providing** [621, 1661]. **Proving** [1873, 2608, 3045]. **proximity** [2939]. **proxy** [2312, 3257]. **Pseudo** [460, 545, 983, 1440, 1467, 1550, 1846, 1858, 2504, 3174]. **pseudo-embeddings** [1467, 1550, 2504]. **pseudo-hyperplanes** [1467, 1550]. **pseudo-ovals** [3174]. **Pseudo-Paley** [983]. **pseudo-planar** [1846]. **Pseudo-random** [545, 1858]. **Pseudocodeword** [2324]. **Pseudocodeword-free** [2324]. **Pseudocyclic** [1477]. **Pseudorandom** [870, 1036, 1142, 1216, 1403, 1444, 1530, 1706, 1711, 2747, 2867, 3001, 3028]. **pseudorandomness** [2204]. **PSL** [1432, 2412]. **Public** [137, 144, 154, 193, 222, 430, 445, 607, 663, 704, 762, 798, 966, 1062, 1091, 1200, 1505, 1622, 1891, 1942, 1975, 1990, 2268, 2295, 2516, 2725, 2806, 2873, 3085, 3365, 3403]. **Public-Key** [144, 154, 222, 430, 607, 663, 762, 966, 1622, 1975, 1990, 2268, 3403]. **Publicly** [1724, 2340, 2518, 2868]. **puncturable** [2952]. **punctured** [2624, 3251]. **punctures** [2952]. **Pure** [1167, 3132, 3346]. **putative** [1848]. **Puzzle** [175]. **puzzles** [1701].

**q** [642, 2412, 2865]. **Q2DC** [2928]. **QARMAv1** [3276]. **QARMAv1-** [3276]. **QARMAv2** [3276]. **QARMAv2-64** [3276]. **QC** [2484]. **QGH** [1392]. **QN** [502]. **QN-type** [502]. **QPCBC** [3272]. **QR** [2839]. **QROM** [2704]. **QS** [2794, 2908]. **quad** [1964]. **quadrangle** [1139, 1468, 1943]. **Quadrangles** [24, 517, 565, 645, 866, 942, 1179, 1436, 1448, 1512, 1550, 1655, 2013, 2169, 2812, 2996, 3174]. **Quadratic** [59, 163, 268, 324, 493, 532, 590, 663, 672, 938, 1255, 1362, 1412, 1502, 1654, 1727, 1839, 1930, 2022, 2056, 2106, 2418, 2510, 2559, 2582, 2697, 2787, 2832, 3040, 3062, 3297, 3307, 3397, 3441]. **Quadrature** [536]. **Quadric** [300, 451, 845, 1504, 1532, 2483, 3297, 3361]. **Quadrics** [106, 235, 842, 1533, 1549, 1608, 1640, 3231, 3293]. **quadrinomials** [2494, 2808]. **quadriphase** [1506]. **Quadruple** [11, 67, 86, 134, 164, 187, 273, 291, 333, 1069, 1553, 2073, 2133, 2566, 2656, 3147]. **Quadruples** [81, 775, 838, 2114]. **Qualified** [738, 1152, 1357]. **Quantifying** [1884]. **Quantum** [631, 1552, 1687, 1704, 1717, 1789, 1832, 1870, 1883, 1915, 2096, 2141, 2153, 2181, 2264, 2292, 2300, 2417, 2429, 2543, 2563, 2597, 2599, 2612, 2657, 2658, 2667, 2669, 2675, 2684, 2734, 2754, 2765, 2791, 3011, 3013, 3078, 3082, 3107, 3110, 3113, 3129, 3176, 3204, 3205, 3210, 3272, 3274, 3304, 3313, 3356, 3359, 3414, 3444]. **quantum-secure** [3272]. **quartic** [1879, 1963, 2763]. **Quasi** [20, 30, 31, 39, 71, 116, 117, 142, 167, 409, 441, 448, 520, 548, 604, 616, 617, 654, 852, 854, 911, 926, 934, 947, 1093, 1137, 1281, 1283, 1286, 1307, 1329, 1375, 1404, 1508, 1609, 1670, 1774, 1844, 1882, 1973, 1990, 2431, 2444, 2473, 2772, 2780, 2834, 2860, 2865, 2980, 2981, 3171, 3252, 3263, 3316, 3339, 3378, 3379, 3444]. **Quasi-** [409, 3171]. **Quasi-abelian** [1774, 2834]. **Quasi-affine** [947]. **quasi-complementary** [3263, 3316]. **Quasi-Cyclic** [31, 167, 441, 654, 852, 854, 1281, 1329, 1375, 1508, 1609, 1670, 1973, 1990, 2772, 2860, 3252, 3339, 3378, 3379, 3444]. **quasi-Feistel** [1283]. **Quasi-Frobenius** [448]. **quasi-Galois** [2980]. **Quasi-Multiple** [520]. **quasi-orthogonal** [2444]. **quasi-perfect** [911, 1093, 1307, 2865]. **Quasi-Symmetric** [20, 30, 39, 71, 116, 117, 142, 520, 604, 616, 617,

926, 934, 1137, 1286, 1404, 1882, 2780]. **Quasi-Twisted** [548, 1844, 2431, 2473]. **Quasideterminant** [310]. **quasidivisible** [1965]. **quasifields** [1647]. **Quasigroups** [36, 815, 825, 1052, 1445]. **quasiprimitive** [1542, 2283]. **quasiregular** [8]. **Quaternary** [88, 167, 723, 839, 1186, 1281, 1309, 1310, 1384, 1585, 1687, 1717, 1929, 2026, 2233, 2614, 2722, 2775, 2778, 2958, 2959, 2972, 3210, 3226]. **Quaternion** [824, 2301, 3230]. **quaternionic** [3190]. **Question** [55, 406]. **questions** [2799]. **Quintic** [717]. **Quotient** [830]. **Quotients** [1437, 1524].

**R** [1513]. **Rabin** [314, 359]. **Rabin-type** [359]. **Rabin-Williams** [314]. **Rackoff** [876, 2720]. **Radii** [72, 418, 507, 943, 1356]. **Radius** [3, 40, 192, 224, 302, 316, 357, 603, 727, 772, 917, 1026, 1061, 1209, 1307, 1555, 1651, 2044, 2183, 2466, 2865, 3178, 3191]. **Rado** [1642, 1658, 1819, 2345]. **rainbow** [1273]. **Ramanujan** [2505]. **Random** [327, 545, 917, 1095, 1106, 1262, 1444, 1573, 1858, 1894, 1939, 2396, 2519, 2531, 3280, 3357]. **randomisation** [3058]. **randomization** [2612, 2988]. **Randomizers** [160]. **Randomness** [264, 2203, 2666]. **range** [2999]. **ranges** [2984]. **Rank** [49, 54, 114, 149, 467, 490, 598, 677, 680, 841, 899, 1082, 1118, 1236, 1347, 1382, 1465, 1475, 1594, 1612, 1755, 1835, 1964, 1969, 1983, 2093, 2103, 2129, 2134, 2149, 2176, 2194, 2196, 2258, 2274, 2280, 2285, 2339, 2353, 2365, 2406, 2436, 2475, 2507, 2516, 2517, 2527, 2536, 2576, 2583, 2591, 2592, 2615, 2621, 2636, 2679, 2785, 2832, 2920, 2964, 3039, 3052, 3065, 3108, 3112, 3124, 3349, 3396, 3418, 3438]. **rank-based** [2516]. **rank-distance** [2527]. **Rank-metric** [1983, 2176, 2517, 2679, 2785, 3065]. **Rankin** [20, 3446]. **Ranks** [124, 594, 665, 719, 1663, 2008, 2026]. **Rao** [1830, 2277, 2330]. **Rate** [146, 167, 225, 257, 510, 1308, 1595, 1609, 2942, 3061, 3360]. **Rate-improved** [3360]. **rates** [3149]. **ratio** [1692, 2382, 2798]. **Rational** [263, 277, 458, 739, 874, 1217, 1398, 1570, 1897, 1959, 2102, 2240, 2509, 2529, 2595, 2862, 3032, 3138, 3220, 3266, 3346, 3425]. **RC4** [1068, 1083, 1873, 2048, 2215, 2625]. **re** [1845, 2312, 3257]. **re-encryption** [2312, 3257]. **re-evaluation** [1845]. **reaching** [2327]. **Real** [163, 2668, 3040, 3416]. **realizability** [1130]. **Realization** [367, 1595]. **realizing** [1960]. **Receiver** [478, 2945]. **receivers** [2383, 3145]. **Reciprocal** [736, 858, 2270, 2822]. **Reconciliation** [649]. **Reconstructed** [552]. **reconstructing** [2198]. **Reconstruction** [328, 892, 966, 3167, 3278]. **records** [3070]. **Recoverable** [2599, 2600, 2605, 2714, 2783, 2958, 2984, 3208, 3259, 3283, 3339, 3415, 3445]. **Recovery** [158, 1728, 1743, 2243, 2254, 2600, 2762, 2786, 2823, 3238, 3283, 3288, 3378]. **rectangle** [2539, 3304]. **Rectangles** [125, 1008, 1144, 1857]. **Rectilinear** [466]. **recurrence** [1820]. **recurring** [2894]. **recursions** [1092]. **Recursive** [296, 776, 1075, 1335, 1734, 2045, 2051, 2095, 2241, 2368, 2390, 2469, 2538, 2804, 2968, 2980, 3147]. **recursively** [3105]. **Redefining** [2046]. **Rédei** [2390, 2578]. **reduce** [3069]. **Reduced** [535, 1596, 1860, 2094, 2214, 2248, 2530, 2823, 3049, 3175, 3288, 3352]. **reduced-round** [1596, 2214, 2823, 3049, 3175, 3288]. **reducibility** [1258, 1446]. **reducible** [1300, 1425, 1594, 1859]. **Reducing** [314, 1017, 3375]. **Reduction** [716, 960, 1106, 1237, 1939, 2010, 2011, 2128, 2231, 2552, 3068, 3115, 3248, 3363, 3406]. **reductions** [1602, 1771, 1825]. **Redundancy** [335, 1184]. **Redundant** [162, 932, 1290]. **Ree** [228, 290, 790, 1027, 1044]. **Reed** [28, 40, 72, 165, 275, 467, 507, 529, 582, 948, 952, 1064, 1072, 1097, 1202, 1210, 1498, 1556, 1558, 1620, 1682, 1707, 1709, 1723, 2183, 2393, 2421, 2438, 2446, 2515, 2581, 2617, 2627, 2633, 2709, 2717,

2758, 2861, 2874, 2901, 2966, 3059, 3071, 3098, 3122, 3155, 3181, 3185, 3224, 3310, 3394, 3423]. **Reflection** [97, 2040]. **Reflections** [1896]. **reflexive** [1824]. **Regev** [2873]. **Register** [91, 682, 1581, 1740, 2041]. **Registers** [682, 1287, 1810, 2070, 2085, 2092, 2509]. **Regular** [22, 55, 85, 179, 182, 255, 294, 395, 464, 468, 565, 706, 746, 748, 844, 877, 1043, 1048, 1169, 1215, 1331, 1366, 1457–1459, 1462, 1510, 1580, 1588, 1648, 1921, 1930, 1962, 2112, 2113, 2115, 2127, 2169, 2185, 2229, 2287, 2424, 2425, 2443, 2546, 2631, 2764, 2872, 2917, 2979, 2993, 3009, 3016, 3064, 3140, 3160, 3200, 3217, 3270, 3363, 3380, 3398]. **Regularity** [752, 2627, 3441]. **regularly** [1952]. **Reguli** [700, 844]. **Regulus** [174]. **Regulus-free** [174]. **Reingold** [545, 2336]. **Reisner** [1669]. **Related** [105, 116, 165, 233, 348, 413, 492, 577, 635, 737, 803, 824, 886, 979, 1028, 1135, 1199, 1278, 1300, 1305, 1311, 1333, 1420, 1433, 1442, 1495, 1549, 1719, 1822, 1846, 1848, 1873, 2059, 2115, 2133, 2150, 2185, 2234, 2314, 2330, 2354, 2390, 2391, 2485, 2539, 2700, 2839, 2927, 2959, 2993, 3072, 3080, 3148, 3160, 3216, 3298]. **related-key** [1311, 1333, 2539]. **Relating** [428, 1306, 3311]. **relation** [1516, 1625, 1696, 2286, 2473, 2903]. **Relations** [51, 1166, 1326, 1750, 1820, 2663, 2947]. **Relationship** [650, 1459]. **Relative** [10, 139, 185, 266, 294, 345, 404, 605, 665, 780, 864, 1057, 1147, 1569, 1652, 1653, 1660, 1697, 1796, 1802, 2013, 2111, 2356, 2547, 2553, 3173, 3195]. **relatively** [2141]. **relatives** [2446]. **release** [2177]. **remaining** [2899]. **remark** [22, 1559]. **Remarks** [6, 226, 643, 695, 949, 1129, 1638, 2481]. **Reminiscence** [155]. **repair** [2462, 3243]. **repairability** [2186]. **repairable** [2199, 2800, 3134, 3198, 3212, 3251]. **repeated** [854, 999, 1235, 1670]. **repeated-root** [999]. **Repetition** [2625, 3160]. **Replacement** [511, 980, 1067]. **replication** [2533, 2922]. **Representation** [550, 624, 647, 933, 948, 1257, 1308, 1593, 1827, 2050, 2097, 2509, 2590, 2626, 3429]. **Representations** [162, 215, 608, 888, 940, 1004, 1164, 1399, 1871, 2435, 2542, 3146]. **reprint** [188, 189]. **repudiation** [808]. **Required** [264]. **Requirements** [157]. **research** [1903]. **Residually** [641]. **residuals** [90]. **Residue** [444, 938, 1811, 2379, 2832]. **residues** [3062]. **residuosity** [2630]. **Resilience** [1701, 2661]. **resiliency** [3028]. **Resilient** [130, 279, 365, 613, 1447, 2004, 2159, 2251, 2423, 2471, 2478, 2690, 2771, 2789, 3055, 3149, 3366]. **Resistance** [285, 766]. **resistant** [1342, 2942]. **Resmini** [1514]. **Resolution** [1669, 3002, 3399]. **Resolutions** [593, 1069, 2241]. **resolvability** [1269]. **Resolvable** [86, 252, 258, 581, 711, 774, 775, 931, 1053, 1218, 1256, 2121, 2133, 2320, 2469, 2536, 2566, 2647, 2656, 2855, 3003, 3069, 3147, 3232, 3289]. **Resource** [878]. **Respect** [715, 757, 834, 1220, 1743, 2617, 3087, 3094, 3217, 3361, 3401]. **Restricted** [628, 1368, 1434, 1925, 2355, 2780, 3103, 3309]. **restrictions** [1439, 2972]. **Result** [98, 610, 938, 993, 1190, 1220, 1343, 1410]. **Results** [60, 72, 331, 355, 558, 635, 653, 748, 772, 1088, 1104, 1212, 1270, 1285, 1353, 1363, 1427, 1496, 1519, 1520, 1562, 1587, 1659, 1736, 1771, 1814, 1897, 1959, 2002, 2091, 2115, 2328, 2341, 2458, 2476, 2491, 2522, 2897, 3012, 3191, 3335, 3372, 3381, 3461]. **Retracted** [2920]. **Retraction** [3289]. **retransmission** [1481]. **retrieval** [2197, 2456]. **retrospective** [1894]. **Reusable** [2308, 2666]. **reveal** [1757]. **reverse** [3105, 3370, 3431]. **reverse-complement** [3431]. **Reversible** [2863, 3440]. **Review** [100, 481, 1122, 2857]. **revised** [3371]. **Revisited** [187, 876, 965, 1491, 1498, 1627, 1701, 1752, 1950, 2132, 2471, 2508, 2725, 2886, 2975, 3453]. **Revisiting** [1696, 2048, 2586, 3052, 3279]. **Revocable** [2145, 2303, 2689, 2704].

**Revocation** [762, 1151]. **rewinding** [2136]. **RFID** [1142]. **Richard** [1469]. **Rick** [1470]. **Riemann** [3215]. **Right** [1085, 1647]. **Rights** [190]. **rigidity** [97]. **Rigorous** [584]. **Rijndael** [2047, 2087]. **Rijndael-160** [2047]. **Rijndael-224** [2047]. **Ring** [319, 367, 442, 526, 566, 893, 999, 1048, 1112, 1401, 1488, 1489, 1747, 2226, 2257, 2323, 2560, 2669, 2752, 2851, 2918, 2919, 2980, 3077, 3458]. **ring-like** [2323]. **ring-linear** [1489]. **Ring-Valued** [566]. **Rings** [185, 236, 448, 514, 525, 543, 569, 654, 789, 874, 936, 954, 955, 974, 1001, 1003, 1103, 1131, 1238, 1265, 1375, 1381, 1495, 1507, 1541, 1601, 1617, 1676, 1678, 1688, 1699, 1738, 1794, 1855, 2085, 2291, 2296, 2317, 2379, 2480, 2520, 2526, 2568, 2636, 2650, 2691, 2732, 2828, 2921, 3086, 3091, 3123, 3150, 3176, 3195, 3224, 3296, 3302, 3432, 3445]. **RIPEMD** [2530]. **RIPEMD-160** [2530]. **rise** [3051]. **risk** [2470]. **River** [2248]. **RKA** [1326, 2256]. **RKA-secure** [1326]. **RLWE** [3416]. **Robust** [339, 779, 2407, 3435]. **Robustly** [2666]. **Roch** [3215]. **Roesser** [1595]. **ROLLO's** [3099]. **Ronald** [571]. **Room** [426, 1626]. **Roos** [2048]. **Root** [330, 999, 1022, 1124, 1383, 1670, 1820, 2182, 3164, 3417]. **Roots** [563, 608, 625, 686, 854, 1014, 2103]. **Rosenbloom** [834]. **rotation** [1418, 1616, 1834, 2582, 2618]. **rotational** [1373, 3033, 3373]. **rotational-XOR** [3373]. **Rothaus** [2960]. **Rötteler** [2966]. **Roulette** [2650]. **Round** [284, 1171, 1413, 1596, 1696, 1998, 2012, 2094, 2214, 2248, 2530, 2720, 2752, 2823, 3049, 3073, 3171, 3175, 3197, 3288, 3352, 3452]. **Round-efficient** [1413]. **round-optimal** [2752]. **round-reduced** [2094, 2248, 2530, 3352]. **rounds** [3118]. **Roux** [915]. **Roux-type** [915]. **row** [96]. **row-cyclic** [96]. **rows** [1880, 2755]. **RQC** [2852]. **RSA** [497, 521, 836, 868, 1312, 1496, 1715, 2071, 3070, 3345]. **RSA-Type** [521]. **ruled** [2521]. **Rules** [536]. **run** [1059]. **run-length** [1059]. **runs** [2460]. **Ruprai** [2363]. **Russian** [1661]. **Ruud** [2589]. **RYDE** [3349].

**S** [586, 601, 939, 1447, 2087, 2558, 2616, 2796, 3053, 3242, 3450]. **S-box** [2616]. **S-Boxes** [601, 939, 1447, 2087, 2558, 2796, 3053, 3242]. **S.** [55]. **Sahai** [2310]. **Salsa** [2608]. **Salsa20** [3288]. **Same** [219, 2167, 2323, 2578, 3370]. **sampler** [2971]. **sampling** [2452, 2971]. **SASCA** [3378]. **Satisfying** [161, 336, 700, 977, 1395, 1695, 2947]. **saturating** [2466, 2884]. **SBIBDs** [518]. **scalable** [2667]. **scalar** [1290, 3258]. **SCARF** [3352]. **Scattered** [2700]. **schedule** [1696, 2539]. **Scheduling** [694, 2048, 3069]. **Scheme** [77, 126, 270, 359, 445, 563, 762, 783, 823, 848, 876, 892, 1054, 1151, 1153, 1200, 1328, 1342, 1413, 1614, 1624, 1635, 1845, 1939, 1989, 2005, 2009, 2066, 2090, 2111, 2254, 2456, 2475, 2570, 2615, 2665, 2690, 2765, 2816, 2868, 3013, 3080, 3172, 3197, 3223, 3349]. **Schemes** [53, 92, 146, 158, 160, 220, 221, 257, 261, 264, 280, 293, 338, 354, 361, 376, 390, 413, 453, 461, 519, 530, 544, 552, 560, 568, 570, 576, 619, 621, 672, 691, 699, 734, 735, 738, 749, 777, 867, 891, 902, 904, 913, 1113, 1152, 1214, 1223, 1322, 1357, 1360, 1417, 1430, 1477, 1511, 1543, 1600, 1611, 1629, 1692, 1736, 1737, 1773, 1780, 1846, 1920, 1921, 1940, 1982, 2007, 2144, 2186, 2217, 2232, 2285, 2382, 2401, 2440, 2472, 2553, 2630, 2702, 2711, 2811, 2873, 3048, 3111, 3158, 3242, 3270, 3336, 3403]. **Schmidt** [2449, 3317]. **Schnorr** [2428]. **Schreier** [3220]. **Schubert** [729, 2326]. **Schur** [514, 793, 2534, 3195]. **Schurian** [2126]. **Scientific** [2857]. **Scott** [1171, 1876]. **Scroll** [1010, 1425]. **scrolls** [2421]. **SDP** [20, 782]. **SE** [2256]. **Search** [460, 998, 1633, 1634, 1838, 1844, 1883, 2011, 2431, 2824, 3137, 3153]. **searchable** [2340]. **searching** [3373, 3450]. **secant** [3361]. **Second** [467, 1072, 1097, 1100, 1707, 1831, 2277, 2330, 2446, 2857]. **secondary**

[2548, 2730, 2768, 2934]. **Secrecy** [133, 160, 293, 733, 1321, 1757, 2272, 2420, 2826, 3218]. **Secret** [53, 68, 92, 126, 146, 160, 220, 257, 261, 264, 280, 328, 354, 361, 453, 497, 521, 530, 560, 621, 647, 738, 892, 900, 902, 913, 1083, 1152, 1153, 1190, 1280, 1357, 1360, 1390, 1408, 1417, 1430, 1692, 1715, 1724, 1736, 1773, 1786, 1901, 2005, 2177, 2382, 2401, 2407, 2472, 2612, 2626, 2710, 2711, 2811, 2868, 2949, 2970, 2979, 2999, 3117, 3197, 3253, 3299, 3378, 3453]. **secret-keys** [1901]. **secret-sharing** [1430, 1692]. **Secrets** [867, 1160, 1635, 2612]. **Sections** [301, 512]. **Secure** [91, 282, 283, 332, 337, 576, 621, 1006, 1034, 1224, 1326, 1413, 1853, 1901, 1913, 1974, 1975, 2062, 2078, 2204, 2217, 2256, 2268, 2275, 2312, 2331, 2381, 2395, 2570, 2662, 2689, 2704, 2806, 2988, 3027, 3074, 3085, 3117, 3169, 3272, 3348]. **securing** [3447]. **Security** [154, 430, 449, 575, 619, 704, 735, 906, 945, 1095, 1122, 1145, 1194, 1225, 1272, 1441, 1443, 1661, 1698, 1767, 1787, 1845, 1884, 1895, 1920, 1939, 1949, 2078, 2089, 2203, 2209, 2210, 2321, 2383, 2396, 2461, 2470, 2476, 2585, 2612, 2615, 2638, 2665, 2669, 2690, 2701, 2704, 2720, 2749, 2766, 2770, 2781, 2795, 2813, 2936, 2945, 3013, 3029, 3073, 3111, 3145, 3171, 3223, 3233, 3242, 3303, 3313, 3328, 3453]. **security-risk** [2470]. **SEEDs** [1731, 1734]. **Segre** [1138, 1387, 1397, 1479, 1504]. **Seidel** [455, 2124]. **selection** [2807]. **selective** [2383, 2585, 2945, 3145, 3348]. **selective-opening** [3145]. **Self** [14, 42, 83, 90, 142, 204, 209, 253, 259, 271, 306, 347, 415, 500, 523, 526, 527, 535, 551, 574, 604, 617, 618, 691, 703, 727, 736, 829, 833, 839, 858, 919, 929, 934, 943, 1051, 1112, 1132, 1155, 1159, 1274, 1291, 1355, 1370, 1371, 1381, 1412, 1419, 1438, 1552, 1601, 1666, 1673, 1691, 1731, 1745, 1770, 1783, 1806, 1816, 1848, 1941, 1942, 1944, 2141, 2142, 2234, 2245, 2270, 2291, 2343, 2445, 2540, 2561, 2593, 2668, 2675, 2676, 2691, 2717, 2753, 2757, 2791, 2825, 2837, 2838, 2918, 2927, 2955, 2972, 3011, 3064, 3110, 3133, 3150, 3162, 3210, 3236, 3440]. **self** [89, 1001, 1007, 1060, 1120, 1402, 1436, 1523, 1560, 1582, 1717, 1742, 1764, 1777, 1805, 1937, 2019, 2100, 2307, 2493, 2560, 2659, 2919, 2960, 2980, 3006, 3076, 3086, 3209, 3234, 3241]. **Self-Complementary** [90, 604, 934]. **Self-conjugacy** [347]. **Self-Dual** [83, 89, 142, 209, 253, 259, 271, 306, 415, 500, 523, 526, 527, 535, 551, 574, 617, 618, 703, 727, 829, 833, 839, 919, 929, 943, 1001, 1007, 1051, 1060, 1120, 1132, 1155, 1159, 1274, 1291, 1355, 1370, 1371, 1381, 1402, 1419, 1436, 1438, 1523, 1560, 1582, 1601, 1666, 1673, 1691, 1731, 1742, 1745, 1764, 1770, 1777, 1783, 1806, 1848, 1937, 1941, 1944, 2019, 2100, 2142, 2234, 2245, 2291, 2307, 2343, 2445, 2493, 2540, 2560, 2593, 2659, 2668, 2676, 2691, 2717, 2753, 2757, 2825, 2838, 2927, 2955, 2960, 2972, 2980, 3006, 3076, 3086, 3110, 3150, 3162, 3210, 3234, 3236, 3241]. **self-dual** [1805]. **Self-embeddings** [1816]. **Self-Healing** [691]. **Self-Orthogonal** [14, 204, 703, 833, 1112, 1552, 1717, 2141, 2561, 2675, 2791, 2837, 2918, 2919, 2980, 3011, 3064, 3086, 3133, 3209]. **Self-Reciprocal** [736, 858, 2270]. **Self-reversible** [3440]. **Self-updatable** [1942]. **Self-witnessing** [42]. **Semantic** [1095, 2210]. **Semi** [85, 255, 294, 850, 1351, 1762, 1992, 2479, 2530, 2742, 2795, 2854, 3398]. **semi-adaptive** [2795]. **Semi-bent** [850, 2742]. **Semi-cyclic** [1762]. **semi-direct** [1992]. **semi-free-start** [2530]. **semi-free-start/near-** [2530]. **semi-linear** [2854]. **Semi-Pappus** [1351]. **semi-primitive** [2479]. **Semi-Regular** [85, 255, 294, 3398]. **semibent** [1277, 1388]. **semibiplanes** [1250]. **Semicyclic** [1420]. **Semidefinite** [2114, 2413, 3036]. **semidirect** [3205]. **Semifield** [661, 1559, 1984, 2453, 2914, 3300]. **Semifields** [793, 982, 984, 1205, 1347, 1358, 1359, 1427, 1540, 1548, 1683, 1927, 1945, 2088, 2134, 2208, 2978, 3104]. **Semigroup** [2010, 2595]. **Semigroups** [830, 1184, 1499, 2277, 2330, 2929, 3132].

**semiovals** [1650]. **Semipartial** [696, 700, 1039]. **semiprimitive** [2989]. **Semiregular** [412, 780, 3173]. **Semisimple** [1561, 1868]. **semisymmetric** [3323]. **sense** [2503, 2574, 2741, 3421]. **sensor** [1511, 1629]. **separable** [1066, 1348, 1595, 1749, 1951, 2024, 2135, 2623]. **Separating** [928, 1575, 1685, 1974, 2012, 2052, 2758]. **separation** [2607, 3261]. **Sequence** [51, 104, 723, 930, 992, 1129, 1142, 1186, 1304, 1309, 1310, 1384, 1566, 1700, 1932, 2082, 2156, 2512, 2739, 2775, 2794, 2907, 2908, 2932, 2933, 2957, 3188, 3263, 3278, 3316, 3370]. **Sequences** [32, 45, 59, 84, 110, 177, 189, 218, 249, 268, 305, 374, 406, 509, 550, 567, 596, 639, 726, 843, 912, 924, 949, 997, 1017, 1047, 1059, 1092, 1126, 1168, 1182, 1187, 1217, 1268, 1298, 1323, 1334, 1335, 1341, 1361, 1367, 1394, 1403, 1423, 1451, 1506, 1524, 1525, 1602, 1615, 1665, 1694, 1705, 1706, 1711, 1740, 1750, 1765, 1771, 1785, 1797, 1798, 1874, 1912, 1925, 1993, 2020, 2137, 2162, 2164, 2168, 2174, 2231, 2250, 2259, 2304, 2372, 2374, 2402, 2403, 2451, 2454, 2511, 2588, 2651, 2652, 2694, 2817, 2864, 2894, 2903, 2955, 3030, 3143, 3188, 3214, 3317, 3328, 3329, 3370, 3389, 3398, 3410, 3429]. **sequences** [2442]. **sequencings** [14, 2820]. **Sequential** [957, 2012, 3050, 3152]. **Ser** [55]. **serial** [1800]. **serial-in-serial-out** [1800]. **Series** [13, 187, 789, 877, 1748, 2014, 2191, 2927, 3003, 3040, 3307, 3441]. **Servers** [190, 2456]. **service** [3366]. **sESTATE** [2684]. **Set** [46, 63, 522, 840, 1140, 1183, 1534, 1566, 1632, 1751, 1804, 1952, 1997, 2038, 2119, 2453, 2551, 2611, 2623, 2833, 2937, 3026, 3046, 3309, 3346, 3385, 3439]. **Sets** [70, 108, 114, 125, 151, 171, 185, 195, 199, 226, 241, 245, 255, 266, 273, 294, 304, 305, 318, 341, 347, 370, 377, 383, 392, 398, 404, 412, 413, 439, 446, 448, 452, 456, 474, 487, 504, 528, 534, 539, 569, 585, 592, 605, 609, 612, 630, 633, 638, 651, 665, 667, 684, 697, 714, 718, 719, 722, 731, 780, 803, 811, 864, 886, 902, 944, 1029, 1046, 1064, 1185, 1191, 1248, 1290, 1409, 1455, 1533, 1537, 1591, 1778, 2080, 2082, 2084, 2125, 2255, 2334, 2356, 2368, 2410, 2645, 2719, 2723, 2761, 2858, 3008, 3051, 3254, 3297, 3361]. **sets** [6, 10, 23, 26, 27, 29, 85, 103, 139, 181, 345, 914, 960, 971, 983, 988, 1002, 1021, 1037, 1076, 1104, 1111, 1119, 1141, 1162, 1164, 1176, 1220, 1239, 1242–1244, 1252, 1259, 1288, 1289, 1367, 1384, 1507, 1544, 1565, 1642, 1655, 1658, 1665, 1675, 1677, 1697, 1700, 1735, 1818, 1819, 1856, 1931, 1932, 1962, 1985, 2021, 2140, 2161, 2191, 2207, 2239, 2252, 2294, 2332, 2347, 2378, 2397, 2437, 2443, 2466, 2517, 2521, 2555, 2642, 2644, 2671, 2693, 2735, 2767, 2773, 2882, 2884, 2890, 2897, 2907, 2917, 2985, 3012, 3030, 3173, 3179, 3182, 3195, 3262, 3263, 3316, 3320, 3335, 3366, 3459]. **sets** [1050, 1212, 1268, 2072, 2156, 2166, 2309, 2794, 2908]. **Setting** [735, 2570, 2684, 2945, 3352]. **setup** [3044, 3428]. **seven** [2818]. **Several** [732, 770, 1172, 2332, 2494, 2905, 2929, 2934, 2993, 3023, 3072, 3145, 3314, 3343, 3346, 3354]. **Severely** [137]. **SFLASH** [1728]. **SHA** [1318]. **SHA-1** [1318]. **Shannon** [1487, 2110, 2228, 2417]. **sharding** [3169]. **Shared** [328, 339, 1263, 2588, 2915, 3378]. **Shares** [762]. **Sharing** [53, 68, 77, 92, 126, 146, 160, 220, 257, 261, 264, 280, 354, 361, 453, 530, 560, 621, 647, 738, 867, 892, 900, 902, 913, 1152, 1153, 1190, 1280, 1357, 1360, 1390, 1408, 1417, 1430, 1692, 1724, 1736, 1773, 1786, 2005, 2177, 2312, 2382, 2401, 2407, 2472, 2612, 2626, 2710, 2711, 2811, 2868, 2949, 2970, 2979, 2999, 3117, 3253, 3299, 3453]. **sharp** [1398, 2405, 2600]. **sharpening** [64]. **Sharper** [2809]. **sharply** [23]. **sharpness** [1675]. **Shen** [961]. **Shift** [91, 131, 218, 682, 1287, 1581, 1740, 1810, 2041, 2070, 2085, 2092, 2509, 2511, 2619, 3281]. **Shift-inequivalent** [2511]. **shift-register** [1581]. **Shiftable** [3454]. **Short** [608, 1235, 1299, 1399, 1465, 1767, 1864, 1901, 1942, 2011, 2516, 2552, 2563, 2646, 2973, 2988, 3085]. **shortened** [1266, 1320, 1450, 1558]. **Shorter**

[1342, 1739, 2000, 2303]. **shortest** [1883, 2085]. **shot** [2194]. **show** [1398]. **Shrinking** [508]. **shuffle** [2991]. **Side** [908, 1573, 3369]. **side-channel** [1573]. **Sidelnikov** [639, 843, 912, 1304, 1785, 2442, 2451, 2511]. **Sides** [1085]. **SIDH** [3158]. **SIDH-like** [3158]. **Sidon** [2891, 2943, 3244]. **Sierpiński** [1562]. **Sieve** [416, 3419]. **sieving** [3356]. **Signal** [446, 2294]. **Signature** [158, 359, 519, 563, 575, 619, 651, 660, 672, 735, 836, 945, 1134, 1200, 1223, 1293, 1920, 2009, 2057, 2160, 2260, 2433, 2489, 2516, 2609, 2667, 2712, 2845, 2915, 3111, 3172, 3349, 3403]. **Signatures** [893, 1229, 1312, 1337, 1864, 1869, 1887, 1975, 2295, 2384, 2428, 2508, 2669, 2782, 2795, 2913, 2930, 2973, 2987, 3237, 3345, 3392, 3458]. **Signcryption** [808, 1600, 1624]. **Signed** [267, 272, 402, 940, 2497, 2739, 2985, 3146, 3182]. **signed-digit** [2739, 3146]. **Significance** [567]. **significant** [1270]. **SIMD** [1610]. **SIMECK** [2713]. **similarities** [3322]. **Simmon** [720]. **SIMON** [2094, 2702]. **Simple** [7, 207, 334, 491, 872, 1114, 1300, 1379, 1522, 1556, 1626, 1662, 1854, 1859, 2095, 2241, 2392, 2428, 2533, 2697, 2987, 3154, 3284]. **Simplectic** [982]. **Simplex** [266, 1488, 1793, 2592, 2624, 2962, 3125, 3251, 3362]. **simplicial** [1679, 2293, 3213]. **Simplicity** [2898]. **Simulation** [2383, 2765]. **Simulation-based** [2383]. **simulators** [2136]. **Simultaneous** [1967, 2331, 3062]. **Singer** [612, 695, 731, 862, 866, 1287, 1431]. **Singhi** [2249, 2388]. **Single** [57, 88, 941, 1052, 2089, 2261, 2319, 2381, 2579, 2977, 3099, 3167, 3352, 3360, 3379]. **single-deletion-correcting** [2579]. **single-error** [941]. **single-error-correcting** [88]. **single-orbit** [3379]. **single-permutation** [2319]. **single-trace** [3099]. **Singleton** [2402, 2403]. **Singly** [191, 209]. **Singly-Even** [191, 209]. **singular** [12, 1251, 1640, 2483]. **Six** [460, 595, 1515, 1861, 2541]. **six-weight** [1861]. **sixty** [2776]. **sixty-four** [2776]. **Size** [60, 73, 121, 145, 150, 244, 254, 258, 287, 311, 366, 498, 573, 577, 587, 737, 743, 835, 931, 1045, 1061, 1158, 1198, 1204, 1227, 1233, 1253, 1278, 1297, 1300, 1313, 1364, 1380, 1423, 1455, 1606, 1658, 1759, 1762, 1859, 1936, 2027, 2098, 2463, 2477, 2484, 2551, 2866, 3018, 3026, 3178, 3254, 3319]. **Sized** [572]. **Sizes** [129, 240, 648, 786, 811, 941, 1023, 1218, 1256, 1449, 1644, 1754, 2166, 2247, 2297, 2525, 3088, 3094, 3142, 3250, 3298, 3396, 3443]. **Skeleton** [1679]. **Skew** [108, 298, 983, 1084, 1104, 1118, 1176, 1375, 1581, 1605, 1678, 2103, 2163, 2617, 3066, 3091, 3098, 3157, 3162, 3216, 3350, 3367]. **skew-feedback** [1581]. **Skew-Hadamard** [298]. **SKINNY** [2539, 3107, 3400]. **Skolem** [1423]. **Skolem-type** [1423]. **slide** [1896]. **Sliding** [950]. **Sliding-window** [950]. **Slim** [818]. **Small** [229, 248, 334, 452, 513, 590, 592, 684, 701, 807, 916, 932, 942, 995, 1015, 1155, 1251, 1252, 1356, 1411, 1512, 1533, 1534, 1582, 1618, 1715, 1718, 1781, 1812, 1816, 1818, 1905, 1912, 1976, 2064, 2125, 2360, 2479, 2523, 2536, 2714, 2835, 3006, 3070, 3174, 3187, 3241, 3243]. **small-block** [1781]. **small-minimum-distance** [1618]. **smaller** [2975]. **smallest** [1091, 1409, 1462, 1639, 2484]. **Smartcard** [859]. **Smith** [39, 298, 2130]. **smooth** [1504]. **smoothing** [2531, 3406]. **Snake** [2093, 2507]. **Snake-in-the-box** [2093, 2507]. **snakes** [1064]. **SNOW** [2569, 2824, 2982, 3153]. **SNOW-V** [2824]. **SO-CCA** [2662]. **socle** [2034, 3057]. **software** [2058]. **software-implemented** [2058]. **Sok** [3047]. **Solomon** [28, 952, 1556, 1558, 1620, 1723, 2393, 2438, 2581, 2617, 2709, 2717, 2758, 2861, 2874, 2901, 2966, 3071, 3098, 3185, 3423]. **Solution** [94, 263, 753]. **solutions** [1661, 1720]. **solvable** [1563]. **Solving** [1078, 1085, 2178, 2231, 2286]. **Some** [6, 25, 40, 71, 86, 99, 199, 227, 229, 232, 267, 269,

282, 331, 350, 355, 364, 370, 388, 402, 408, 409, 418, 483, 502, 508, 532, 638, 643, 653, 664, 687, 698, 707, 737, 748, 755, 788, 799, 826, 843, 849, 875, 936, 972, 1029, 1073, 1104, 1136, 1143, 1211, 1243, 1245, 1270, 1317, 1349, 1373, 1442, 1446, 1643, 1644, 1650, 1651, 1659, 1704, 1890, 1934, 1982, 1991, 2049, 2091, 2163, 2244, 2294, 2328, 2468, 2481, 2543, 2641, 2658, 2673, 2728, 2734, 2811, 2916, 2964, 2972, 2976, 2993, 3002, 3004, 3162, 3212, 3222, 3234, 3395, 3448]. **some** [1070, 1117, 1197, 1510, 1613, 1730, 1836, 1908, 1970, 1987, 2003, 2015, 2020, 2070, 2185, 2220, 2237, 2405, 2418, 2461, 2498, 2614, 2792, 2810, 2962, 3205, 3387]. **Something** [155, 484]. **Somewhat** [3357]. **Sophie** [1822]. **Space** [361, 381, 466, 696, 909, 922, 935, 1053, 1181, 1198, 1433, 1435, 1455, 1465, 1534, 2043, 3007, 3151, 3231, 3294]. **space-time** [935]. **Spaces** [19, 49, 186, 196, 212, 217, 243, 250, 387, 390, 397, 461, 467, 513, 534, 539, 542, 588, 606, 674, 681, 807, 861, 960, 1041, 1045, 1125, 1185, 1208, 1228, 1247, 1249, 1254, 1340, 1397, 1421, 1434, 1453, 1549, 1633, 1634, 1642, 1667, 1675, 1744, 1838, 1964, 1994, 2123, 2218, 2239, 2349, 2410, 2419, 2466, 2521, 2761, 2883, 2884, 2891, 2940, 2943, 2956, 3025, 3035, 3100, 3215, 3244, 3326, 3332–3334, 3336, 3454]. **span** [1367, 1506]. **Spanned** [582]. **spanning** [1534]. **Spans** [59, 627]. **Sparse** [278, 932, 1078, 1324, 1956, 2150]. **Spatial** [1625, 1729]. **Special** [987, 1176, 1193, 1219, 1469, 1494, 1637, 1708, 1876, 1953, 1997, 2039, 2108, 2189, 2344, 2589, 3042, 3179, 3193, 3273]. **Specific** [213]. **Specified** [552, 801, 1555, 1704]. **specifying** [2869]. **SPECK** [2713]. **Spectra** [308, 1081, 1502, 2672, 3113]. **Spectral** [212, 1059, 1460, 1925, 2877, 3275]. **Spectral-Null** [212]. **Spectrum** [76, 786, 1220, 1461, 1639, 1754, 2326, 2352, 2740, 2821, 2967, 3017, 3384]. **speed** [1889]. **Speeding** [878, 1518, 1799, 2325]. **SPEEDY** [3130]. **Spence** [3320]. **Sperner** [3296]. **SPG** [700]. **SPG-Reguli** [700]. **Sphere** [536, 1339, 1577, 3396]. **spheres** [1313, 3199]. **Spherical** [62, 97, 456, 758, 824, 1148, 1463, 1487, 2607, 2830, 3000, 3455]. **Spin** [554, 782]. **splash** [1852]. **splice** [3024]. **splice-and-cut** [3024]. **Split** [279, 414, 3036]. **splittable** [2708]. **splitting** [856, 1012, 1344, 1377, 2272, 2696, 2826, 3202]. **SPN** [2731, 3242]. **spontaneous** [2158, 2532]. **Sporadic** [661, 1646, 2034, 3057]. **spotty** [1613]. **Spread** [71, 73, 498, 951, 1198, 1331, 2143, 2197, 2453, 2622, 2894]. **spread-based** [951]. **spread-like** [2622]. **spreading** [3030, 3333]. **Spreads** [74, 78, 174, 179, 239, 358, 421, 472, 495, 635, 636, 650, 667, 683, 690, 715, 786, 860, 982, 1041, 1640, 1702, 1921, 2147, 2349, 2812, 2914, 3231]. **spurs** [2131]. **Spyros** [1219]. **SQS** [81]. **Square** [534, 608, 686, 754, 905, 1037, 1169, 1383, 1650, 1885, 2005, 2598, 2922, 2950, 3164, 3407, 3417]. **Square-Free** [754]. **square-root** [3417]. **squared** [2449]. **squared-sum** [2449]. **Squares** [58, 460, 581, 638, 662, 705, 722, 746, 894, 895, 926, 1157, 1626, 1631, 1817, 2119, 2334, 2371, 2502, 2557, 2645, 2994, 3443]. **Squaring** [1990]. **stabilisers** [3292]. **stability** [1376]. **stabilized** [1645]. **stabilizer** [2612]. **stabilizer-based** [2612]. **stable** [3360]. **stage** [2162]. **Standard** [562, 1090, 1295, 1622, 2321, 2366, 2747, 2789, 2973, 3018, 3154, 3233]. **Stanica** [2212]. **Stanley** [1669]. **STARKs** [3240]. **start/near** [2530]. **State** [250, 434, 535, 556, 2341, 2762, 3141]. **states** [1063]. **statistical** [2281]. **STD** [820]. **Steane** [2597]. **Steane-enlargement** [2597]. **Steganographic** [2440]. **Steganography** [1018, 1833, 2849]. **Steiner** [11, 43, 55, 67, 76, 86, 134, 164, 172, 184, 187, 273, 288, 289, 291, 322, 333, 394, 420, 462, 531, 585, 643, 785, 787, 899, 988, 996, 1069, 1373, 1395, 1482, 1553, 1681, 1816, 2073, 2121, 2133, 2201, 2353, 2467, 2536, 2565, 2566, 2628, 2656,

2726, 2802, 2820, 3114, 3147]. **Step** [670]. **stepwise** [906]. **Stern** [2739, 3111, 3146]. **Stern-like** [3111]. **Stichtenoth** [3127]. **Stickelberger** [214]. **Storage** [2465, 2565, 3061, 3259]. **Stories** [177, 189]. **STP** [2796]. **STP-based** [2796]. **strategies** [1584]. **strategy** [1164]. **Stream** [507, 1068, 1527, 1572, 2041, 2226, 2243, 2492, 2728, 2982, 3228]. **Strength** [372, 586, 814, 1123, 1385, 1740, 1880, 2315, 3048]. **strength-3** [1740]. **Strengthening** [2203]. **strengths** [915]. **stretch** [3405]. **Stretching** [2164]. **strictly** [2073, 2478]. **String** [511]. **strings** [1325]. **Strong** [1147, 1312, 1593, 1936, 2151, 2152, 2238, 2256, 2328, 2612, 2654, 2751, 3054, 3139, 3372]. **strong-RSA** [1312]. **Strongly** [179, 395, 464, 1048, 1169, 1510, 1853, 1921, 1930, 1951, 1955, 1962, 2062, 2127, 2169, 2185, 2443, 2471, 2631, 2872, 2917, 3140, 3211, 3309, 3380]. **Structural** [1329, 1940, 2926, 3060, 3284]. **Structure** [96, 128, 213, 243, 478, 526, 527, 548, 560, 654, 763, 854, 970, 1523, 1687, 1729, 1737, 1887, 1961, 2098, 2451, 2553, 2603, 2652, 2654, 2751, 2834, 2933, 2950, 2951, 2981, 3124, 3204, 3239, 3246, 3410, 3452]. **structure-preserving** [1887]. **Structures** [161, 348, 477, 586, 685, 759, 893, 908, 1254, 1515, 1545, 1651, 1692, 1780, 2060, 2323, 2354, 2461, 2600, 2651, 2685, 2958, 2970, 2979, 3053, 3163, 3216, 3245, 3442, 3450]. **structures-applications** [3450]. **study** [1201, 2078, 2455, 2758, 2960, 3053]. **Studying** [1483, 3409]. **sub** [1615, 1801, 2060, 2850, 3243]. **sub-code** [2850]. **sub-families** [1615, 1801, 2060]. **sub-packetization** [3243]. **Subclass** [312]. **subcode** [1025, 1558, 1653]. **subcode-subfields** [1558]. **Subcodes** [467, 582, 952, 1057, 1353, 1386, 1590, 1760, 1789, 1832, 2515, 2860, 3103, 3192]. **subconstituent** [1169]. **subcovers** [3401]. **Subdesign** [602]. **subfield** [1590, 1832, 2668, 3103, 3192]. **subfield-subcodes** [1832, 3192]. **subfields** [1558, 3416, 3419]. **subgeometries** [1031, 1871, 2884]. **subgeometry** [1022]. **Subgraphs** [751, 1510]. **Subgroup** [178, 798, 1052, 1812, 2097, 2587, 2893, 3022, 3031, 3194]. **Subgroups** [487, 780, 1916, 1976, 2885, 3022, 3131, 3401]. **sublattice** [3068]. **sublinear** [2295, 3044]. **Sublines** [399, 840]. **Submatrices** [205, 212]. **Submodule** [3000]. **submodules** [2296]. **Subplane** [457, 1468, 1852, 1986, 2953]. **subplanes** [1636, 2356]. **subquadrangle** [1652]. **Subregular** [860, 921]. **subring** [2296]. **subring-submodules** [2296]. **subsequences** [1047, 2588]. **Subset** [1151, 1455, 2145, 2771, 2866, 3001, 3007]. **subset-resilient** [2771]. **Subset-Sum** [2866]. **Subsets** [101, 472, 738, 1059, 1152, 1156, 1176, 1357, 1997, 2954]. **Subspace** [1252, 1449, 1571, 1743, 1924, 1972, 2031, 2098, 2154, 2191, 2606, 2943, 3034, 3092, 3142, 3235, 3242, 3244, 3283, 3379]. **Subspaces** [58, 606, 680, 1664, 1972, 2513, 2700, 2767, 2882, 3025, 3338]. **Subsquares** [58]. **Substitution** [428, 2782]. **substring** [1979]. **substructures** [1970]. **subsystems** [1049]. **Subterranean** [2701]. **succeeding** [77]. **success** [1302]. **Successive** [326, 535]. **succinct** [3046]. **succinctness** [3453]. **Sudan** [1204, 1723]. **Sudoku** [2069, 2119, 2334]. **Sudoku-like** [2069]. **Sufficient** [227, 1011, 1181]. **Suitable** [340, 810, 1858]. **Sum** [456, 622, 1047, 1098, 2405, 2436, 2443, 2449, 2587, 2592, 2866, 2917, 2943, 2948, 2963, 3001, 3194, 3396, 3418]. **Sum-Free** [456]. **sum-rank** [2436, 2592, 3396, 3418]. **Sums** [66, 401, 483, 543, 1099, 1316, 1494, 1985, 2032, 2086, 2168, 2415, 2541, 2932, 3007, 3027, 3123, 3221, 3338]. **sunflower** [2883]. **Super** [872, 1300, 1379, 1626, 1662, 1859, 2125, 2256]. **Super-simple** [872, 1300, 1379, 1626, 1662, 1859]. **Super-strong** [2256].

**super-Vandermonde** [2125]. **superposition** [2781, 2813]. **supersingular** [953, 1897, 1919, 3230]. **supersolvable** [1563]. **superstable** [1425]. **supertail** [1571, 2098]. **Support** [764, 1353, 1517, 1673, 1745, 1937, 2769, 2952, 3354]. **supported** [2287]. **supporting** [1729, 2653, 2802]. **supports** [1025, 2436]. **Surface** [400, 1136, 1652, 1802, 2904, 3291]. **surfaces** [1504, 2360, 2886]. **surjective** [284, 1026]. **survey** [103, 1630, 1908, 1911, 3043, 3045, 3318]. **Suzuki** [2029, 2117]. **Suzuki-invariant** [2029]. **Swan** [1363]. **Swan-like** [1363]. **swap** [2991]. **swap-or-not** [2991]. **Swaps** [882]. **Switched** [2008, 2185, 2910]. **Switching** [368, 2122, 2856]. **Switchings** [1984]. **SXDH** [3221]. **Sylow** [487, 780]. **symbol** [1748, 2135, 2221, 2792, 2818, 2974, 2989, 3386, 3388]. **symbol-pair** [2135, 2221, 2818, 2974, 3386, 3388]. **symbols** [1986]. **Symmetric** [20, 25, 30, 34, 39, 62, 71, 109, 116, 117, 142, 147, 235, 241, 242, 286, 323, 392, 490, 520, 541, 554, 604, 616, 617, 624, 655, 662, 677, 706, 716, 741, 776, 803, 813, 820, 926, 934, 947, 1023, 1071, 1137, 1237, 1263, 1286, 1331, 1404, 1418, 1542, 1611, 1616, 1619, 1695, 1755, 1834, 1839, 1882, 1941, 1953, 1980, 2034, 2053, 2167, 2212, 2273, 2322, 2340, 2439, 2527, 2582, 2618, 2644, 2677, 2744, 2780, 2830, 2924, 2952, 2992, 3083, 3188, 3235, 3273, 3312, 3362, 3433, 3434]. **Symmetries** [630, 2564]. **Symmetrized** [658]. **Symmetry** [645, 2839, 2877, 3284]. **Symplectic** [690, 951, 1433, 1466, 1549, 1559, 1652, 1655, 1943, 2008, 2185, 2239, 2978, 3347]. **synchronization** [66]. **Synchronous** [446]. **syndrome** [2913, 2915, 3349, 3363, 3395]. **Synthesis** [682, 1581, 2231]. **synthetic** [1070]. **System** [222, 966, 1069, 1191, 1981, 2000, 2052, 2256, 2312, 2581, 2852]. **Systematic** [740, 936, 1079, 1556, 1609, 1682, 1800, 2465]. **Systematizing** [2899]. **Systems** [11, 36, 43, 67, 76, 86, 134, 164, 172, 176, 184, 186, 187, 234, 273, 279, 288, 289, 291, 301, 309, 322, 333, 339, 400, 420, 446, 462, 531, 585, 642, 643, 709, 739, 778, 785, 787, 815, 825, 899, 906, 971, 977, 988, 996, 1049, 1050, 1140, 1145, 1189, 1208, 1212, 1232, 1268, 1276, 1288, 1373, 1395, 1403, 1473, 1553, 1681, 1816, 1878, 2072, 2073, 2080, 2101, 2133, 2150, 2166, 2201, 2353, 2368, 2439, 2467, 2536, 2551, 2565, 2566, 2611, 2623, 2628, 2656, 2726, 2744, 2802, 2820, 2833, 2908, 3012, 3043, 3114, 3147, 3179, 3195, 3259, 3309, 3385, 3426, 3441].

**T** [586, 3204]. **Table** [260, 802, 1416, 1999, 3371]. **Tables** [428, 2375, 3371]. **Tactical** [1668, 1863, 3333]. **Tag** [2256, 2653, 2703]. **Tag-based** [2256, 2703]. **tails** [2109]. **Taking** [625, 1744]. **Tallini** [216]. **Tang** [2857, 3188]. **Tangent** [685, 1570, 1636, 1852, 3361]. **Tangents** [633]. **Taniguchi** [3104]. **Tanner** [1257, 1829, 2324]. **tap** [2289]. **Tardos** [1023, 1054, 1173, 1426, 1611, 1752, 1756, 1823]. **tau** [2171]. **TCC** [2816]. **Technical** [1905]. **Technique** [323, 1705, 3024, 3275]. **techniques** [1148, 1725, 1737, 1874, 1982, 2137, 2983, 3002]. **telescopic** [2277]. **template** [3395]. **ten** [1621, 2947]. **Tenengolts** [2279]. **tensor** [1528]. **tensored** [2182]. **tensors** [1548, 2482, 3165]. **term** [1156, 1630]. **terms** [1685, 3362]. **Ternary** [31, 35, 51, 105, 167, 168, 227, 229, 260, 269, 297, 302, 350, 423, 424, 480, 509, 510, 727, 768, 839, 1093, 1291, 1307, 1346, 1552, 2014, 2309, 2467, 2488, 2498, 2515, 2722, 2769, 2784, 2839, 2892, 2927, 2972, 3064, 3134, 3198, 3314, 3358, 3391]. **Terwilliger** [3036]. **Test** [883, 2630, 2725, 3139]. **testing** [2398, 3271]. **testings** [3031]. **tests** [1890, 2939]. **th** [625, 1022, 1124]. **th-Root** [1022]. **Their** [82, 90, 92, 211, 365, 418, 447, 476, 515, 518, 567, 593, 644, 665, 695, 916, 952, 1057, 1084, 1110, 1135, 1147, 1208, 1290, 1347, 1503, 1588, 1620, 1789, 1800, 1811, 1832, 1861,

1887, 1907, 1922, 1954, 1983, 2006, 2008, 2015, 2116, 2182, 2244, 2348, 2416, 2429, 2446, 2473, 2490, 2517, 2550, 2599, 2632, 2711, 2829, 2833, 2846, 2917, 2923, 2948, 2958, 2959, 2993, 3064, 3066, 3072, 3084, 3123, 3170, 3192, 3253, 3323, 3343, 3371, 3451]. **them** [1098]. **Theorem** [9, 183, 207, 391, 393, 397, 486, 565, 751, 853, 1156, 1163, 1171, 1174, 1175, 1376, 1378, 1419, 1448, 1463, 1476, 1598, 1773, 2016, 2043, 2118, 2201, 2232, 2345, 2379, 2389, 2460, 2647, 2810, 3004, 3296]. **Theorems** [526, 1396, 1480, 2392, 2591, 2660]. **theoretic** [94, 291, 333, 1277, 1388, 1938, 2007, 2441, 2655, 2766, 3166, 3351]. **theoretical** [2457]. **Theory** [55, 135, 233, 299, 561, 849, 889, 933, 1352, 1369, 1508, 1576, 1609, 1826, 1834, 1914, 1983, 2436, 2450, 2827, 2831, 2916, 3091, 3224, 3420, 3432, 3446]. **There** [491, 899, 967, 1159, 2175]. **Theta** [789, 1839, 3040, 3307]. **Thin** [749]. **third** [1820, 2183, 2432]. **Thirteen** [774]. **Thirteen-Player** [774]. **Three** [101, 130, 150, 309, 372, 457, 464, 612, 652, 733, 738, 915, 963, 1011, 1083, 1152, 1306, 1389, 1404, 1537, 1552, 1657, 1730, 1762, 1795, 1815, 1880, 1955, 2022, 2027, 2068, 2082, 2084, 2219, 2233, 2309, 2315, 2359, 2415, 2443, 2489, 2529, 2742, 2832, 3314, 3344, 3375]. **three-character** [2084]. **Three-Dimensional** [457, 1795]. **three-independent** [101]. **Three-weight** [2068, 2219, 2309, 2415, 2443]. **Threshold** [126, 221, 309, 552, 777, 823, 892, 1360, 1524, 1600, 1635, 2177, 2186, 2710, 2999, 3085, 3458]. **Thwarts** [127]. **Tight** [257, 536, 758, 1011, 1106, 1111, 1128, 1253, 1533, 1685, 1877, 1931, 1939, 2400, 2585, 2704, 2708, 3005, 3171, 3303]. **Tightly** [1975, 2204, 2570]. **tilings** [3039]. **Time** [42, 935, 1713, 1860, 2254, 2311, 2404, 2449, 2609, 2712, 3019, 3078, 3099, 3257]. **Time-based** [3257]. **time-lock** [2311]. **time/memory/data** [3078]. **Timed** [2177]. **Timed-release** [2177]. **times** [3279]. **Tits** [1044, 3292]. **TLS** [1873]. **TLS-attack** [1873]. **TMDTO** [2762]. **tms** [946]. **tms-nets** [946]. **Toeplitz** [3241]. **tokens** [1299]. **Tonchev** [520]. **TOPAS** [3218]. **Topology** [694]. **Topology-Transparent** [694]. **Tori** [138, 1096, 3131, 3143, 3408]. **torus** [1935]. **torus-based** [1935]. **Total** [1009, 2035, 3194]. **totally** [1570, 2668]. **Tournament** [60, 254, 1028]. **Tournaments** [774]. **tower** [930, 1573, 2117, 3127, 3419]. **towers** [2804]. **tR** [2466]. **Trace** [532, 550, 831, 875, 1089, 1812, 2097, 2387, 2748, 2822, 3010, 3099, 3128, 3138, 3411, 3429, 3457]. **Trace-One** [831]. **Traceability** [673, 2271, 2611, 2942]. **Traceable** [2669]. **Traces** [739, 801]. **Tracing** [762, 1342, 1611, 2528]. **Trade** [859, 1297, 3028]. **Trade-off** [859, 1297, 3028]. **tradeoff** [1999, 3078]. **tradeoffs** [1273]. **Trades** [419]. **Trading** [267, 873]. **Trails** [1473, 2713]. **Traitor** [762, 1342, 1611]. **transfer** [1280, 2017]. **transform** [1711, 1726]. **transform-domain** [1726]. **transformation** [1186, 1625, 1810, 2092, 2752]. **Transformations** [757, 3425]. **Transforming** [547]. **Transforms** [484, 2061, 2290, 2749]. **Transient** [781]. **Transitive** [17, 19, 23, 422, 457, 489, 754, 871, 923, 925, 981, 985, 1045, 1228, 1237, 1261, 1539, 1582, 1646, 1667, 1689, 1691, 1788, 1953, 1966, 1971, 2034, 2273, 2283, 2412, 2463, 2533, 2545, 2670, 2677, 2779, 2812, 2888, 2922, 3020, 3057, 3083, 3189, 3248, 3264, 3433]. **transitivity** [1529, 1627]. **Translation** [18, 93, 118, 120, 232, 517, 599, 611, 715, 964, 980, 985, 1055, 1067, 1540, 2956, 3100, 3174, 3300]. **translation-invariant** [3100]. **transmission** [1413]. **Transparency** [2046, 2422]. **Transparent** [694]. **transvection** [2887]. **Transversal** [127, 244, 353, 599, 820, 1234, 1331, 1633, 1634]. **Transversal-Free** [599]. **transversals** [426, 905, 2371]. **trapdoor** [1166, 2452, 2662]. **tree** [1692]. **tree-based** [1692]. **Trellis**

[527]. **trellises** [2450]. **Triads** [410]. **trial** [1723]. **Trialities** [778]. **Triangle** [714, 1208, 2719, 3061]. **Triangle-Free** [714, 3061]. **Triangular** [116, 906, 1403]. **tribute** [3277]. **Tridiagonal** [757]. **trigonometric** [2405, 2932]. **Trims** [2787]. **trinomials** [986, 987, 1363, 2049, 2799]. **triplanes** [1261]. **Triple** [43, 67, 76, 134, 164, 172, 184, 273, 288, 289, 322, 502, 585, 709, 761, 822, 899, 971, 988, 1049, 1050, 1212, 1373, 1395, 1473, 1659, 1681, 1815–1817, 2072, 2101, 2166, 2201, 2353, 2443, 2536, 2554, 2726, 2744, 2917, 3012, 3179, 3390, 3426]. **triple-cycle** [2554]. **triple-error-correcting** [1659]. **triple-twisted** [3390]. **Triples** [352, 592, 1445, 1473, 2205, 3424]. **triplets** [3268]. **triply** [182, 1450]. **triply-shortened** [1450]. **Trivial** [491, 2947]. **TRIVIUM** [1393, 2341, 2634, 3369]. **Troika** [2488]. **Trojan** [3313]. **tropical** [3246]. **True** [532, 799]. **Truncated** [49, 981, 2094, 2262, 2538, 2968, 3276]. **trusted** [3044, 3428]. **Tsfasman** [834, 2545]. **Tsujii** [562, 987, 2058]. **Turing** [2973]. **Turyn** [1374, 1398, 3173]. **Tutte** [2990, 3136]. **tweak** [2936]. **tweakable** [1781, 2209, 2702, 2720, 2936, 3435]. **Tweaking** [2321]. **tweaks** [3352]. **twenty** [1894]. **twenty-year** [1894]. **TWINE** [3450]. **twist** [1896, 3237]. **Twisted** [548, 1040, 1208, 1504, 1528, 1844, 2122, 2431, 2473, 2581, 2698, 2709, 2717, 2718, 2861, 2874, 2889, 3157, 3359, 3390, 3423]. **Two** [51, 84, 114, 150, 226, 346, 438, 462, 489, 509, 541, 704, 757, 790, 800, 809, 837, 884, 887, 916, 944, 967, 970, 984, 985, 1029, 1031, 1048, 1063, 1098, 1100, 1119, 1191, 1195, 1223, 1224, 1243, 1267, 1286, 1304, 1320, 1389, 1409, 1420, 1424, 1433, 1516, 1542, 1597, 1748, 1790, 1843, 1846, 1859, 1921, 1946, 1953, 2006, 2022, 2120, 2170, 2190, 2228, 2242, 2289, 2305, 2307, 2322, 2434, 2573, 2588, 2604, 2631, 2705, 2768, 2793, 2798, 2882, 2923, 2969, 2975, 2998, 3014, 3041, 3094, 3108, 3168, 3244, 3266, 3302, 3314, 3335, 3385, 3419, 3423, 3461]. **two-channel** [1224]. **two-character** [944, 1029, 1191, 1243]. **two-dimensional** [984, 1195, 1420, 1424, 2322, 2798, 3385]. **two-fold** [1921]. **two-graph** [1063]. **Two-level** [509]. **two-party** [2289]. **Two-Point** [837, 884, 887, 1100, 1267]. **two-prime** [1304]. **two-to-one** [1119, 2923]. **Two-Transitive** [489, 985]. **Two-Weight** [462, 916, 1048, 1946, 2242, 2573, 2705, 2969, 3108]. **Twofold** [2101]. **Type** [151, 307, 359, 370, 371, 375, 475, 502, 521, 541, 559, 587, 637, 656, 664, 671, 743, 789, 915, 995, 1037, 1109, 1162, 1229, 1288, 1327, 1331, 1354, 1374, 1396, 1401, 1419, 1423, 1431, 1456, 1466, 1494, 1542, 1543, 1594, 1650, 1671, 1759, 1778, 1835, 2182, 2213, 2266, 2280, 2289, 2421, 2435, 2439, 2591, 2660, 2699, 2841, 3109, 3224, 3285, 3337, 3462]. **Type-1** [475]. **types** [1651, 2501, 3168].

**Ubiquity** [1683]. **ultrametric** [3254]. **Unbalanced** [1164, 1303]. **Unbiased** [1840, 1977, 2265]. **unbounded** [2000, 2795, 2952, 3221]. **Unconditionally** [91, 282, 332, 337, 576, 621, 1224, 2078, 2988, 3117]. **uncover** [2899]. **Uncoverings** [923]. **Uncoverings-by-bases** [923]. **Undeniable** [672]. **Understanding** [3422]. **Undetected** [363, 1058]. **Uni** [446]. **Uni-Polar** [446]. **unicast** [3225]. **unified** [1629, 2063, 2846]. **Uniform** [246, 721, 732, 1654, 1722, 1866, 1917, 1972, 2267, 2333, 2590, 2620]. **uniformity** [2263, 2394, 2559, 2616, 2629, 2673, 2737, 2808, 3341, 3448]. **uniformly** [1053, 1256]. **unions** [2356]. **Unique** [723, 1468, 1593, 1725, 2986]. **Uniquely** [386, 451, 3041]. **Uniqueness** [321, 634, 747, 977, 1117, 2115, 2413, 2435, 2441, 2776, 3080, 3260]. **Unital** [55, 228, 1027, 2851, 2918, 2919, 3077]. **Unitals** [242, 290, 313, 348, 399, 860, 1213, 1230, 1338, 1645, 2362, 2474, 2956, 3292]. **Unitary** [52, 242, 512, 1177, 1869, 2335, 2887].

**Universal** [112, 262, 403, 1297, 1435, 1574, 1851, 3119, 3408]. **universally** [935]. **unknown** [1572, 2538, 2968]. **Unreal** [1947]. **unrestricted** [812]. **unsigncryption** [1600]. **Untransferability** [190]. **Untrusted** [878]. **Unweighted** [2279]. **updatable** [1942]. **update** [198, 2303, 3257]. **upon** [1566]. **Upper** [316, 418, 501, 547, 657, 1140, 1937, 2042, 2147, 2262, 2271, 2607, 2623, 2838, 3421]. **Use** [497, 763, 876, 902]. **User** [446, 735, 1932, 2321, 2396, 2570]. **user-irrepressible** [1932]. **uses** [2464]. **Using** [132, 135, 185, 193, 234, 266, 286, 295, 301, 444, 535, 663, 685, 704, 716, 762, 813, 815, 825, 878, 926, 936, 952, 1079, 1121, 1297, 1392, 1398, 1499, 1573, 1605, 1618, 1822, 1828, 1883, 1982, 1989, 1990, 2037, 2135, 2241, 2358, 2373, 2413, 2426, 2475, 2484, 2499, 2579, 2680, 2702, 2789, 2862, 2884, 2971, 3030, 3077, 3143, 3196, 3238, 3339]. **Utilizing** [144, 3245, 3419]. **Uwe** [3317].

**V** [2824]. **v3** [3369]. **valuations** [927, 1592]. **value** [1192, 1937, 2023, 2932, 3186]. **Valued** [566, 3254]. **Values** [518, 678, 1116, 1217, 1692, 1735]. **Vandermonde** [1452, 2125, 2873]. **vanishing** [2822]. **Vanstone** [1876]. **Variable** [122, 2653, 2833, 3301, 3319, 3383]. **Variable-Length** [122, 3319, 3383]. **variable-weight** [2833]. **variables** [1418, 2478, 2618, 3301]. **Variant** [1106, 1134, 1293, 1715, 2363, 2449, 3172]. **Variants** [1551, 1562, 1860, 2653, 2831, 3098]. **variation** [2358]. **Variations** [2389]. **Varieties** [21, 36, 301, 476, 627, 729, 759, 953, 1101, 1107, 1244, 1251, 1397, 1504, 1608, 1880, 1886, 2030, 3093, 3151]. **variety** [295, 1138, 1387, 1570, 1832, 2763, 2976]. **various** [1302, 2501, 3100, 3245]. **Varshamov** [885, 2279, 2343]. **Vault** [848]. **Vazirani** [2373]. **Vector** [361, 1053, 1181, 1198, 1260, 1299, 1403, 1425, 1455, 1838, 2043, 2182, 2870, 3007, 3047, 3231, 3294, 3338]. **Vectorial** [760, 1305, 1306, 1865, 2143, 2278, 2455, 2723, 2730, 2742, 2897, 3097, 3284, 3322, 3368]. **Vectors** [161, 582, 628, 812, 882, 896, 1131, 1318, 1346, 1455, 1465, 1728, 1883, 2315, 2552, 2900, 2916]. **Vera** [2827]. **Verheul** [1175]. **Verifiable** [549, 1724, 1893, 2340, 2518, 2868]. **Verifiably** [1864, 2970]. **verification** [2713]. **Veronese** [301, 476, 944, 2031, 2976, 3291]. **Veronesean** [570, 1536]. **Veroneseans** [755]. **Version** [137, 993, 1713]. **versions** [1054]. **versus** [2243, 2447, 2470]. **Vertex** [754, 1395, 1542, 2362, 2655]. **vertex-isoperimetric** [2362]. **vertex-quasiprimitive** [1542]. **Vertex-Transitive** [754]. **Vertices** [539, 914, 2424, 2425]. **very** [1593]. **VES** [1864]. **VI** [2982]. **via** [236, 272, 398, 622, 703, 896, 1369, 1483, 1511, 1739, 2102, 2144, 2145, 2154, 2180, 2250, 2251, 2295, 2541, 2550, 2575, 2605, 2703, 2719, 2874, 2891, 2939, 2943, 3054, 3144, 3195, 3225, 3244, 3251, 3275, 3312, 3385, 3406, 3409, 3444]. **view** [2462, 2846, 3446]. **viewed** [1685]. **Vinegar** [3441]. **virtual** [1578]. **Visual** [261, 453, 544, 552, 600, 777, 847, 892, 904, 1113, 1214, 1360, 1614, 1737, 1982, 2066, 2144, 2401]. **Vladut** [2545]. **Volume** [802]. **vs** [3284].

**Wagner** [1343]. **Walk** [1648, 2443, 2917]. **Walk-regular** [1648]. **Wall** [948]. **Walnut** [2433]. **Walsh** [1081, 1710, 2740, 3275, 3384]. **Wan** [3021]. **Ward** [1174, 1279]. **Warning** [1480]. **WARP** [3450]. **Watching** [156]. **Waterloo** [584]. **way** [783, 1521]. **Weak** [63, 832, 883, 984, 1043, 2584, 2867, 3033, 3426, 3436]. **Weakly** [641, 2546, 2993, 3064, 3200, 3270]. **Weaknesses** [284]. **Web** [779]. **Wegman** [2653]. **Wei** [1396, 2591]. **Wei-type** [1396, 2591]. **Weierstrass** [482, 770, 830, 1499, 2595, 2929, 3132]. **Weighing** [128, 272, 351, 655, 813, 920, 1674,

1840, 2318, 3203]. **Weight** [129, 219, 259, 265, 336, 356, 362, 388, 407, 414, 423, 424, 427, 440, 462, 529, 538, 554, 582, 658, 675, 724, 764, 871, 916, 920, 938, 942, 961, 1011, 1015, 1048, 1057, 1059, 1072, 1100, 1163, 1164, 1170, 1251, 1262, 1366, 1411, 1421, 1649, 1657, 1669, 1674, 1707, 1709, 1714, 1730, 1733, 1748, 1796, 1815, 1831, 1861, 1934, 1938, 1946, 1954, 1987, 2015, 2075, 2160, 2176, 2213, 2216, 2219, 2233, 2314, 2377, 2379, 2386, 2409, 2432, 2446, 2523, 2641, 2676, 2698, 2705, 2778, 2828, 2889, 2892, 2900, 2928, 2931, 2964, 2972, 3059, 3122, 3187, 3203, 3342, 3344, 3394, 3395, 3411]. **weight** [106, 958, 1058, 1253, 1380, 1517, 1569, 1613, 1660, 1672, 1795, 1807, 1839, 1955, 2006, 2068, 2220, 2242, 2309, 2326, 2352, 2415, 2443, 2489, 2573, 2583, 2792, 2833, 2969, 2989, 3108, 3265, 3386, 3407]. **Weight-preserving** [871]. **Weighted** [993, 1088, 1111, 1165, 1410, 1498, 1847, 2584, 2814, 3027, 3087, 3131, 3221, 3405]. **Weights** [128, 319, 329, 527, 668, 839, 875, 974, 1183, 1353, 1389, 1471, 1495, 1948, 2022, 2030, 2086, 2106, 2332, 2337, 2437, 2546, 2547, 2576, 2633, 2637, 2706, 2836, 2993, 3391, 3417]. **Weightwise** [2408]. **Weil** [2055]. **Welch** [263, 651, 1414, 3324]. **Welch-Berlekamp** [263]. **well** [48]. **WEM** [2823]. **WEM-8** [2823]. **Weng** [1522]. **wet** [1833]. **where** [2853]. **Which** [15, 631, 750, 1455, 1468, 1809, 2595, 2929, 3338]. **Whirlwind** [1246, 3049]. **Whist** [774]. **Whiteness** [552]. **whose** [19, 1152, 1239, 1389, 2018, 2598, 2744]. **Wide** [2574, 2687, 3421]. **Wide-sense** [2574, 3421]. **Wiedemann** [1081, 3102]. **Wieferich** [1187]. **Williams** [314]. **Williamson** [382, 769, 1035, 1374]. **Wilson** [1469, 1470]. **window** [950]. **wire** [2289]. **wire-tap** [2289]. **wireless** [933]. **Wiretap** [1718]. **wise** [1916]. **within** [3092]. **Without** [283, 347, 633, 701, 894, 895, 1047, 1095, 1797, 2101, 2768, 2930, 2954, 3044, 3124, 3239]. **witness** [2310]. **witnessing** [42]. **Witt** [2504, 3080]. **Wolfmann** [2361]. **WOM** [1584]. **Word** [783, 1194, 1287]. **word-oriented** [1287]. **wordlength** [15]. **words** [2523, 2650, 2817]. **Work** [170]. **World** [2857]. **Worst** [1825, 2011]. **Worst-case** [1825].

**Xedni** [436, 437]. **Xing** [1789]. **Xing-Ling** [1789]. **Xof** [3175]. **XOR** [2144, 3373, 3460]. **XOR-based** [2144].

**Yang** [1206, 1272]. **year** [1894]. **Yield** [782]. **Yin** [555]. **Youden** [1817]. **Yoyo** [3197]. **Yu** [2652].

**Z** [671, 863, 2798]. **Z-complementary** [2798]. **Z-cyclic** [863]. **Z2s** [1523]. **ZCZ** [2798]. **Zero** [110, 270, 1047, 1603, 1812, 1898, 1930, 2037, 2097, 2281, 2384, 2434, 2447, 2461, 2550, 2663, 2793, 2915, 3042, 3046, 3047, 3338]. **Zero-correlation** [2037, 2281]. **zero-difference** [1930, 2434, 2447]. **zero-divisor** [2550, 2793]. **Zero-Knowledge** [270, 1898, 2384, 2663, 2915, 3042, 3046, 3047]. **zero-sum** [1047]. **zeros** [1081, 1316, 1389, 2018, 3314]. **ZeroSum** [3284]. **zeta** [2274]. **Zetterberg** [2001]. **Zhexian** [3021]. **Zink** [2545]. **ZLR** [3223]. **Zolotarev** [535]. **zone** [1334, 1700, 1798, 2137, 2156].

# References

**Anonymous:1991:E**

[1] Anonymous. Editorial. *Designs, Codes, and Cryptography*, 1(1):5–??, May 1991. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Moorhouse:1991:BNC**

[2] G. Eric Moorhouse. Bruck nets, codes, and characters of loops. *Designs, Codes, and Cryptography*, 1 (1):7–29, May 1991. CODEN DC-

CREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Tietavainen:1991:CRD**

[3] A. Tietäväinen. Covering radius and dual distance. *Designs, Codes, and Cryptography*, 1(1):31–46, May 1991. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**LaMacchia:1991:CDL**

[4] B. A. LaMacchia and A. M. Odlyzko. Computation of discrete logarithms in prime fields. *Designs, Codes, and Cryptography*, 1(1):47–62, May 1991. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.research.att.com/~amo/doc/arch/prime.discrete.logs.pdf`; `http://www.research.att.com/~amo/doc/arch/prime.discrete.logs.ps`; `http://www.research.att.com/~amo/doc/arch/prime.discrete.logs.tex`.

**Lamken:1991:FPB**

[5] E. R. Lamken, W. H. Mills, and R. M. Wilson. Four pairwise balanced designs. *Designs, Codes, and Cryptography*, 1(1):63–68, May 1991. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Ho:1991:SRO**

[6] Chat Yin Ho. Some remarks on orders of projective planes, planar difference sets and multipliers. *Designs, Codes, and Cryptography*, 1(1):69–75, May 1991. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Simonis:1991:SPD**

[7] Juriaan Simonis and Cornelis de Vroedt. A simple proof of the Delsarte inequalities. *Designs, Codes, and Cryptography*, 1(1):77–82, May 1991. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Arasu:1991:QCG**

[8] K. T. Arasu and Alexander Pott. On quasiregular collineation groups of projective planes. *Designs, Codes, and Cryptography*, 1(1):83–92, May 1991. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Metsch:1991:IBC**

[9] Klaus Metsch. Improvement of Bruck's completion theorem. *Designs, Codes, and Cryptography*, 1(2):99–116, June 1991. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Davis:1991:NPR**

[10] James A. Davis. A note on products of relative difference sets. *Designs, Codes, and Cryptography*, 1(2):117–119, June 1991. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Siemon:1991:CSQ**

[11] Helmut Siemon. Cyclic Steiner quadruple systems and Köhler's orbit graphs. *Designs, Codes, and Cryptography*, 1 (2):121–132, June 1991. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Peterson:1991:FPS**

[12] David J. Peterson. Fractal properties of the singular function $s(u)$. *Designs, Codes, and Cryptography*, 1(2):

133–139, June 1991. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Bierbrauer:1991:HOS**

[13] Jürgen Bierbrauer and Tran Van Trung. Halving $\mathrm{PGL}(2, 2^f)$, $f$ odd: a series of cryptocodes. *Designs, Codes, and Cryptography*, 1(2):141–148, June 1991. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Anderson:1991:CSO**

[14] B. A. Anderson and P. A. Leonard. A class of self-orthogonal 2-sequencings. *Designs, Codes, and Cryptography*, 1 (2):149–181, June 1991. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Leonard:1991:LCC**

[15] Douglas A. Leonard. Linear cyclic codes of wordlength $v$ over $\mathrm{GF}(q^s)$ which are also linear cyclic codes of wordlength $sv$ over $\mathrm{GF}(q)$. *Designs, Codes, and Cryptography*, 1(2): 183–189, June 1991. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Bruen:1991:JMG**

[16] A. A. Bruen and J. C. Fisher. The Jamison method in Galois geometries. *Designs, Codes, and Cryptography*, 1 (3):199–205, September 1991. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Pfaff:1991:CDT**

[17] Oliver Pfaff. The classification of doubly transitive affine designs. *Designs, Codes, and Cryptography*, 1(3):207–217, September 1991. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Hachenberger:1991:CLT**

[18] Dirk Hachenberger. Constructions of large translation nets with non-abelian translation groups. *Designs, Codes, and Cryptography*, 1(3):219–236, September 1991. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Delandtsheer:1991:DLS**

[19] Anne Delandtsheer. Dimensional linear spaces whose automorphism group is (line, hyperplane)-flag transitive. *Designs, Codes, and Cryptography*, 1(3): 237–245, September 1991. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Jungnickel:1991:ENQ**

[20] D. Jungnickel and Vladimir D. Tonchev. Exponential number of quasi-symmetric SDP designs and codes meeting the Grey-Rankin bound. *Designs, Codes, and Cryptography*, 1(3): 247–253, September 1991. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Key:1991:HVC**

[21] J. D. Key. Hermitian varieties as codewords. *Designs, Codes, and Cryptography*, 1(3):255–259, September 1991. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Lambeck:1991:RIA**

[22] E. W. Lambeck. A remark on the intersection arrays of distance regular graphs and the distance regular graphs of diameter $d = 3i - 1$ with $b_i = 1$ and

$k > 2$. *Designs, Codes, and Cryptography*, 1(3):261–266, September 1991. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Pasini:1991:DGS**

[23] Antonio Pasini. Diagram geometries for sharply $n$-transitive sets of permutations or of mappings. *Designs, Codes, and Cryptography*, 1(4):275–297, December 1991. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**VanMaldeghem:1991:DFG**

[24] H. Van Maldeghem, J. A. Thas, and S. E. Payne. Desarguesian finite generalized quadrangles are classical or dual classical. *Designs, Codes, and Cryptography*, 1(4):299–305, December 1991. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Bierbrauer:1991:SHS**

[25] Jürgen Bierbrauer and Tran Van Trung. Some highly symmetric authentication perpendicular arrays. *Designs, Codes, and Cryptography*, 1(4): 307–319, December 1991. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Ma:1991:MCA**

[26] S. L. Ma. McFarland's conjecture on abelian difference sets with multiplier $-1$. *Designs, Codes, and Cryptography*, 1(4):321–332, December 1991. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Leung:1991:DSD**

[27] Ka Hin Leung, Siu Lun Ma, and Yan Loi Wong. Difference sets in dihedral groups. *Designs, Codes, and Cryptography*, 1(4):333–338, December 1991. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Yaghoobian:1992:HCG**

[28] Tomik Yaghoobian and Ian F. Blake. Hermitian codes as generalized Reed–Solomon codes. *Designs, Codes, and Cryptography*, 2(1):5–17, March 1992. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Jedwab:1992:GPA**

[29] Jonathan Jedwab. Generalized perfect arrays and Menon difference sets. *Designs, Codes, and Cryptography*, 2 (1):19–68, March 1992. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Bagchi:1992:QSD**

[30] Bhaskar Bagchi. On quasi-symmetric designs. *Designs, Codes, and Cryptography*, 2(1):69–79, March 1992. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Greenough:1992:OTQ**

[31] P. P. Greenough and R. Hill. Optimal ternary quasi-cyclic codes. *Designs, Codes, and Cryptography*, 2(1): 81–91, March 1992. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Jedwab:1992:NNB**

[32] Jonathan Jedwab and Sheelagh Lloyd. A note on the nonexistence of Barker sequences. *Designs, Codes, and Cryptography*, 2(1):93–97, March 1992. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Diffie:1992:AAK**

[33] Whitfield Diffie, Paul C. van Oorschot, and Michael J. Wiener. Authentication and authenticated key exchanges. *Designs, Codes, and Cryptography*, 2 (2):107–125, June 1992. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Spence:1992:CCS**

[34] Edward Spence. A complete classification of symmetric $(31, 10, 3)$ designs. *Designs, Codes, and Cryptography*, 2 (2):127–136, June 1992. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Hill:1992:OTL**

[35] R. Hill and D. E. Newton. Optimal ternary linear codes. *Designs, Codes, and Cryptography*, 2(2):137–157, June 1992. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Bryant:1992:VQA**

[36] Darryn E. Bryant. Varieties of quasigroups arising from 2-perfect $m$-cycle systems. *Designs, Codes, and Cryptography*, 2(2):159–168, June 1992. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Cohen:1992:ECI**

[37] Stephen D. Cohen. The explicit construction of irreducible polynomials over finite fields. *Designs, Codes, and Cryptography*, 2(2):169–174, June 1992. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Stinson:1992:CCA**

[38] D. R. Stinson. Combinatorial characterizations of authentication codes. *Designs, Codes, and Cryptography*, 2 (2):175–187, June 1992. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Blokhuis:1992:QSD**

[39] A. Blokhuis and A. R. Calderbank. Quasi-symmetric designs and the Smith normal form. *Designs, Codes, and Cryptography*, 2(2):189–206, June 1992. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Hou:1992:SIA**

[40] Xiang Dong Hou. Some inequalities about the covering radius of Reed–Muller codes. *Designs, Codes, and Cryptography*, 2(3):215–224, September 1992. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Hamada:1992:CCM**

[41] Noboru Hamada, Tor Helleseth, and Øyvind Ytrehus. On the construction of $[q^4 + q^2 - q, 5, q^4 - q^3 + q^2 - 2q; q]$-codes meeting the Griesmer bound. *Designs, Codes, and Cryptography*, 2(3): 225–229, September 1992. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Fellows:1992:SWP**

[42] Michael R. Fellows and Neal Koblitz. Self-witnessing polynomial-time complexity and prime factorization. *Designs, Codes, and Cryptography*, 2(3): 231–235, September 1992. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Colbourn:1992:CMA**

[43] Charles J. Colbourn, Eric Mendelsohn, Cheryl E. Praeger, and Vladimir D. Tonchev. Concerning multiplier automorphisms of cyclic Steiner triple systems. *Designs, Codes, and Cryptography*, 2(3):237–251, September 1992. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Shaw:1992:CP**

[44] Ronald Shaw. A characterization of the primals in PG$(m, 2)$. *Designs, Codes, and Cryptography*, 2(3):253–256, September 1992. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Arasu:1992:EPC**

[45] K. T. Arasu and Qing Xiang. On the existence of periodic complementary binary sequences. *Designs, Codes, and Cryptography*, 2(3):257–262, September 1992. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Pott:1992:ADS**

[46] Alexander Pott. On abelian difference set codes. *Designs, Codes, and Cryptography*, 2(3):263–271, September 1992. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Landrock:1992:CCI**

[47] Peter Landrock and Olaf Manz. Classical codes as ideals in group algebras. *Designs, Codes, and Cryptography*, 2 (3):273–285, September 1992. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Beth:1992:DMA**

[48] Thomas Beth and Volker Hatz. Design machines: algebraically well described interconnection networks. *Designs, Codes, and Cryptography*, 2(3): 287–298, September 1992. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Melone:1992:RTI**

[49] Nicola Melone and Udo Ott. On the rank of truncated incidence matrices of linear spaces. *Designs, Codes, and Cryptography*, 2(4):307–313, 1992. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Gao:1992:ONB**

[50] Shuhong Gao and Hendrik W. Lenstra, Jr. Optimal normal bases. *Designs, Codes, and Cryptography*, 2(4):315–323, 1992. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Jackson:1992:RBT**

[51] W.-A. Jackson and P. R. Wild. Relations between two perfect ternary sequence constructions. *Designs, Codes, and Cryptography*, 2(4):325–332, 1992. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Wan:1992:CCA**

[52] Zhe Xian Wan. Construction of Cartesian authentication codes from unitary geometry. *Designs, Codes, and Cryptography*, 2(4):333–356, 1992. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Stinson:1992:ESS**

[53] D. R. Stinson. An explication of secret sharing schemes. *Designs, Codes, and Cryptography*, 2(4):357–390, 1992. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**deCaen:1992:RIM**

[54] D. de Caen, C. D. Godsil, and G. F. Royle. On the $p$-rank of incidence matrices and a bound of Bruen and Ott. *Designs, Codes, and Cryptography*, 2 (4):391–394, December 1992. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Schmidt:1992:NQB**

[55] Bernhard Schmidt. Note on a question by S. Bagchi and B. Bagchi: "Designs from pairs of finite fields. I. A cyclic unital $U(6)$ and other regular Steiner 2-designs" [J. Combin. Theory Ser. A **52** (1989), no. 1, 51–61; MR 90k:05025]. *Designs, Codes, and Cryptography*, 2 (4):395, December 1992. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Hare:1993:CBI**

[56] Donovan R. Hare and William McCuaig. The connectivity of the block-intersection graphs of designs. *Designs, Codes, and Cryptography*, 3 (1):5–8, March 1993. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Wallis:1993:SCC**

[57] W. D. Wallis, J. L. Yucas, and G.-H. Zhang. Single change covering designs. *Designs, Codes, and Cryptography*, 3 (1):9–19, March 1993. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Laywine:1993:SOL**

[58] Charles Laywine. Subsquares in orthogonal Latin squares as subspaces in affine geometries: a generalization of an equivalence of Bose. *Designs, Codes, and Cryptography*, 3(1):21–28, March 1993. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Khachatrian:1993:LBQ**

[59] Levon H. Khachatrian. The lower bound of the quadratic spans of de Bruijn sequences. *Designs, Codes, and Cryptography*, 3(1):29–32, March 1993. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Lamken:1993:ERG**

[60] E. R. Lamken. Existence results for generalized balanced tournament designs with block size 3. *Designs, Codes, and Cryptography*, 3(1):33–61, March 1993. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Skinner:1993:NDM**

[61] Chris M. Skinner. Nonsymmetric 2-designs modulo 2. *Designs, Codes, and Cryptography*, 3(1):63–68, March 1993. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Boyvalenkov:1993:NCS**

[62] Peter Boyvalenkov. Nonexistence of certain symmetric spherical codes. *Designs, Codes, and Cryptography*, 3(1): 69–74, March 1993. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**deLauney:1993:WDS**

[63] W. de Launey and K. J. Horadam. A weak difference set construction for higher-dimensional designs. *Designs, Codes, and Cryptography*, 3(1): 75–87, March 1993. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Brouwer:1993:SJB**

[64] A. E. Brouwer and L. M. G. M. Tolhuizen. A sharpening of the Johnson bound for binary linear codes and the nonexistence of linear codes with Preparata parameters. *Designs, Codes, and Cryptography*, 3(2):95–98, May 1993. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Mavron:1993:CAC**

[65] V. C. Mavron and W. D. Wallis. Cubic arcs in cubic nets. *Designs, Codes, and Cryptography*, 3(2):99–104, May 1993. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Barg:1993:ISD**

[66] Alexander Barg. Incomplete sums, dc-constrained codes, and codes that maintain synchronization. *Designs, Codes, and Cryptography*, 3(2):105–116, May 1993. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Key:1993:CST**

[67] J. D. Key and F. E. Sullivan. Codes of Steiner triple and quadruple systems. *Designs, Codes, and Cryptography*, 3 (2):117–125, May 1993. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). See erratum [134] and correction [164].

**Beutelspacher:1993:LSS**

[68] Albrecht Beutelspacher and Ferenc Wettl. On 2-level secret sharing. *Designs, Codes, and Cryptography*, 3(2): 127–134, May 1993. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Carlet:1993:PBF**

[69] Claude Carlet. Partially-bent functions. *Designs, Codes, and Cryptography*, 3(2):135–145, May 1993. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Chan:1993:NCM**

[70] W. K. Chan. Necessary conditions for Menon difference sets. *Designs, Codes, and Cryptography*, 3(2):147–154, May 1993. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Sane:1993:SCQ**

[71] S. S. Sane and M. S. Shrikhande. Some characterizations of quasi-symmetric designs with a spread. *Designs, Codes, and Cryptography*, 3(2):155–166, May 1993. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Hou:1993:FRC**

[72] Xiang Dong Hou. Further results on the covering radii of the Reed–Muller codes. *Designs, Codes, and Cryptography*, 3(2):167–177, May 1993. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Blokhuis:1993:SMP**

[73] Aart Blokhuis and Klaus Metsch. On the size of a maximal partial spread. *Designs, Codes, and Cryptography*, 3

(3):187–191, 1993. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**vanDam:1993:CS**

[74] Edwin R. van Dam. Classification of spreads of PG$(3,4) \longrightarrow$ PG$(3,2)$. *Designs, Codes, and Cryptography*, 3(3): 193–198, July 1993. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Beth:1993:DCG**

[75] Thomas Beth. The GF($p$)-dimension of the codes generated by the classical point-line geometries over GF($p$). *Designs, Codes, and Cryptography*, 3 (3):199–207, July 1993. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Colbourn:1993:SMP**

[76] Charles J. Colbourn, Alexander Rosa, and Štefan Znám. The spectrum of maximal partial Steiner triple systems. *Designs, Codes, and Cryptography*, 3 (3):209–219, July 1993. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Rifa-Coma:1993:HAC**

[77] Josep Rifà-Coma. How to avoid the cheaters succeeding in the key sharing scheme. *Designs, Codes, and Cryptography*, 3(3):221–228, July 1993. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**OKeefe:1993:SGD**

[78] Christine M. O'Keefe and Alan Rahilly. Spreads and group divisible designs. *Designs, Codes, and Cryptography*, 3 (3):229–235, July 1993. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Carlet:1993:AGD**

[79] Claude Carlet. The automorphism groups of the Delsarte-Goethals codes. *Designs, Codes, and Cryptography*, 3 (3):237–249, July 1993. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Hamalainen:1993:BBM**

[80] Heikki O. Hämäläinen, Iiro S. Honkala, Markku K. Kaikkonen, and Simon N. Litsyn. Bounds for binary multiple covering codes. *Designs, Codes, and Cryptography*, 3(3):251–275, July 1993. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Bitan:1993:LPN**

[81] Sara Bitan and Tuvi Etzion. The last packing number of quadruples, and cyclic SQS. *Designs, Codes, and Cryptography*, 3(4):283–313, October 1993. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Dougherty:1993:NTC**

[82] Steven Dougherty. Nets and their codes. *Designs, Codes, and Cryptography*, 3(4):315–331, October 1993. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Geiselmann:1993:SDB**

[83] Willi Geiselmann and Dieter Gollmann. Self-dual bases in $\mathbf{F}_{q^n}$. *Designs, Codes, and Cryptography*, 3(4): 333–345, October 1993. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Klapper:1993:CCG**

[84] A. Klapper. Cross-correlations of geometric sequences in characteristic two. *Designs, Codes, and Cryptography*, 3 (4):347–377, October 1993. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Davis:1993:NNS**

[85] James A. Davis and Jonathan Jedwab. A note on new semi-regular divisible difference sets. *Designs, Codes, and Cryptography*, 3(4):379–381, October 1993. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Teirlinck:1994:SNR**

[86] Luc Teirlinck. Some new 2-resolvable Steiner quadruple systems. *Designs, Codes, and Cryptography*, 4(1):5–10, January 1994. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Mitchell:1994:DPM**

[87] Chris J. Mitchell and Kenneth G. Paterson. Decoding perfect maps. *Designs, Codes, and Cryptography*, 4(1): 11–30, January 1994. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Conway:1994:QCB**

[88] J. H. Conway and N. J. A. Sloane. Quaternary constructions for the binary single-error-correcting codes of Julin, Best and others. *Designs, Codes, and Cryptography*, 4(1):31–42, January 1994. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Kennedy:1994:DFS**

[89] George T. Kennedy and Vera Pless. On designs and formally self-dual codes. *Designs, Codes, and Cryptography*, 4 (1):43–55, January 1994. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Dodunekov:1994:BSC**

[90] Stefan M. Dodunekov, Silvia B. Encheva, and Stoyan N. Kapralov. On the $[28, 7, 12]$ binary self-complementary codes and their residuals. *Designs, Codes, and Cryptography*, 4(1):57–67, January 1994. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Johansson:1994:SRC**

[91] Thomas Johansson. A shift register construction of unconditionally secure authentication codes. *Designs, Codes, and Cryptography*, 4(1):69–81, January 1994. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Jackson:1994:GSS**

[92] Wen-Ai Jackson and Keith M. Martin. Geometric secret sharing schemes and their duals. *Designs, Codes, and Cryptography*, 4(1):83–95, January 1994. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Dempwolff:1994:TPO**

[93] U. Dempwolff. Translation planes of order 27. *Designs, Codes, and Cryptography*, 4(2):105–121, April 1994. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). See corrections [120, 291].

**Dougherty:1994:CTS**

[94] Steven T. Dougherty. A coding-theoretic solution to the 36 officer problem. *Designs, Codes, and Cryptography*, 4(2):123–128, April 1994. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Hachenberger:1994:CFE**

[95] Dirk Hachenberger. On completely free elements in finite fields. *Designs, Codes, and Cryptography*, 4(2): 129–143, April 1994. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Sabin:1994:RCC**

[96] Roberta Evans Sabin. On row-cyclic codes with algebraic structure. *Designs, Codes, and Cryptography*, 4(2): 145–155, April 1994. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Sali:1994:RSD**

[97] Attila Sali. On the rigidity of spherical $t$-designs that are orbits of finite reflection groups. *Designs, Codes, and Cryptography*, 4(2):157–170, April 1994. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Seguin:1994:CER**

[98] Gérald E. Séguin. A counter-example to a recent result on the $q$-ary image of a $q^s$-ary cyclic code. *Designs, Codes, and Cryptography*, 4(2):171–175, April 1994. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Quinn:1994:SCK**

[99] Kathleen A. S. Quinn. Some constructions for key distribution patterns. *Designs, Codes, and Cryptography*, 4(2): 177–191, April 1994. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Menezes:1994:BR**

[100] Alfred Menezes. Book review. *Designs, Codes, and Cryptography*, 4(2): 193–??, April 1994. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Calderbank:1994:MTI**

[101] A. R. Calderbank and P. C. Fishburn. Maximal three-independent subsets of $\{0,1,2\}^n$. *Designs, Codes, and Cryptography*, 4(3):203–211, 1994. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Heden:1994:BPC**

[102] Olof Heden. A binary perfect code of length 15 and codimension 0. *Designs, Codes, and Cryptography*, 4(3):213–220, 1994. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Ma:1994:SPD**

[103] S. L. Ma. A survey of partial difference sets. *Designs, Codes, and Cryptography*, 4(3):221–261, 1994. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Robshaw:1994:ELC**

[104] M. J. B. Robshaw. On evaluating the linear complexity of a sequence of least

period $2^n$. *Designs, Codes, and Cryptography*, 4(3):263–269, 1994. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**vanEupen:1994:OTC**

[105] M. van Eupen and R. Hill. An optimal ternary $[69, 5, 45]$ code and related codes. *Designs, Codes, and Cryptography*, 4(3):271–282, 1994. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Wan:1994:WHP**

[106] Zhe Xian Wan. The weight hierarchies of the projective codes from nondegenerate quadrics. *Designs, Codes, and Cryptography*, 4(3):283–300, 1994. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Baker:1994:BC**

[107] R. D. Baker and G. L. Ebert. A Bruen chain for $q = 19$. *Designs, Codes, and Cryptography*, 4(4):307–312, 1994. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Chen:1994:EBS**

[108] Yu Qing Chen, Qing Xiang, and Surinder K. Sehgal. An exponent bound on skew Hadamard abelian difference sets. *Designs, Codes, and Cryptography*, 4(4):313–317, 1994. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Jungnickel:1994:NCS**

[109] Dieter Jungnickel and Alexander Pott. A new class of symmetric $(v, k, \lambda)$-designs. *Designs, Codes, and Cryptography*, 4(4):319–325, 1994. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Koukouvinos:1994:SZA**

[110] C. Koukouvinos, S. Kounias, J. Seberry, C. H. Yang, and J. Yang. On sequences with zero autocorrelation. *Designs, Codes, and Cryptography*, 4(4):327–340, 1994. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Mitchell:1994:CAP**

[111] Chris J. Mitchell. Constructing $c$-ary perfect factors. *Designs, Codes, and Cryptography*, 4(4):341–368, 1994. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Stinson:1994:UHA**

[112] D. R. Stinson. Universal hashing and authentication codes. *Designs, Codes, and Cryptography*, 4(4):369–380, 1994. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Zemor:1994:HFC**

[113] Gilles Zémor. Hash functions and Cayley graphs. *Designs, Codes, and Cryptography*, 4(4):381–394, 1994. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Arasu:1995:DSA**

[114] K. T. Arasu and Surinder K. Sehgal. Difference sets in Abelian groups of $p$-rank two. *Designs, Codes, and Cryptography*, 5(1):5–12, January 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/77807`.

**Buratti:1995:PMC**

[115] Marco Buratti. A powerful method for constructing difference families and optimal optical orthogonal codes. *Designs, Codes, and Cryptography*, 5(1): 13–25, January 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/77809`.

**Coster:1995:QSD**

[116] M. J. Coster and W. H. Haemers. Quasi-symmetric designs related to the triangular graph. *Designs, Codes, and Cryptography*, 5(1):27–42, January 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/77812`.

**Lam:1995:QSD**

[117] Clement Lam, Larry Thiel, and Vladimir D. Tonchev. On quasi-symmetric 2-$(28, 12, 11)$ and 2-$(36, 16, 12)$ designs. *Designs, Codes, and Cryptography*, 5(1):43–55, January 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/77815`.

**Mathon:1995:TPO**

[118] Rudolf Mathon and Gordon F. Royle. The translation planes of order 49. *Designs, Codes, and Cryptography*, 5(1): 57–72, January 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/77818`.

**Naccache:1995:CMP**

[119] David Naccache, David M'Raïhi, and Dan Raphaeli. Can Montgomery parasites be avoided? A design methodology based on key and cryptosystem modifications. *Designs, Codes, and Cryptography*, 5(1):73–80, January 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/77820; http://link.springer.com/article/10.1007/BF01388505`.

**Dempwolff:1995:CTP**

[120] U. Dempwolff. Correction to: "Translation planes of order 27" [Des. Codes Cryptogr. **4** (1994), no. 2, 105–121; MR 95a:51012]. *Designs, Codes, and Cryptography*, 5(1):81, January 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). See [93].

**Assaf:1995:CDB**

[121] Ahmed M. Assaf. On covering designs with block size 5 and index 5. *Designs, Codes, and Cryptography*, 5(2): 91–107, March 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/78675`.

**Gillman:1995:CVL**

[122] David Gillman and Ronald L. Rivest. Complete variable-length "fix-free" codes. *Designs, Codes, and Cryptography*, 5(2):109–114, March 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/78676`.

**Paterson:1995:PFB**

[123] Kenneth G. Paterson. Perfect factors in the de Bruijn graph. *Designs, Codes, and Cryptography*, 5(2):

115–138, March 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/78677`.

**Peeters:1995:RNG**

[124] René Peeters. On the $p$-ranks of net graphs. *Designs, Codes, and Cryptography*, 5(2):139–153, March 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/78678`.

**Suchower:1995:NCS**

[125] Stephan J. Suchower. Nonisomorphic complete sets of $F$-rectangles with prime power dimensions. *Designs, Codes, and Cryptography*, 5(2):155–174, March 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/78679`.

**Carpentieri:1995:PTS**

[126] Marco Carpentieri. A perfect threshold secret sharing scheme to identify cheaters. *Designs, Codes, and Cryptography*, 5(3):183–187, May 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/81443`.

**Colbourn:1995:TTD**

[127] Charles J. Colbourn, Jeffrey H. Dinitz, and Mieczysław Wojtas. Thwarts in transversal designs. *Designs, Codes, and Cryptography*, 5(3):189–197, May 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/81444`.

**Craigen:1995:SWM**

[128] R. Craigen. The structure of weighing matrices having large weights. *Designs, Codes, and Cryptography*, 5(3):199–216, May 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/81446`.

**Etzion:1995:BSC**

[129] Tuvi Etzion, Victor Wei, and Zhen Zhang. Bounds on the sizes of constant weight covering codes. *Designs, Codes, and Cryptography*, 5(3):217–239, May 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/81447`.

**Gopalakrishnan:1995:TCN**

[130] K. Gopalakrishnan and D. R. Stinson. Three characterizations of non-binary correlation-immune and resilient functions. *Designs, Codes, and Cryptography*, 5(3):241–251, May 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/81448`.

**Munemasa:1995:PSC**

[131] Akihiro Munemasa. On perfect $t$-shift codes in Abelian groups. *Designs, Codes, and Cryptography*, 5(3):253–259, May 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/81449`.

**OKeefe:1995:KDP**

[132] Christine M. O'Keefe. Key distribution patterns using Minkowski planes. *Designs, Codes, and Cryptography*, 5

(3):261–267, May 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/81450`.

**Trung:1995:CAS**

[133] Tran Van Trung. On the construction of authentication and secrecy codes. *Designs, Codes, and Cryptography*, 5 (3):269–280, May 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/81452`.

**Key:1995:ECS**

[134] J. D. Key and F. E. Sullivan. Erratum: "Codes of Steiner triple and quadruple systems" [Des. Codes Cryptogr. **3** (1993), no. 2, 117–125; MR 94e:05050]. *Designs, Codes, and Cryptography*, 5(3):281, May 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). See [67, 164].

**Bours:1995:CPD**

[135] Patrick A. H. Bours. On the construction of perfect deletion-correcting codes using design theory. *Designs, Codes, and Cryptography*, 6(1):5–20, July 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/85445`.

**Calderbank:1995:MAC**

[136] A. R. Calderbank and N. J. A. Sloane. Modular and $p$-adic cyclic codes. *Designs, Codes, and Cryptography*, 6 (1):21–35, July 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/85446`.

**Gibson:1995:SDG**

[137] J. K. Gibson. Severely denting the Gabidulin version of the McEliece public key cryptosystem. *Designs, Codes, and Cryptography*, 6(1):37–45, July 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/85447`.

**Hurlbert:1995:NCB**

[138] Glenn Hurlbert and Garth Isaak. New constructions for de Bruijn tori. *Designs, Codes, and Cryptography*, 6 (1):47–56, July 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/85448`.

**Ma:1995:RDS**

[139] S. L. Ma and Bernhard Schmidt. On $(p^a, p, p^a, p^{a-1})$-relative difference sets. *Designs, Codes, and Cryptography*, 6 (1):57–71, July 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/85449`.

**Martin:1995:AGB**

[140] W. J. Martin and X. J. Zhu. Anticodes for the Grassman and bilinear forms graphs. *Designs, Codes, and Cryptography*, 6(1):73–79, July 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/85451`.

**Harada:1995:NED**

[141] Masaaki Harada and Hiroshi Kimura. New extremal doubly-even $[64, 32, 12]$ codes. *Designs, Codes, and Cryptography*, 6(2):91–96, September 1995.

CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/87693`.

**Huffman:1995:EES**

[142] W. Cary Huffman and Vladimir D. Tonchev. The existence of extremal self-dual $[50, 25, 10]$ codes and quasi-symmetric 2-$(49, 9, 6)$ designs. *Designs, Codes, and Cryptography*, 6(2): 97–106, September 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/87694`.

**Meyn:1995:EPP**

[143] Helmut Meyn. Explicit $N$-polynomials of 2-power degree over finite fields, I. *Designs, Codes, and Cryptography*, 6 (2):107–116, September 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/87695`.

**Scheidler:1995:PKC**

[144] Renate Scheidler and Hugh C. Williams. A public-key cryptosystem utilizing cyclotomic fields. *Designs, Codes, and Cryptography*, 6(2):117–131, September 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/87696`.

**Shalaby:1995:DPB**

[145] N. Shalaby and J. Yin. Directed packings with block size 5 and even $\nu$. *Designs, Codes, and Cryptography*, 6(2): 133–142, September 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/87697`.

**vanDijk:1995:IRP**

[146] Marten van Dijk. On the information rate of perfect secret sharing schemes. *Designs, Codes, and Cryptography*, 6 (2):143–169, September 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/87698`.

**Dey:1995:SIM**

[147] P. Dey and J. L. Hayden. On symmetric incidence matrices of projective planes. *Designs, Codes, and Cryptography*, 6(3):179–188, November 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/93420`.

**Glynn:1995:CGC**

[148] D. G. Glynn and J. W. P. Hirschfeld. On the classification of geometric codes by polynomial functions. *Designs, Codes, and Cryptography*, 6(3):189–204, November 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/93421`.

**Johansson:1995:ACN**

[149] Thomas Johansson. Authentication codes for nontrusting parties obtained from rank metric codes. *Designs, Codes, and Cryptography*, 6(3):205–218, November 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/93422`.

**Klein:1995:TNB**

[150] Yaron Klein, Simon Litsyn, and Alexander Vardy. Two new bounds

on the size of binary codes with a minimum distance of three. *Designs, Codes, and Cryptography*, 6(3):219–227, November 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/93423`.

**Penttila:1995:STA**

[151] Tim Penttila and Gordon F. Royle. Sets of type $(m, n)$ in the affine and projective planes of order nine. *Designs, Codes, and Cryptography*, 6(3): 229–245, November 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/93424`.

**Phelps:1995:KNH**

[152] Kevin T. Phelps and Mike Levan. Kernels of nonlinear Hamming codes. *Designs, Codes, and Cryptography*, 6(3): 247–257, November 1995. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/93425`.

**Anonymous:1996:FI**

[153] Anonymous. Foreword to this issue. *Designs, Codes, and Cryptography*, 7 (1–2):7–8, January 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/102693`.

**Diffie:1996:NSE**

[154] Whitfield Diffie. The national security establishment and the development of public-key cryptography. *Designs, Codes, and Cryptography*, 7(1–2):9–12, January 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/102697`. Special issue dedicated to Gustavus J. Simmons.

**Fischer:1996:NSC**

[155] Mary Fischer. "and now for something completely different" (the Egyptologist and the cryptographer: a personal reminiscence). *Designs, Codes, and Cryptography*, 7(1–2):13–15, January 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/102698`. Special issue dedicated to Gustavus J. Simmons.

**Beth:1996:WBM**

[156] Thomas Beth. Watching the Bhang meter and flying through dirt. *Designs, Codes, and Cryptography*, 7(1–2):17–25, January 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/102700`.

**Syverson:1996:FLC**

[157] Paul Syverson and Catherine Meadows. A formal language for cryptographic protocol requirements. *Designs, Codes, and Cryptography*, 7(1–2):27–59, January 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/102719`. Special issue dedicated to Gustavus J. Simmons.

**Nyberg:1996:MRS**

[158] Kaisa Nyberg and Rainer A. Rueppel. Message recovery for signature schemes based on the discrete logarithm problem. *Designs, Codes, and Cryptography*, 7(1–2):61–81, January 1996. CODEN DCCREC. ISSN

0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/102701`.

**Safavi-Naini:1996:ACP**

[159] R. Safavi-Naini and L. Tombak. Authentication codes in plaintext and chosen-content attacks. *Designs, Codes, and Cryptography*, 7(1–2):83–99, January 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/102703`. Special issue dedicated to Gustavus J. Simmons.

**Mitchell:1996:ASP**

[160] C. J. Mitchell, F. C. Piper, M. Walker, and P. Wild. Authentication schemes, perfect local randomizers, perfect secrecy and secret sharing schemes. *Designs, Codes, and Cryptography*, 7(1–2):101–110, January 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/102706`. Special issue dedicated to Gustavus J. Simmons.

**Zhang:1996:CSC**

[161] Xian-Mo Zhang and Yuliang Zheng. Characterizing the structures of cryptographic functions satisfying the propagation criterion for almost all vectors. *Designs, Codes, and Cryptography*, 7(1–2):111–134, January 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/102708`. Special issue dedicated to Gustavus J. Simmons.

**Gollmann:1996:RIR**

[162] Dieter Gollmann, Yongfei Han, and Chris J. Mitchell. Redundant integer representations and fast exponentiation. *Designs, Codes, and Cryptography*, 7(1–2):135–151, January 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/102709`. Special issue dedicated to Gustavus J. Simmons.

**Scheidler:1996:KER**

[163] R. Scheidler, A. Stein, and Hugh C. Williams. Key-exchange in real quadratic congruence function fields. *Designs, Codes, and Cryptography*, 7 (1–2):153–174, January 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/102711`. Special issue dedicated to Gustavus J. Simmons.

**Key:1996:CCS**

[164] J. D. Key and F. E. Sullivan. Correction to: "Codes of Steiner triple and quadruple systems" [Des. Codes Cryptogr. **3** (1993), no. 2, 117–125; MR 94e:05050]. *Designs, Codes, and Cryptography*, 7(1–2):175, January 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). Special issue dedicated to Gustavus J. Simmons. See [67, 134].

**Ashikhmin:1996:FDA**

[165] Alexey E. Ashikhmin and Simon N. Litsyn. Fast decoding algorithms for first order Reed–Muller and related codes. *Designs, Codes, and Cryptography*, 7(3):187–214, March 1996. CODEN DCCREC. ISSN

0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/105392`.

**Berger:1996:AGA**

[166] Thierry P. Berger. On the automorphism groups of affine-invariant codes. *Designs, Codes, and Cryptography*, 7 (3):215–221, March 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/105393`.

**Gulliver:1996:NGR**

[167] T. Aaron Gulliver and Vijay K. Bhargava. New good rate $(m-1)/pm$ ternary and quaternary quasi-cyclic codes. *Designs, Codes, and Cryptography*, 7(3):223–233, March 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/105394`.

**VanEupen:1996:NTC**

[168] Marijn Van Eupen, Noboru Hamada, and Yoko Watamori. The nonexistence of ternary $[50, 5, 32]$ codes. *Designs, Codes, and Cryptography*, 7(3): 235–237, March 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/105395`.

**Rees:1996:CCA**

[169] Rolf S. Rees and Douglas R. Stinson. Combinatorial characterizations of authentication codes. II. *Designs, Codes, and Cryptography*, 7(3):239–259, March 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/105397`.

**Jungnickel:1996:LWG**

[170] Dieter Jungnickel and Günter Pickert. A life's work in geometry: An homage to Hanfried Lenz. *Designs, Codes, and Cryptography*, 8(1–2):9–22, May 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/110870`. Special issue dedicated to Hanfried Lenz.

**Arasu:1996:ICC**

[171] K. T. Arasu and Alexander Pott. Impossibility of a certain cyclotomic equation with applications to difference sets. *Designs, Codes, and Cryptography*, 8 (1–2):23–27, May 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/110871`. Special issue dedicated to Hanfried Lenz.

**Baartmans:1996:BCS**

[172] Alphonse Baartmans, Ivan Landjev, and Vladimir D. Tonchev. On the binary codes of Steiner triple systems. *Designs, Codes, and Cryptography*, 8 (1–2):29–43, May 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/110873`. Special issue dedicated to Hanfried Lenz.

**Bailey:1996:OPDa**

[173] R. A. Bailey. Orthogonal partitions in designed experiments. *Designs, Codes, and Cryptography*, 8(1–2):45–77, May 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/110874`. Special issue dedicated to Hanfried Lenz. See corrected reprint [188].

**Baker:1996:RFS**

[174] R. D. Baker and G. L. Ebert. Regulus-free spreads of PG$(3, q)$. *Designs, Codes, and Cryptography*, 8(1–2):79–89, May 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/110875`. Special issue dedicated to Hanfried Lenz.

**Beth:1996:DCC**

[175] Thomas Beth. Designs, codes and crypts — a puzzle altogether. *Designs, Codes, and Cryptography*, 8(1–2):91–101, May 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/110876`. Special issue dedicated to Hanfried Lenz.

**Bryant:1996:CSH**

[176] Darryn E. Bryant, D. G. Hoffman, and C. A. Rodger. 5-cycle systems with holes. *Designs, Codes, and Cryptography*, 8(1–2):103–108, May 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/110877`. Special issue dedicated to Hanfried Lenz.

**Cameron:1996:SAGa**

[177] Peter J. Cameron. Stories about groups and sequences. *Designs, Codes, and Cryptography*, 8(1–2):109–133, May 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/110879`. Special issue dedicated to Hanfried Lenz. See corrected reprint [189].

**Hachenberger:1996:GAK**

[178] Dirk Hachenberger. Groups admitting a Kantor family and a factorized normal subgroup. *Designs, Codes, and Cryptography*, 8(1–2):135–143, May 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/110880`. Special issue dedicated to Hanfried Lenz.

**Haemers:1996:SSR**

[179] Willem H. Haemers and Vladimir D. Tonchev. Spreads in strongly regular graphs. *Designs, Codes, and Cryptography*, 8(1–2):145–157, May 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/110881`. Special issue dedicated to Hanfried Lenz.

**Jungnickel:1996:CBC**

[180] Dieter Jungnickel, Marialuisa J. de Resmini, and Scott A. Vanstone. Codes based on complete graphs. *Designs, Codes, and Cryptography*, 8(1–2):159–165, May 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/110883`. Special issue dedicated to Hanfried Lenz.

**Leung:1996:CPD**

[181] Ka Hin Leung and Siu Lun Ma. A construction of partial difference sets in $Z_{p^2} \times Z_{p^2} \times \cdots \times Z_{p^2}$. *Designs, Codes, and Cryptography*, 8(1–2):167–172, May 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/110884`. Special issue dedicated to Hanfried Lenz.

**Pascasio:1996:CPN**

[182] Arlene A. Pascasio, Cheryl E. Praeger, and Blessilda P. Raposa. On the characterisation of $\mathrm{AG}(n, q)$ by its parameters as a nearly triply regular design. *Designs, Codes, and Cryptography*, 8(1–2):173–179, May 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/110885`. Special issue dedicated to Hanfried Lenz.

**Payne:1996:FTC**

[183] S. E. Payne. The fundamental theorem of $q$-clan geometry. *Designs, Codes, and Cryptography*, 8(1–2):181–202, May 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/110886`. Special issue dedicated to Hanfried Lenz.

**Pickert:1996:EGC**

[184] Günter Pickert. Extension of gravity centers configuration to Steiner triple systems. *Designs, Codes, and Cryptography*, 8(1–2):203–214, May 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/110887`. Special issue dedicated to Hanfried Lenz.

**Ray-Chaudhuri:1996:CPD**

[185] D. K. Ray-Chaudhuri and Qing Xiang. Constructions of partial difference sets and relative difference sets using Galois rings. *Designs, Codes, and Cryptography*, 8(1–2):215–227, May 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/110888`. Special issue dedicated to Hanfried Lenz.

**Shult:1996:SPS**

[186] E. E. Shult and J. A. Thas. $m$-systems and partial $m$-systems of polar spaces. *Designs, Codes, and Cryptography*, 8(1–2):229–238, May 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/110891`. Special issue dedicated to Hanfried Lenz.

**Siemon:1996:PIS**

[187] Helmut Siemon. Piotrowski's infinite series of Steiner quadruple systems revisited. *Designs, Codes, and Cryptography*, 8(1–2):239–254, May 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/110894`. Special issue dedicated to Hanfried Lenz.

**Bailey:1996:OPDb**

[188] R. A. Bailey. Orthogonal partitions in designed experiments. Corrected reprint. *Designs, Codes, and Cryptography*, 8(3):45–77, June 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). See [173].

**Cameron:1996:SAGb**

[189] Peter J. Cameron. Stories about groups and sequences. Corrected reprint of "Stories about groups and sequences" [Des. Codes Cryptogr. **8** (1996), no. 1–2, 109–133; MR 97f:20004a]. *Designs, Codes, and Cryptography*, 8(3): 109–133, June 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). See [177].

**Domingo-Ferrer:1996:ARU**

[190] Josep Domingo-Ferrer. Achieving rights untransferability with client-independent servers. *Designs, Codes, and Cryptography*, 8(3):263–271, June 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/115284`.

**Harada:1996:ENE**

[191] Masaaki Harada. Existence of new extremal doubly-even codes and extremal singly-even codes. *Designs, Codes, and Cryptography*, 8(3):273–283, June 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/116715`.

**Hou:1996:CR**

[192] Xiang dong Hou. The covering radius of $R(1,9)$ in $R(4,9)$. *Designs, Codes, and Cryptography*, 8(3):285–292, June 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/116716`.

**Janwa:1996:MPK**

[193] Heeralal Janwa and Oscar Moreno. McEliece public key cryptosystems using algebraic-geometric codes. *Designs, Codes, and Cryptography*, 8(3):293–307, June 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/116717`.

**Landgev:1996:CGD**

[194] Ivan N. Landgev. Constructions of group divisible designs. *Designs, Codes, and Cryptography*, 8(3):309–318, June 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/116718`.

**Meisner:1996:NCG**

[195] D. B. Meisner. New classes of groups containing Menon difference sets. *Designs, Codes, and Cryptography*, 8(3):319–325, June 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/116719`.

**Szonyi:1996:CCP**

[196] Tamás Szönyi. On cyclic caps in projective spaces. *Designs, Codes, and Cryptography*, 8(3):327–332, June 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/116720`.

**Tonchev:1996:P**

[197] Vladimir Tonchev. Preface. *Designs, Codes, and Cryptography*, 9(1):5–6, August 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). Special Issue containing papers presented at the Second Upper Michigan Combinatorics Workshop on Designs, Codes and Geometries.

**Assmus:1996:DCU**

[198] E. F. Assmus, Jr. and J. D. Key. Designs and codes: an update. *Designs, Codes, and Cryptography*, 9(1):7–27, August 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/119816`. Second Upper Michigan Combinatorics Work-

shop on Designs, Codes and Geometries (Houghton, MI, 1994).

**Bierbrauer:1996:SHS**

[199] Jürgen Bierbrauer, Stephen Black, and Yves Edel. Some $t$-homogeneous sets of permutations. *Designs, Codes, and Cryptography*, 9(1):29–38, August 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/119817`. Second Upper Michigan Combinatorics Workshop on Designs, Codes and Geometries (Houghton, MI, 1994).

**Bonn:1996:FLG**

[200] Jeffrey T. Bonn. Forcing linearity on greedy codes. *Designs, Codes, and Cryptography*, 9(1):39–49, August 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/119818`. Second Upper Michigan Combinatorics Workshop on Designs, Codes and Geometries (Houghton, MI, 1994).

**Carpenter:1996:ODD**

[201] Laurel L. Carpenter. Oval designs in Desarguesian projective planes. *Designs, Codes, and Cryptography*, 9(1): 51–59, August 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/119819`. Second Upper Michigan Combinatorics Workshop on Designs, Codes and Geometries (Houghton, MI, 1994).

**Colbourn:1996:CDM**

[202] Charles J. Colbourn and Donald L. Kreher. Concerning difference matrices. *Designs, Codes, and Cryptography*, 9(1):61–70, August 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/119820`. Second Upper Michigan Combinatorics Workshop on Designs, Codes and Geometries (Houghton, MI, 1994).

**Kimura:1996:HMD**

[203] Hiroshi Kimura. Hadamard matrices and dihedral groups. *Designs, Codes, and Cryptography*, 9(1):71–77, August 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/119821`. Second Upper Michigan Combinatorics Workshop on Designs, Codes and Geometries (Houghton, MI, 1994).

**Monroe:1996:SOG**

[204] Laura Monroe. Self-orthogonal greedy codes. *Designs, Codes, and Cryptography*, 9(1):79–83, August 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/119822`. Second Upper Michigan Combinatorics Workshop on Designs, Codes and Geometries (Houghton, MI, 1994).

**Pinelis:1996:MNE**

[205] Iosif Pinelis. On the minimal number of even submatrices of 0-1 matrices. *Designs, Codes, and Cryptography*, 9(1):85–93, August 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/119823`. Second Upper Michigan Combinatorics Workshop on Designs, Codes and Geometries (Houghton, MI, 1994).

**Thas:1996:AHP**

[206] J. A. Thas. $k$-arcs, hyperovals, partial flocks and flocks. *Designs, Codes, and Cryptography*, 9(1):95–104, August 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/119826`. Second Upper Michigan Combinatorics Workshop on Designs, Codes and Geometries (Houghton, MI, 1994).

**Trung:1996:GTD**

[207] Tran Van Trung. A generalization of a theorem of Dehon for simple $t$-designs. *Designs, Codes, and Cryptography*, 9(1):105–114, August 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/119828`. Second Upper Michigan Combinatorics Workshop on Designs, Codes and Geometries (Houghton, MI, 1994).

**Walker:1996:NAM**

[208] Judy L. Walker. A new approach to the main conjecture on algebraic-geometric MDS codes. *Designs, Codes, and Cryptography*, 9(1):115–120, August 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/119830`. Second Upper Michigan Combinatorics Workshop on Designs, Codes and Geometries (Houghton, MI, 1994).

**Buyuklieva:1996:SES**

[209] Stefka Buyuklieva and Vassil Yorgov. Singly-even self-dual codes of length 40. *Designs, Codes, and Cryptography*, 9 (2):131–141, October 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/111646`.

**deBoer:1996:AMC**

[210] Mario A. de Boer. Almost MDS codes. *Designs, Codes, and Cryptography*, 9 (2):143–155, October 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/111647`.

**Park:1996:NMD**

[211] Chang-Seop Park, Gui-Liang Feng, and Kenneth K. Tzeng. The new minimum distance bounds of Goppa codes and their decoding. *Designs, Codes, and Cryptography*, 9(2):157–176, October 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/111648`.

**Roth:1996:SNC**

[212] Ron M. Roth. Spectral-null codes and null spaces of Hadamard submatrices. *Designs, Codes, and Cryptography*, 9 (2):177–191, October 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/111649`.

**Scheerhorn:1996:DPC**

[213] Alfred Scheerhorn. Dickson polynomials, completely normal polynomials and the cyclic module structure of specific extensions of finite fields. *Designs, Codes, and Cryptography*, 9(2):193–202, October 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/111650`.

**Shokrollahi:1996:SC**

[214] M. A. Shokrollahi. Stickelberger codes. *Designs, Codes, and Cryptography*, 9 (2):203–213, October 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/111651`.

**Skorobogatov:1996:NRM**

[215] A. N. Skorobogatov. On the number of representations of matroids over finite fields. *Designs, Codes, and Cryptography*, 9(2):215–226, October 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/111652`.

**Ceccherini:1996:GT**

[216] Pier Vittorio Ceccherini. Giuseppe Tallini (1930–1995). *Designs, Codes, and Cryptography*, 9(3):237–245, November 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/113933`.

**Tallini:1996:CPI**

[217] Giuseppe Tallini. Combinatorial problems in infinite spaces. *Designs, Codes, and Cryptography*, 9(3):247–249, November 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/113934`.

**Blackburn:1996:NSS**

[218] S. R. Blackburn. A note on sequences with the shift and add property. *Designs, Codes, and Cryptography*, 9(3): 251–256, November 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/113935`.

**Helleseth:1996:CSW**

[219] Tor Helleseth, P. Vijay Kumar, and Abhijit Shanbhag. Codes with the same weight distributions as the Goethals codes and the Delsarte-Goethals codes. *Designs, Codes, and Cryptography*, 9 (3):257–266, November 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/113936`.

**Jackson:1996:PSS**

[220] Wen-Ai Jackson and Keith M. Martin. Perfect secret sharing schemes on five participants. *Designs, Codes, and Cryptography*, 9(3):267–286, November 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/113937`.

**Jackson:1996:CMT**

[221] Wen-Ai Jackson, Keith M. Martin, and Christine M. O'Keefe. A construction for multisecret threshold schemes. *Designs, Codes, and Cryptography*, 9(3): 287–303, November 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/113938`.

**Maurer:1996:NIP**

[222] Ueli M. Maurer and Yacov Yacobi. A non-interactive public-key distribution system. *Designs, Codes, and Cryptography*, 9(3):305–316, November 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/113939`.

**Huybrechts:1996:GO**

[223] Cécile Huybrechts and Antonio Pasini. On $c^{n-2}.c^*$ geometries of order 2. *Designs, Codes, and Cryptography*, 9(3): 317–330, November 1996. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/113940`.

**Cohen:1997:LPB**

[224] Stephen D. Cohen. The length of primitive BCH codes with minimal covering radius. *Designs, Codes, and Cryptography*, 10(1):5–16, January 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/124965`.

**Conan:1997:EGN**

[225] Jean Conan. On the enumeration and generation of nonweight equivalent rate $\frac{1}{2}$ convolutional codes. *Designs, Codes, and Cryptography*, 10(1): 17–27, January 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/124966`.

**Gacs:1997:TRB**

[226] András Gács, Péter Sziklai, and Tamás Szőnyi. Two remarks on blocking sets and nuclei in planes of prime order. *Designs, Codes, and Cryptography*, 10(1): 29–39, January 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/124967`.

**Hamada:1997:NSC**

[227] Noboru Hamada. A necessary and sufficient condition for the existence of some ternary $[n, k, d]$ codes meeting the Greismer bound. *Designs, Codes, and Cryptography*, 10(1):41–56, January 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/124968`.

**Hiss:1997:IMR**

[228] Gerhard Hiss. On the incidence matrix of the Ree unital. *Designs, Codes, and Cryptography*, 10(1):57–62, January 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/124969`.

**vanEupen:1997:CSO**

[229] Marijn van Eupen and Petr Lisoněk. Classification of some optimal ternary linear codes of small length. *Designs, Codes, and Cryptography*, 10(1): 63–84, January 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/124970`.

**vanZanten:1997:LOL**

[230] A. J. van Zanten. Lexicographic order and linearity. *Designs, Codes, and Cryptography*, 10(1):85–97, January 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/124971`.

**Jungnickel:1997:P**

[231] Dieter Jungnickel. Preface. *Designs, Codes, and Cryptography*, 10(2): 107, February 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). Special issue #2 dedicated to Hanfried Lenz.

**Bonisoli:1997:SMD**

[232] Arrigo Bonisoli, Gábor Korchmáros, and Tamás Szönyi. Some multiply derived translation planes with $\mathrm{SL}(2,5)$ as an inherited collineation group in the translation complement. *Designs, Codes, and Cryptography*, 10(2):109–114, February 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/122512`.

**Bouzette:1997:TNP**

[233] Sabine Bouzette, Francis Buekenhout, Edmond Dony, and Alain Gottcheiner. A theory of nets for polyhedra and polytopes related to incidence geometries. *Designs, Codes, and Cryptography*, 10(2):115–136, February 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/122513`.

**Broecker:1997:CCS**

[234] Claudia Broecker, Ralph-Hardo Schulz, and Gernot Stroth. Check character systems using Chevalley groups. *Designs, Codes, and Cryptography*, 10(2):137–143, February 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/122514`.

**Bruen:1997:PQS**

[235] Aiden A. Bruen and David L. Wehlau. Partitioning quadrics, symmetric group divisible designs and caps. *Designs, Codes, and Cryptography*, 10(2):145–155, February 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/122515`.

**Calderbank:1997:CCG**

[236] A. R. Calderbank and Gary M. McGuire. Construction of a $(64, 2^{37}, 12)$ code via Galois rings. *Designs, Codes, and Cryptography*, 10(2):157–165, February 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/122516`.

**Coulter:1997:PFP**

[237] Robert S. Coulter and Rex W. Matthews. Planar functions and planes of Lenz-Barlotti class II. *Designs, Codes, and Cryptography*, 10(2):167–184, February 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/122517`.

**Jackson:1997:GDC**

[238] Wen-Ai Jackson and Peter R. Wild. On GMW designs and cyclic Hadamard designs. *Designs, Codes, and Cryptography*, 10(2):185–191, February 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/122518`.

**Johnson:1997:MPS**

[239] Norman L. Johnson and Guglielmo Lunardon. Maximal partial spreads and flocks. *Designs, Codes, and Cryptography*, 10(2):193–202, February 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/122519`.

**Ling:1997:PBD**

[240] Alan C. H. Ling, Xiaojun Zhu, Charles J. Colbourn, and Ronald C.

Mullin. Pairwise balanced designs with consecutive block sizes. *Designs, Codes, and Cryptography*, 10(2):203–222, February 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/122520`.

**Ma:1997:DSC**

[241] Siu Lun Ma and Bernhard Schmidt. Difference sets corresponding to a class of symmetric designs. *Designs, Codes, and Cryptography*, 10(2):223–236, February 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/122521`.

**Mathon:1997:UUP**

[242] Rudolf Mathon and Tran Van Trung. Unitals and unitary polarities in symmetric designs. *Designs, Codes, and Cryptography*, 10(2):237–250, February 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/122522`.

**Metsch:1997:ELS**

[243] Klaus Metsch. Embedding the linear structure of planar spaces into projective spaces. *Designs, Codes, and Cryptography*, 10(2):251–263, February 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/122523`.

**Abel:1997:EIT**

[244] R. J. R. Abel, Charles J. Colbourn, Jianxing Yin, and Hantao Zhang. Existence of incomplete transversal designs with block size five and any index $\lambda$. *Designs, Codes, and Cryptography*, 10 (3):275–307, March 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/124750`.

**Batten:1997:BSD**

[245] Lynn Margaret Batten, Kris Coolsaet, and Anne Penfold Street. Blocking sets in $(v, \{2, 4\}, 1)$-designs. *Designs, Codes, and Cryptography*, 10(3): 309–314, March 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/124751`.

**Bernard:1997:LCN**

[246] Margaret Ann Bernard and Bhu Dev Sharma. Linear codes with non-uniform error correction capability. *Designs, Codes, and Cryptography*, 10(3): 315–323, March 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/124752`.

**Erdmann:1997:ADM**

[247] Diane Erdmann and Sean Murphy. An approximate distribution for the maximum order complexity. *Designs, Codes, and Cryptography*, 10(3):325–339, March 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/124753`.

**Faldum:1997:CSD**

[248] A. Faldum and W. Willems. Codes of small defect. *Designs, Codes, and Cryptography*, 10(3):341–350, March 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (elec-

tronic). URL `http://www.wkap.nl/oasis.htm/124754`.

**Houston:1997:LMD**

[249] Alice E. D. Houston. On the limit of maximal density of sequences with a perfect linear complexity profile. *Designs, Codes, and Cryptography*, 10(3): 351–359, March 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/124755`.

**Wan:1997:SSC**

[250] Zhe-Xian Wan. State spaces of convolutional codes. *Designs, Codes, and Cryptography*, 10(3):361–369, March 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/124756`.

**Buratti:1997:DF**

[251] Marco Buratti. From a $(G, k, 1)$ to a $(Ck \oplus G, k, 1)$ difference family. *Designs, Codes, and Cryptography*, 11 (1):5–9, April 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/125555`.

**Buratti:1997:RDF**

[252] Marco Buratti. On resolvable difference families. *Designs, Codes, and Cryptography*, 11(1):11–23, April 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/125556`.

**Gulliver:1997:CED**

[253] T. Aaron Gulliver and Masaaki Harada. Classification of extremal double circulant formally self-dual even codes. *Designs, Codes, and Cryptography*, 11(1):25–35, April 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/125554`.

**Lamken:1997:EPG**

[254] E. R. Lamken. The existence of partitioned generalized balanced tournament designs with block size 3. *Designs, Codes, and Cryptography*, 11 (1):37–71, April 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/125557`.

**Ma:1997:FSR**

[255] Siu Lun Ma and Surinder K. Sehgal. A family of semi-regular divisible difference sets. *Designs, Codes, and Cryptography*, 11(1):73–78, April 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/125558`.

**Perkins:1997:CDP**

[256] Stephanie Perkins. Codes with a disparity property. *Designs, Codes, and Cryptography*, 11(1):79–97, April 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/125559`.

**Blundo:1997:TBI**

[257] Carlo Blundo, Alfredo de Santis, Roberto de Simone, and Ugo Vaccaro. Tight bounds on the information rate of secret sharing schemes. *Designs, Codes, and Cryptography*, 11 (2):107–122, May 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-

7586 (electronic). URL http://www.wkap.nl/oasis.htm/129332.

**Greig:1997:RBI**

[258] Malcolm Greig and Julian Abel. Resolvable balanced incomplete block designs with block size 8. *Designs, Codes, and Cryptography*, 11(2):123–140, May 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/129333.

**Gulliver:1997:WED**

[259] T. Aaron Gulliver and Masaaki Harada. Weight enumerators of double circulant codes and new extremal self-dual codes. *Designs, Codes, and Cryptography*, 11(2):141–150, May 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/129334.

**Ostergaard:1997:NTB**

[260] Patric R. J. Östergård and Heikki O. Hämäläinen. A new table of binary/ternary mixed covering codes. *Designs, Codes, and Cryptography*, 11(2):151–178, May 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/129335.

**Verheul:1997:CPV**

[261] Eric R. Verheul and Henk C. A. van Tilborg. Constructions and properties of $k$ out of $n$ visual secret sharing schemes. *Designs, Codes, and Cryptography*, 11(2):179–196, May 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/129336.

**Bierbrauer:1997:UHG**

[262] Jürgen Bierbrauer. Universal hashing and geometric codes. *Designs, Codes, and Cryptography*, 11(3):207–221, July 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/131331.

**Blackburn:1997:GRI**

[263] Simon R. Blackburn. A generalized rational interpolation problem and the solution of the Welch-Berlekamp key equation. *Designs, Codes, and Cryptography*, 11(3):223–234, July 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/131332.

**Blundo:1997:DRR**

[264] C. Blundo, A. Giorgio Gaggia, and D. R. Stinson. On the dealer's randomness required in secret sharing schemes. *Designs, Codes, and Cryptography*, 11(3):235–259, July 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/131333.

**Brouwer:1997:CBP**

[265] A. E. Brouwer and M. van Eupen. The correspondence between projective codes and 2-weight codes. *Designs, Codes, and Cryptography*, 11(3):261–266, July 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/131334.

**Davis:1997:USC**

[266] James A. Davis and Surinder K. Sehgal. Using the simplex code to construct relative difference sets in 2-groups. *Designs, Codes, and Cryptography*, 11(3):267–277, July 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/131335`.

**Khosrovshahi:1997:TSD**

[267] G. B. Khosrovshahi, A. Nowzari-Dalini, and R. Torabi. Trading signed designs and some new $4-(12,5,4)$ designs. *Designs, Codes, and Cryptography*, 11(3):279–288, July 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/131336`.

**Klapper:1997:CCQ**

[268] A. Klapper. Cross-correlations of quadratic form sequences in odd characteristic. *Designs, Codes, and Cryptography*, 11(3):289–305, July 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/131337`.

**Boukliev:1997:SNO**

[269] Iliya Boukliev. Some new optimal ternary linear codes. *Designs, Codes, and Cryptography*, 12(1):5–11, September 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/136843`.

**Burmester:1997:GZK**

[270] Mike Burmester, Yvo G. Desmedt, Fred Piper, and Michael Walker. A general zero-knowledge scheme. *Designs, Codes, and Cryptography*, 12(1): 13–37, September 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/136844`.

**Buyuklieva:1997:BSD**

[271] Stefka Buyuklieva. On the binary self-dual codes with an automorphism of order 2. *Designs, Codes, and Cryptography*, 12(1):39–48, September 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/136845`.

**Craigen:1997:HMW**

[272] R. Craigen and H. Kharaghani. Hadamard matrices from weighing matrices via signed groups. *Designs, Codes, and Cryptography*, 12(1):49–58, September 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/136846`.

**Franek:1997:LSM**

[273] F. Franek, A. Rosa, and T. S. Griggs. Large sets of mutually almost disjoint Steiner triple systems not from Steiner quadruple systems. *Designs, Codes, and Cryptography*, 12(1):59–67, September 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/136847`.

**Hayden:1997:GHM**

[274] J. L. Hayden. Generalized Hadamard matrices. *Designs, Codes, and Cryptography*, 12(1):69–73, September 1997.

CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/136848`.

**Hou:1997:RMC**

[275] Xiang-Dong Hou. The Reed–Muller code $R(1,7)$ is normal. *Designs, Codes, and Cryptography*, 12(1):75–82, September 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/136849`.

**Maruta:1997:AGB**

[276] Tatsuya Maruta. On the achievement of the Griesmer bound. *Designs, Codes, and Cryptography*, 12(1):83–87, September 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/136850`.

**Storme:1997:NRC**

[277] L. Storme. Normal rational curves over prime fields. *Designs, Codes, and Cryptography*, 12(1):89–96, September 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/136851`.

**Lefmann:1997:SPC**

[278] Hanno Lefmann, Pavel Pudlák, and Petr Savický. On sparse parity check matrices. *Designs, Codes, and Cryptography*, 12(2):107–130, October 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/139524`.

**Levenshtein:1997:SOA**

[279] Vladimir I. Levenshtein. Split orthogonal arrays and maximum independent resilient systems of functions. *Designs, Codes, and Cryptography*, 12(2):131–160, October 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/139525`.

**vanDijk:1997:LCS**

[280] Marten van Dijk. A linear construction of secret sharing schemes. *Designs, Codes, and Cryptography*, 12(2):161–201, October 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/139526`.

**Kranakis:1997:I**

[281] Evangelos Kranakis and Paul C. Van Oorschot. Introduction. *Designs, Codes, and Cryptography*, 12(3):213, November 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/142380`.

**Stinson:1997:SMU**

[282] Doug R. Stinson. On some methods for unconditionally secure key distribution and broadcast encryption. *Designs, Codes, and Cryptography*, 12(3):215–243, November 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/141935`. Selected areas in cryptography (Ottawa, ON, 1995).

**Rogier:1997:SCB**

[283] N. Rogier and Pascal Chauvaud. MD2 is not secure without the check-

sum byte. *Designs, Codes, and Cryptography*, 12(3):245–251, November 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/141937`. Selected areas in cryptography (Ottawa, ON, 1995).

**Rijmen:1997:WNS**

[284] Vincent Rijmen, Bart Preneel, and Erik De Win. On weaknesses of non-surjective round functions. *Designs, Codes, and Cryptography*, 12(3):253–266, November 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/141938`. Selected areas in cryptography (Ottawa, ON, 1995).

**Lee:1997:RCL**

[285] J. Lee, H. M. Heys, and S. E. Tavares. Resistance of a CAST-like encryption algorithm to linear and differential cryptanalysis. *Designs, Codes, and Cryptography*, 12(3):267–282, November 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/141939`. Selected areas in cryptography (Ottawa, ON, 1995).

**Adams:1997:CSC**

[286] Carlisle M. Adams. Constructing symmetric ciphers using the CAST design procedure. *Designs, Codes, and Cryptography*, 12(3):283–316, November 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/141940`. Selected areas in cryptography (Ottawa, ON, 1995).

**Abel:1998:BIB**

[287] R. Julian R. Abel and Malcolm Greig. Balanced incomplete block designs with block size 7. *Designs, Codes, and Cryptography*, 13(1):5–30, January 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/145563`.

**Assmus:1998:LDS**

[288] E. F. Assmus, Jr. Linearly derived Steiner triple systems. *Designs, Codes, and Cryptography*, 13(1):31–49, January 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/145565`.

**Bruen:1998:CCS**

[289] Aiden Bruen, Lucien Haddad, and David Wehlau. Caps and colouring Steiner triple systems. *Designs, Codes, and Cryptography*, 13(1):51–55, January 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/145566`.

**McGuire:1998:CHR**

[290] Gary McGuire, Vladimir D. Tonchev, and Harold N. Ward. Characterizing the Hermitian and Ree unitals on 28 points. *Designs, Codes, and Cryptography*, 13(1):57–61, January 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/145567`.

**Siemon:1998:NTC**

[291] Helmut Siemon. A number-theoretic conjecture and the existence of $S$-

cyclic Steiner quadruple systems. *Designs, Codes, and Cryptography*, 13(1): 63–94, January 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/145568`. See erratum [333] and also [93].

**Bryant:1998:ODC**

[292] Darryn E. Bryant and A. Khodkar. On orthogonal double covers of graphs. *Designs, Codes, and Cryptography*, 13(2): 103–105, February 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/147885`.

**Casse:1998:BCA**

[293] L. R. A. Casse, K. M. Martin, and P. R. Wild. Bounds and characterizations of authentication/secrecy schemes. *Designs, Codes, and Cryptography*, 13(2): 107–129, February 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/147886`.

**Davis:1998:NFS**

[294] James A. Davis, Jonathan Jedwab, and Miranda Mowbray. New families of semi-regular relative difference sets. *Designs, Codes, and Cryptography*, 13 (2):131–146, February 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/147887`.

**Fitzgerald:1998:DAV**

[295] J. Fitzgerald and R. F. Lax. Decoding affine variety codes using Gröbner bases. *Designs, Codes, and Cryptography*, 13(2):147–158, February 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/147888`.

**Mackenzie-Fleming:1998:RCD**

[296] Kirsten Mackenzie-Fleming. A recursive construction for 2-designs. *Designs, Codes, and Cryptography*, 13(2): 159–164, February 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/147889`.

**Hamada:1998:NTC**

[297] Noboru Hamada and Marijn van Eupen. The nonexistence of ternary $[38, 6, 23]$ codes. *Designs, Codes, and Cryptography*, 13(2):165–172, February 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/147890`.

**Michael:1998:SHM**

[298] T. S. Michael and W. D. Wallis. Skew-Hadamard matrices and the Smith Normal Form. *Designs, Codes, and Cryptography*, 13(2):173–176, February 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/147891`.

**Morgan:1998:EFH**

[299] Ilene H. Morgan. Equiorthogonal frequency hypercubes: Preliminary theory. *Designs, Codes, and Cryptography*, 13(2):177–185, February 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/147892`.

**Panigrahi:1998:CGQ**

[300] Pratima Panigrahi. The collinearity graph of the $O^-(8,2)$ quadric is not geometrisable. *Designs, Codes, and Cryptography*, 13(2):187–198, February 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/147893`.

**Zanella:1998:LSF**

[301] Corrado Zanella. Linear sections of the finite Veronese varieties and authentication systems defined using geometry. *Designs, Codes, and Cryptography*, 13 (2):199–212, February 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/147894`.

**Baicheva:1998:CRT**

[302] Tsonka Stefanova Baicheva. The covering radius of ternary cyclic codes with length up to 25. *Designs, Codes, and Cryptography*, 13(3):223–227, March 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/150396`.

**Brennan:1998:AIM**

[303] J. J. Brennan and Bruce Geist. Analysis of iterated modular exponentiation: the orbits of $x^\alpha \bmod N$. *Designs, Codes, and Cryptography*, 13(3): 229–245, March 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/150398`.

**Chen:1998:CDS**

[304] Yu Qing Chen. A construction of difference sets. *Designs, Codes, and Cryptography*, 13(3):247–250, March 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/150399`.

**Dokovic:1998:NPC**

[305] Dragomir Ž. Đoković. Note on periodic complementary sets of binary sequences. *Designs, Codes, and Cryptography*, 13(3):251–256, March 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/150401`.

**Gulliver:1998:CED**

[306] T. Aaron Gulliver and Masaaki Harada. Classification of extremal double circulant self-dual codes of lengths 64 to 72. *Designs, Codes, and Cryptography*, 13(3):257–269, March 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/150403`.

**Harada:1998:NET**

[307] Masaaki Harada. New extremal type II codes over $\mathbf{Z}_4$. *Designs, Codes, and Cryptography*, 13(3):271–284, March 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/150404`.

**Krasikov:1998:BSC**

[308] Ilia Krasikov and Simon Litsyn. Bounds on spectra of codes with known dual distance. *Designs, Codes, and Cryptography*, 13(3):285–297, March 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (elec-

tronic). URL `http://www.wkap.nl/oasis.htm/150405`.

**Safavi-Naini:1998:TST**

[309] R. Safavi-Naini. Three systems for threshold generation of authenticators. *Designs, Codes, and Cryptography*, 13 (3):299–312, March 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/150408`.

**Zain:1998:QCM**

[310] A. A. Zain and B. Sundar Rajan. Quasideterminant characterization of MDS group codes over Abelian groups. *Designs, Codes, and Cryptography*, 13 (3):313–330, March 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/150410`.

**Bennett:1998:PMP**

[311] F. E. Bennett, J. Yin, H. Zhang, and R. J. R. Abel. Perfect Mendelsohn packing designs with block size five. *Designs, Codes, and Cryptography*, 14 (1):5–22, April 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/153098`.

**Bezzateev:1998:SBG**

[312] Sergei V. Bezzateev and Natalia A. Shekhunova. A subclass of binary Goppa codes with improved estimation of the code dimension. *Designs, Codes, and Cryptography*, 14 (1):23–38, April 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/153099`.

**Jaffe:1998:CLC**

[313] David B. Jaffe and Vladimir D. Tonchev. Computing linear codes and unitals. *Designs, Codes, and Cryptography*, 14(1):39–52, April 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/153100`.

**Joye:1998:REC**

[314] Marc Joye and Jean-Jacques Quisquater. Reducing the elliptic curve cryptosystem of Meyer-Müller to the cryptosystem of Rabin-Williams. *Designs, Codes, and Cryptography*, 14(1):53–56, April 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/153101`.

**Koc:1998:MM**

[315] Çetin K. Koç and Tolga Acar. Montgomery multiplication in GF($2^k$). *Designs, Codes, and Cryptography*, 14 (1):57–69, April 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/153102`.

**Laihonen:1998:UBM**

[316] Tero Laihonen and Simon Litsyn. On upper bounds for minimum distance and covering radius of non-binary codes. *Designs, Codes, and Cryptography*, 14(1):71–80, April 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/153103`.

**Mahmoodi:1998:EPD**

[317] A. Mahmoodi. Existence of perfect 3-deletion-correcting codes. *De-*

*signs, Codes, and Cryptography*, 14 (1):81–87, April 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/153104`.

**Maschietti:1998:DSH**

[318] Antonio Maschietti. Difference sets and hyperovals. *Designs, Codes, and Cryptography*, 14(1):89–98, April 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/153105`.

**Ashikhmin:1998:GHW**

[319] Alexei Ashikhmin. On generalized Hamming weights for Galois ring linear codes. *Designs, Codes, and Cryptography*, 14(2):107–126, May 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/156974`.

**Bruen:1998:NEC**

[320] Aiden A. Bruen and Keldon Drudge. On the non-existence of certain Cameron-Liebler line classes in PG$(3, q)$. *Designs, Codes, and Cryptography*, 14 (2):127–132, May 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/156975`.

**Carlet:1998:ACB**

[321] Claude Carlet and Philippe Guillot. An alternate characterization of the bentness of binary functions, with uniqueness. *Designs, Codes, and Cryptography*, 14(2):133–140, May 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/156976`.

**Colbourn:1998:PCM**

[322] Charles J. Colbourn and Alan C. H. Ling. Point code minimum Steiner triple systems. *Designs, Codes, and Cryptography*, 14(2):141–146, May 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/156977`.

**Ionin:1998:TCS**

[323] Yury J. Ionin. A technique for constructing symmetric designs. *Designs, Codes, and Cryptography*, 14(2): 147–158, May 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/156978`.

**Muller:1998:DLB**

[324] Volker Müller, Scott Vanstone, and Robert Zuccherato. Discrete logarithm based cryptosystems in quadratic function fields of characteristic 2. *Designs, Codes, and Cryptography*, 14(2): 159–178, May 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/156980`.

**Simonis:1998:AAC**

[325] Juriaan Simonis and Alexei Ashikhmin. Almost affine codes. *Designs, Codes, and Cryptography*, 14(2):179–197, May 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/156984`.

**Banihashemi:1998:ICG**

[326] Amir H. Banihashemi and Amir K. Khandani. An inequality on the coding gain of densest lattice packings in successive dimensions. *Designs, Codes, and Cryptography*, 14(3):207–212, September 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/166114`.

**Fripertinger:1998:ECR**

[327] Harald Fripertinger. Enumeration, construction and random generation of block codes. *Designs, Codes, and Cryptography*, 14(3):213–219, September 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/166115`.

**He:1998:SSR**

[328] Jingmin He and Ed Dawson. Shared secret reconstruction. *Designs, Codes, and Cryptography*, 14(3):221–237, September 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/166116`.

**Langevin:1998:WAC**

[329] Philippe Langevin. Weights of Abelian codes. *Designs, Codes, and Cryptography*, 14(3):239–245, September 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/166118`.

**Paterson:1998:RCD**

[330] Kenneth G. Paterson. Root counting, the DFT and the linear complexity of nonlinear filtering. *Designs, Codes, and Cryptography*, 14(3):247–259, September 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/166119`.

**Stinson:1998:SNR**

[331] Doug R. Stinson and Tran Van Trung. Some new results on key distribution patterns and broadcast encryption. *Designs, Codes, and Cryptography*, 14(3):261–279, September 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/166120`.

**vanDijk:1998:USG**

[332] Marten van Dijk, Christian Gehrmann, and Ben Smeets. Unconditionally secure group authentication. *Designs, Codes, and Cryptography*, 14(3):281–296, September 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/166121`.

**Siemon:1998:ENT**

[333] Helmut Siemon. Erratum: "A number-theoretic conjecture and the existence of $S$-cyclic Steiner quadruple systems" [Des. Codes Cryptogr. **13** (1998), no. 1, 63–94; 1 600 695]. *Designs, Codes, and Cryptography*, 14(3):297, September 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). See [291].

**Betten:1998:SDS**

[334] Anton Betten, Adalbert Kerber, Reinhard Laue, and Alfred Wassermann. Simple 8-designs with small parameters. *Designs, Codes, and Cryptography*, 15(1):5–27, October 1998.

CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/168579.

**DePrisco:1998:LBR**

[335] Roberto De Prisco and Alfredo De Santis. On lower bounds for the redundancy of optimal codes. *Designs, Codes, and Cryptography*, 15(1): 29–45, October 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/168580.

**Chen:1998:WHL**

[336] Wende Chen and Torleiv Kløve. Weight hierarchies of linear codes satisfying the chain condition. *Designs, Codes, and Cryptography*, 15(1):47–66, October 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/168581.

**Gehrmann:1998:MUS**

[337] Christian Gehrmann. Multiround unconditionally secure authentication. *Designs, Codes, and Cryptography*, 15 (1):67–86, October 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/168582.

**Kurosawa:1998:NCB**

[338] Kaoru Kurosawa, Koji Okada, Hajime Saido, and Douglas R. Stinson. New combinatorial bounds for authentication codes and key predistribution schemes. *Designs, Codes, and Cryptography*, 15(1):87–100, October 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/168583.

**Anderson:1998:HBR**

[339] Ross Anderson, Cunsheng Ding, Tor Helleseth, and Torleiv Kløve. How to build robust shared control systems. *Designs, Codes, and Cryptography*, 15(2):111–124, 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/181759.

**Carlet:1998:CBF**

[340] Claude Carlet, Pascale Charpin, and Victor Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes, and Cryptography*, 15(2):125–156, 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/181760.

**Chen:1998:NCD**

[341] Wende Chen, Zhi Chen, and Torleiv Kløve. New constructions of disjoint distinct difference sets. *Designs, Codes, and Cryptography*, 15(2):157–165, 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/181761.

**Chen:1998:EDF**

[342] K. Chen and L. Zhu. Existence of $(q, 6, 1)$ difference families with $q$ a prime power. *Designs, Codes, and Cryptography*, 15(2):167–173, 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/181762.

**Helleseth:1998:IFD**

[343] Tor Helleseth, P. Vijay Kumar, and Kyeongcheol Yang. An infinite family of 3-designs from Preparata codes over $Z_4$. *Designs, Codes, and Cryptography*, 15(2):175–181, 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/181763`.

**Kaikkonen:1998:CAP**

[344] Markku Kaikkonen. Codes from affine permutation groups. *Designs, Codes, and Cryptography*, 15(2):183–186, 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/181764`.

**Perera:1998:CGH**

[345] A. A. I. Perera and K. J. Horadam. Cocyclic generalised Hadamard matrices and central relative difference sets. *Designs, Codes, and Cryptography*, 15(2):187–200, 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/181765`.

**Yang:1998:TNI**

[346] Kyeongcheol Yang and Tor Helleseth. Two new infinite families of 3-designs from Kerdock codes over $Z_4$. *Designs, Codes, and Cryptography*, 15 (2):201–214, 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/181767`.

**Arasu:1998:ADS**

[347] K. T. Arasu and S. L. Ma. Abelian difference sets without self-conjugacy. *Designs, Codes, and Cryptography*, 15(3):223–230, December 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/185600`.

**Ball:1998:PUR**

[348] Simeon Ball. Partial unitals and related structures in Desarguesian planes. *Designs, Codes, and Cryptography*, 15(3):231–236, December 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/186357`.

**Bhandari:1998:LBC**

[349] M. C. Bhandari, K. K. P. Chanduka, and A. K. Lal. On lower bounds for covering codes. *Designs, Codes, and Cryptography*, 15(3):237–243, December 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/185601`.

**Landjev:1998:NSO**

[350] Ivan N. Landjev. The nonexistence of some optimal ternary codes of dimension five. *Designs, Codes, and Cryptography*, 15(3):245–258, December 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/185603`.

**Ohmori:1998:CWM**

[351] Hiroyuki Ohmori and Takashi Miyamoto. Construction of weighing matrices $(17, 9)$ having the intersection number 8. *Designs, Codes, and Cryptography*, 15(3):259–269, December 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (elec-

tronic). URL `http://www.wkap.nl/oasis.htm/185604`.

**Shalaby:1998:NOP**

[352] Nabil Shalaby and Jianxing Yin. Nested optimal $\lambda$-packings and $\lambda$-coverings of pairs with triples. *Designs, Codes, and Cryptography*, 15(3): 271–278, December 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/185607`.

**Stevens:1998:LBT**

[353] Brett Stevens, Lucia Moura, and Eric Mendelsohn. Lower bounds for transversal covers. *Designs, Codes, and Cryptography*, 15(3):279–299, December 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/185608`.

**vanDijk:1998:GDC**

[354] Marten van Dijk, Wen-Ai Jackson, and Keith M. Martin. A general decomposition construction for incomplete secret sharing schemes. *Designs, Codes, and Cryptography*, 15(3):301–321, December 1998. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/185609`.

**Bhandari:1999:SRN**

[355] M. C. Bhandari, M. K. Gupta, and A. K. Lal. Some results on NQR codes. *Designs, Codes, and Cryptography*, 16 (1):5–9, January 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/189026`.

**Blake-Wilson:1999:CWC**

[356] Simon Blake-Wilson and Kevin T. Phelps. Constant weight codes and group divisible designs. *Designs, Codes, and Cryptography*, 16(1):11–27, January 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/189027`.

**Davydov:1999:NLC**

[357] Alexander A. Davydov and Patric R. J. Ostergaard. New linear codes with covering radius 2 and odd basis. *Designs, Codes, and Cryptography*, 16(1): 29–39, January 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/189028`.

**Jha:1999:COS**

[358] Vikram Jha and Norman Johnson. Cyclic Ostrom spreads. *Designs, Codes, and Cryptography*, 16(1):41–51, January 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/189029`.

**Kurosawa:1999:ERT**

[359] Kaoru Kurosawa and Wakaha Ogata. Efficient Rabin-type digital signature scheme. *Designs, Codes, and Cryptography*, 16(1):53–64, January 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/189030`.

**Ostergaard:1999:CCC**

[360] Patric R. J. Ostergård and William D. Weakley. Constructing covering codes

with given automorphisms. *Designs, Codes, and Cryptography*, 16(1):65–73, January 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/189031`.

**Padro:1999:DCV**

[361] Carles Padro, Germán Sáez, and Jorge Luis Villar. Detection of cheaters in vector space secret sharing schemes. *Designs, Codes, and Cryptography*, 16 (1):75–85, January 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/189032`.

**Shiromoto:1999:WEL**

[362] Keisuke Shiromoto. The weight enumerator of linear codes over GF($qm$) having generator matrix over GF($q$). *Designs, Codes, and Cryptography*, 16 (1):87–92, January 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/189033`.

**Barg:1999:BMD**

[363] A. Barg and A. Ashikhmin. Binomial moments of the distance distribution and the probability of undetected error. *Designs, Codes, and Cryptography*, 16 (2):103–116, February 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/195203`.

**Buratti:1999:SBC**

[364] Marco Buratti. Some $(17q, 17, 2)$ and $(25q, 25, 3)$ BIBD constructions. *Designs, Codes, and Cryptography*, 16(2): 117–120, February 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/195204`.

**Camion:1999:CIR**

[365] Paul Camion and Anne Canteaut. Correlation-immune and resilient functions over a finite alphabet and their applications in cryptography. *Designs, Codes, and Cryptography*, 16(2):121–149, February 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/195205`.

**Edel:1999:LSC**

[366] Yves Edel and Jürgen Bierbrauer. 41 is the largest size of a cap in PG$(4, 4)$. *Designs, Codes, and Cryptography*, 16(2): 151–160, February 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/195206`.

**Norton:1999:MRF**

[367] Graham Norton. On minimal realization over a finite chain ring. *Designs, Codes, and Cryptography*, 16(2): 161–178, February 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/195207`.

**Phelps:1999:SEC**

[368] Kevin T. Phelps and Mike LeVan. Switching equivalence classes of perfect codes. *Designs, Codes, and Cryptography*, 16(2):179–184, February 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/195208`.

**vanZanten:1999:CCC**

[369] A. J. van Zanten and Agung Lukito. Construction of certain cyclic distance-preserving codes having linear-algebraic characteristics. *Designs, Codes, and Cryptography*, 16(2): 185–199, February 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/195209`.

**Batten:1999:SST**

[370] L. M. Batten and J. M. Dover. Some sets of type in cubic order planes. *Designs, Codes, and Cryptography*, 16(3): 211–213, May 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/199814`.

**Bonnecaze:1999:JPT**

[371] Alexis Bonnecaze, Bernard Mourrain, and Patrick Solé. Jacobi polynomials, type II codes, and designs. *Designs, Codes, and Cryptography*, 16(3): 215–234, May 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/199815`.

**Chateauneuf:1999:CAS**

[372] M. A. Chateauneuf, Charles J. Colbourn, and D. L. Kreher. Covering arrays of strength three. *Designs, Codes, and Cryptography*, 16(3): 235–242, May 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/199816`.

**Egner:1999:HP**

[373] Sebastian Egner and Thomas Beth. How to play $M_{13}$? *Designs, Codes, and Cryptography*, 16(3):243–247, May 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/199817`.

**Friedlander:1999:CBS**

[374] John Friedlander, Michael Larsen, Daniel Lieman, and Igor Shparlinski. On the correlation of binary $M$-sequences. *Designs, Codes, and Cryptography*, 16(3):249–256, May 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/199818`.

**Gaborit:1999:CET**

[375] Philippe Gaborit and Masaaki Harada. Construction of extremal type II codes over $\mathbf{Z}_4$. *Designs, Codes, and Cryptography*, 16(3):257–269, May 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/199820`.

**Martin:1999:DPA**

[376] William J. Martin. Designs in product association schemes. *Designs, Codes, and Cryptography*, 16(3):271–289, May 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/199821`.

**Smeltzer:1999:PCD**

[377] Deirdre Longacher Smeltzer. Properties of codes from difference sets in 2-groups. *Designs, Codes, and Cryptography*, 16(3):291–306, May 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (elec-

tronic). URL `http://www.wkap.nl/oasis.htm/199822`.

**Anonymous:1999:GE**

[378] Anonymous. Guest editorial. *Designs, Codes, and Cryptography*, 17(1–3):5–6, September 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/232072`.

**Key:1999:EFA**

[379] J. D. Key and H. F. Mattson, Jr. Edward F. Assmus, Jr. (1931–1998). *Designs, Codes, and Cryptography*, 17(1–3):7–11, September 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/232073`.

**Anonymous:1999:EA**

[380] Anonymous. Ed Assmus. *Designs, Codes, and Cryptography*, 17(1–3):13–14, September 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/232075`.

**Bruen:1999:LBL**

[381] Aiden A. Bruen and David L. Wehlau. Long binary linear codes and large caps in projective space. *Designs, Codes, and Cryptography*, 17(1–3):37–60, September 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/232077`.

**Schmidt:1999:WMC**

[382] Bernhard Schmidt. Williamson matrices and a conjecture of ito's. *Designs, Codes, and Cryptography*, 17(1–3):61–68, September 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/232078`.

**Chen:1999:FCE**

[383] Yu Qing Chen. On a family of covering extended building sets. *Designs, Codes, and Cryptography*, 17(1–3):69–72, September 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/232079`.

**Ward:1999:IDC**

[384] Harold N. Ward. An introduction to divisible codes. *Designs, Codes, and Cryptography*, 17(1–3):73–79, September 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/232080`.

**Charpin:1999:MDN**

[385] Pascale Charpin, Aimo Tietäväinen, and Victor Zinoviev. On the minimum distances of non-binary cyclic codes. *Designs, Codes, and Cryptography*, 17 (1–3):81–85, September 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/232081`.

**Cohen:1999:CLU**

[386] G. Cohen, J. Rifà, J. Tena, and G. Zémor. On the characterization of linear uniquely decodable codes. *Designs, Codes, and Cryptography*, 17(1–3):87–96, September 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/232083`.

**Thas:1999:EFG**

[387] Joseph A. Thas and Hendrik Van Maldeghem. On embeddings of the flag geometries of projective planes in finite projective spaces. *Designs, Codes, and Cryptography*, 17(1–3):97–104, September 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/232084`.

**Calkin:1999:MWD**

[388] Neil J. Calkin, J. D. Key, and M. J. De Resmini. Minimum weight and dimension formulas for some geometric codes. *Designs, Codes, and Cryptography*, 17(1–3):105–120, September 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/232085`.

**Tonchev:1999:LPC**

[389] Vladimir D. Tonchev. Linear perfect codes and a characterization of the classical designs. *Designs, Codes, and Cryptography*, 17(1–3):121–128, September 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/232086`.

**Eisfeld:1999:EBM**

[390] Jörg Eisfeld. The eigenspaces of the Bose–Mesner-algebras of the association schemes corresponding to projective spaces and polar spaces. *Designs, Codes, and Cryptography*, 17(1–3):129–150, September 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/232087`.

**Hill:1999:ETL**

[391] Ray Hill. An extension theorem for linear codes. *Designs, Codes, and Cryptography*, 17(1–3):151–157, September 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/232088`.

**Ionin:1999:BSD**

[392] Yury J. Ionin. Building symmetric designs with building sets. *Designs, Codes, and Cryptography*, 17(1–3):159–175, September 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/232090`.

**Dobbertin:1999:APK**

[393] Hans Dobbertin. Another proof of Kasami's theorem. *Designs, Codes, and Cryptography*, 17(1–3):177–180, September 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/232091`.

**Betten:1999:SDP**

[394] Anton Betten, Reinhard Laue, and Alfred Wassermann. A Steiner 5-design on 36 points. *Designs, Codes, and Cryptography*, 17(1–3):181–186, September 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/232092`.

**Haemers:1999:BCS**

[395] Willem H. Haemers, René Peeters, and Jeroen M. van Rijckevorsel. Binary codes of strongly regular graphs. *Designs, Codes, and Cryptography*, 17(1–3):187–209, September 1999. CODEN

DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/232093`.

**Xiang:1999:MNF**

[396] Qing Xiang. Maximally nonlinear functions and bent functions. *Designs, Codes, and Cryptography*, 17(1–3):211–218, September 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/232094`.

**Metsch:1999:BBT**

[397] Klaus Metsch. A Bose-Burton theorem for elliptic polar spaces. *Designs, Codes, and Cryptography*, 17(1–3):219–224, September 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/232095`.

**Dillon:1999:MDS**

[398] J. F. Dillon. Multiplicative difference sets via additive characters. *Designs, Codes, and Cryptography*, 17(1–3):225–235, September 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/232096`.

**Ball:1999:UMB**

[399] Simeon Ball, Aart Blokhuis, and Christine M. O'Keefe. On unitals with many Baer sublines. *Designs, Codes, and Cryptography*, 17(1–3):237–252, September 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/232097`.

**Ebert:1999:CSL**

[400] G. L. Ebert and J. W. P. Hirschfeld. Complete systems of lines on a Hermitian surface over a finite field. *Designs, Codes, and Cryptography*, 17(1–3):253–268, September 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/232098`.

**Helleseth:1999:LGC**

[401] Tor Helleseth and Victor Zinoviev. On $Z_4$-linear Goethals codes and Kloosterman sums. *Designs, Codes, and Cryptography*, 17(1–3):269–288, September 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/232099`.

**Wilson:1999:SHD**

[402] Richard M. Wilson. Signed hypergraph designs and diagonal forms for some incidence matrices. *Designs, Codes, and Cryptography*, 17(1–3):289–297, September 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/232100`.

**Blokhuis:1999:UED**

[403] A. Blokhuis and A. E. Brouwer. The universal embedding dimension of the near polygon on the 1-factors of a complete graph. *Designs, Codes, and Cryptography*, 17(1–3):299–303, September 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/233540`.

**Davis:1999:NFR**

[404] James A. Davis and Jonathan Jedwab. A new family of relative difference sets in 2-groups. *Designs, Codes, and Cryptography*, 17(1–3):305–312, September 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/233540`.

**Jungnickel:1999:E**

[405] Dieter Jungnickel and Jack van Lint. Editorial. *Designs, Codes, and Cryptography*, 18(1–3):5–6, December 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/240902`.

**Arasu:1999:AQP**

[406] K. T. Arasu and N. J. Voss. Answering a question of Pott on almost perfect sequences. *Designs, Codes, and Cryptography*, 18(1–3):7–10, December 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/240903`.

**Bachoc:1999:HWE**

[407] Christine Bachoc. On harmonic weight enumerators of binary codes. *Designs, Codes, and Cryptography*, 18(1–3):11–28, December 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/240905`.

**Berger:1999:AGB**

[408] Thierry P. Berger and Pascale Charpin. The automorphism groups of BCH codes and of some affine-invariant codes over extension fields. *Designs, Codes, and Cryptography*, 18(1–3):29–53, December 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/240906`.

**Broughton:1999:SOQ**

[409] Wayne Broughton and Gary McGuire. Some observations on quasi-3 designs and Hadamard matrices. *Designs, Codes, and Cryptography*, 18(1–3):55–61, December 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/240907`.

**Brown:1999:TFC**

[410] Matthew R. Brown, Christine M. O'Keefe, and Tim Penttila. Triads, flocks of conics and $Q^{-(5,1)}$. *Designs, Codes, and Cryptography*, 18(1–3):63–70, December 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/240908`.

**Cohen:1999:AC**

[411] Gérard D. Cohen, Sylvia B. Encheva, and Gilles Zémor. Antichain codes. *Designs, Codes, and Cryptography*, 18 (1–3):71–80, December 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/240909`.

**Cusack:1999:SLS**

[412] Charles A. Cusack and Spyros S. Magliveras. Semiregular large sets. *Designs, Codes, and Cryptography*, 18(1–3):81–87, December 1999. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/240911.

**deCaen:1999:ASR**

[413] D. de Caen and E. R. van Dam. Association schemes related to Kasami codes and Kerdock sets. *Designs, Codes, and Cryptography*, 18(1–3):89–102, December 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/240912.

**Duursma:1999:SWE**

[414] Iwan Duursma, Tor Helleseth, Chunming Rong, and Kyeongcheol Yang. Split weight enumerators for the Preparata codes with applications to designs. *Designs, Codes, and Cryptography*, 18(1–3):103–124, December 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/240913.

**Fields:1999:CEE**

[415] J. E. Fields, P. Gaborit, W. C. Huffman, and V. Pless. On the classification of extremal even formally self-dual codes. *Designs, Codes, and Cryptography*, 18(1–3):125–148, December 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/240915.

**Gao:1999:GPS**

[416] Shuhong Gao and Jason Howell. A general polynomial sieve. *Designs, Codes, and Cryptography*, 18(1–3):149–157, December 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/240916.

**Ho:1999:IMC**

[417] Chat Yin Ho. Incidence matrices and collineations of finite projective planes. *Designs, Codes, and Cryptography*, 18(1–3):159–162, December 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/240917. See correction [555].

**Janwa:1999:SUB**

[418] H. Janwa and H. F. Mattson, Jr. Some upper bounds on the covering radii of linear codes over and their applications. *Designs, Codes, and Cryptography*, 18(1–3):163–181, December 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/240918.

**Khosrovshahi:1999:HCA**

[419] G. B. Khosrovshahi and Reza Naserasr. Hypergraphical codes arising from binary trades. *Designs, Codes, and Cryptography*, 18(1–3):183–186, December 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/240920.

**Mathon:1999:DPD**

[420] Rudolf Mathon and Tran van Trung. Directed $t$-packings and directed $t$-Steiner systems. *Designs, Codes, and Cryptography*, 18(1–3):187–198, December 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/240921.

**Metsch:1999:PS**

[421] Klaus Metsch and L. Storme. Partial $t$-spreads in PG$(2t + 1, q)$. *Designs, Codes, and Cryptography*, 18(1–3):199–216, December 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/240923`.

**Prince:1999:FTA**

[422] Alan R. Prince. Flag-transitive affine planes of order 64. *Designs, Codes, and Cryptography*, 18(1–3):217–221, December 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/240924`.

**Svanstrom:1999:CPT**

[423] Mattias Svanström. A class of perfect ternary constant-weight codes. *Designs, Codes, and Cryptography*, 18(1–3):223–229, December 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/240925`.

**vanLint:1999:PTC**

[424] Jack van Lint and Ludo Tolhuizen. On perfect ternary constant weight codes. *Designs, Codes, and Cryptography*, 18(1–3):231–234, December 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/240926`.

**Szhonyi:1999:EAM**

[425] Tamás Szhonyi. On the embedding of $(k, p)$-arcs is maximal arcs. *Designs, Codes, and Cryptography*, 18(1–3):235–246, December 1999. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/240927`.

**Dinitz:2000:HCR**

[426] J. H. Dinitz and E. R. Lamken. HOPs and COPs: Room frames with partitionable transversals. *Designs, Codes, and Cryptography*, 19(1):5–26, January 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/202743`.

**Vance:2000:GGC**

[427] Todd D. Vance. A gap in GRM code weight distributions. *Designs, Codes, and Cryptography*, 19(1):27–43, January 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/202744`.

**Zhang:2000:RDD**

[428] Xian-Mo Zhang, Yuliang Zheng, and Hideki Imai. Relating differential distribution tables to other properties of substitution boxes. *Designs, Codes, and Cryptography*, 19(1):45–63, January 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/202745`.

**Koblitz:2000:GE**

[429] Neal Koblitz. Guest editorial. *Designs, Codes, and Cryptography*, 19(2–3):75–76, March 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/253934`.

**Blake-Wilson:2000:ISM**

[430] Simon Blake-Wilson. Information security, mathematics, and public-key cryptography. *Designs, Codes, and Cryptography*, 19(2–3):77–99, March 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/253935`.

**Lenstra:2000:IF**

[431] Arjen K. Lenstra. Integer factoring. *Designs, Codes, and Cryptography*, 19 (2–3):101–128, March 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/253936`.

**Odlyzko:2000:DLP**

[432] Andrew Odlyzko. Discrete logarithms: The past and the future. *Designs, Codes, and Cryptography*, 19(2–3):129–145, March 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.research.att.com/~amo/doc/discrete.logs.future.abst`; `http://www.research.att.com/~amo/doc/discrete.logs.future.pdf`; `http://www.research.att.com/~amo/doc/discrete.logs.future.ps`; `http://www.research.att.com/~amo/doc/discrete.logs.future.tex`; `http://www.wkap.nl/oasis.htm/253937`.

**Maurer:2000:DHP**

[433] Ueli M. Maurer and Stefan Wolf. The Diffie–Hellman protocol. *Designs, Codes, and Cryptography*, 19(2–3):147–171, March 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/253938`.

**Koblitz:2000:SEC**

[434] Neal Koblitz, Alfred Menezes, and Scott Vanstone. The state of elliptic curve cryptography. *Designs, Codes, and Cryptography*, 19(2–3):173–193, March 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/253939`.

**Solinas:2000:EAK**

[435] Jerome A. Solinas. Efficient arithmetic on Koblitz curves. *Designs, Codes, and Cryptography*, 19(2–3):195–249, March 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/253940`.

**Silverman:2000:XCE**

[436] Joseph H. Silverman. The Xedni calculus and the elliptic curve discrete logarithm problem. *Designs, Codes, and Cryptography*, 20(1):5–40, April 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/256958`.

**Jacobson:2000:AXC**

[437] Michael J. Jacobson, Neal Koblitz, Joseph H. Silverman, Andreas Stein, and Edlyn Teske. Analysis of the Xedni calculus attack. *Designs, Codes, and Cryptography*, 20(1):41–64, April 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/256957`.

**McQuillan:2000:PHP**

[438] James M. McQuillan. Pencils of hyperconics in projective planes of characteristic two. *Designs, Codes, and Cryptography*, 20(1):65–71, April 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/256959`.

**Wolfmann:2000:DSZ**

[439] Jacques Wolfmann. Difference sets in $Z_4^m$ and $F_2^{2m}$. *Designs, Codes, and Cryptography*, 20(1):73–88, April 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/256960`.

**Schulz:2000:ACW**

[440] Ralph-Hardo Schulz and Antonino Giorgio Spera. Automorphisms of constant weight codes and of divisible designs. *Designs, Codes, and Cryptography*, 20 (1):89–97, April 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/256961`.

**Bommier:2000:BQC**

[441] Grégoire Bommier and Francis Blanchet. Binary quasi-cyclic Goppa codes. *Designs, Codes, and Cryptography*, 20(2): 107–124, June 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/264688`.

**Norton:2000:KEC**

[442] Graham H. Norton and Ana Salagean-Mandache. On the key equation over a commutative ring. *Designs, Codes, and Cryptography*, 20(2):125–141, June 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/264689`.

**Bonisoli:2000:MPP**

[443] Arrigo Bonisoli and Antonio Cossidente. Mixed partitions of projective geometries. *Designs, Codes, and Cryptography*, 20(2):143–154, June 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/264690`.

**Halbutogullari:2000:PMU**

[444] A. Halbutogullari and C. K. Koc. Parallel multiplication in using polynomial residue arithmetic. *Designs, Codes, and Cryptography*, 20(2):155–173, June 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/264691`.

**Patarin:2000:CMI**

[445] Jacques Patarin. Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'98. *Designs, Codes, and Cryptography*, 20(2):175–209, June 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/264692`.

**Colbourn:2000:MKS**

[446] Charles J. Colbourn and Sufang Zhao. Maximum Kirkman signal sets for synchronous uni-polar multi-user communication systems. *Designs, Codes, and Cryptography*, 20(3):219–227, July 2000. CODEN DCCREC. ISSN

0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/266672`.

**Encheva:2000:LCT**

[447] Sylvia B. Encheva and Gérard D. Cohen. Linear codes and their coordinate ordering. *Designs, Codes, and Cryptography*, 20(3):229–250, July 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/266673`.

**Hou:2000:BFP**

[448] Xiang dong Hou. Bent functions, partial difference sets, and quasi-Frobenius local rings. *Designs, Codes, and Cryptography*, 20(3):251–268, July 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/266674`.

**Juels:2000:HCC**

[449] Ari Juels and Marcus Peinado. Hiding cliques for cryptographic security. *Designs, Codes, and Cryptography*, 20 (3):269–280, July 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/266675`.

**Obana:2000:CCO**

[450] Satoshi Obana and Kaoru Kurosawa. Combinatorial classification of optimal authentication codes with arbitration. *Designs, Codes, and Cryptography*, 20 (3):281–305, July 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/266676`.

**Panigrahi:2000:NCG**

[451] Pratima Panigrahi. The non-collinearity graph of the $(8, 2)$ quadric is uniquely geometrisable. *Designs, Codes, and Cryptography*, 20(3):307–317, July 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/266677`.

**Polverino:2000:SBS**

[452] Olga Polverino. Small blocking sets in $\mathrm{PG}(2, p)$. *Designs, Codes, and Cryptography*, 20(3):319–324, July 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/266678`.

**Yang:2000:NCV**

[453] Ching-Nung Yang and Chi-Sung Laih. New colored visual secret sharing schemes. *Designs, Codes, and Cryptography*, 20(3):325–336, July 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/266679`.

**Blokhuis:2000:P**

[454] Aart Blokhuis and Willem H. Haemers. Preface. *Designs, Codes, and Cryptography*, 21(1–3):5, October 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/272547`.

**deBruijn:2000:JS**

[455] N. G. de Bruijn. Jaap Seidel 80. *Designs, Codes, and Cryptography*, 21(1–3):7–10, October 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-

7586 (electronic). URL http://www.wkap.nl/oasis.htm/272548.

**Bajnok:2000:SDG**

[456] Béla Bajnok. Spherical designs and generalized sum-free sets in Abelian groups. *Designs, Codes, and Cryptography*, 21(1–3):11–18, October 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/272549.

**Baker:2000:PBS**

[457] R. D. Baker, J. M. Dover, G. L. Ebert, and K. L. Wantz. Perfect Baer subplane partitions and three-dimensional flag-transitive planes. *Designs, Codes, and Cryptography*, 21(1–3):19–39, October 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/272551.

**Beelen:2000:NPP**

[458] Peter Beelen and Ruud Pellikaan. The Newton polygon of plane curves with many rational points. *Designs, Codes, and Cryptography*, 21(1–3):41–67, October 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/272553.

**Brouwer:2000:LPG**

[459] A. E. Brouwer. Locally Paley graphs. *Designs, Codes, and Cryptography*, 21 (1–3):69–76, October 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/272554.

**Bussemaker:2000:SPO**

[460] Frans C. Bussemaker, Willem H. Haemers, and Edward Spence. The search for pseudo orthogonal Latin squares of order six. *Designs, Codes, and Cryptography*, 21(1–3):77–82, October 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/272555.

**vanDam:2000:CAS**

[461] Edwin R. van Dam. A characterization of association schemes from affine spaces. *Designs, Codes, and Cryptography*, 21(1–3):83–86, October 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/272556.

**DeClerck:2000:TWC**

[462] Frank De Clerck and Mario Delanote. Two-weight codes, partial geometries and Steiner systems. *Designs, Codes, and Cryptography*, 21(1–3):87–98, October 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/272557.

**Gramlich:2000:EGP**

[463] Ralf Gramlich and Hendrik Van Maldeghem. Epimorphisms of generalized polygons part 1: Geometrical characterizations. *Designs, Codes, and Cryptography*, 21(1–3):99–111, October 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.wkap.nl/oasis.htm/272558.

**Ionin:2000:SRG**

[464] Yury J. Ionin and M. S. Shrikhande. Strongly regular graphs and designs with three intersection numbers. *Designs, Codes, and Cryptography*, 21(1–3):113–125, October 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/272559`.

**Jurivsic:2000:LAH**

[465] Aleksandar Jurivsic and Jack Koolen. A local approach to 1-homogeneous graphs. *Designs, Codes, and Cryptography*, 21(1–3):127–147, October 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/272560`.

**Koolen:2000:EDR**

[466] Jack Koolen, Monique Laurent, and Alexander Schrijver. Equilateral dimension of the rectilinear space. *Designs, Codes, and Cryptography*, 21(1–3):149–164, October 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/272561`.

**Maks:2000:OSS**

[467] Johannes Maks and Juriaan Simonis. Optimal subcodes of second order Reed–Muller codes and maximal linear spaces of bivectors of maximal rank. *Designs, Codes, and Cryptography*, 21 (1–3):165–180, October 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/272562`.

**Martin:2000:MDB**

[468] William J. Martin. Minimum distance bounds for $s$-regular codes. *Designs, Codes, and Cryptography*, 21(1–3):181–187, October 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/272563`.

**Muhlherr:2000:IBC**

[469] Bernhard Mühlherr. On isomorphisms between Coxeter groups. *Designs, Codes, and Cryptography*, 21(1–3):189, October 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/272564`.

**Rylands:2000:COE**

[470] L. J. Rylands and D. E. Taylor. Constructions for octonion and exceptional Jordan algebras. *Designs, Codes, and Cryptography*, 21(1–3):191–203, October 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/272565`.

**Seress:2000:LFC**

[471] Akos Seress. Large families of cospectral graphs. *Designs, Codes, and Cryptography*, 21(1–3):205–208, October 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/272566`.

**Shaw:2000:SMP**

[472] Ron Shaw. Subsets of PG$(n, 2)$ and maximal partial spreads in PG$(4, 2)$. *Designs, Codes, and Cryptography*, 21 (1–3):209–222, October 2000. CODEN

DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/272567`.

**Siap:2000:NLC**

[473] Irfan Siap and Dijen K. Ray-Chaudhuri. New linear codes over and improvements on bounds. *Designs, Codes, and Cryptography*, 21(1–3):223–233, October 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/272568`.

**Storme:2000:BS**

[474] L. Storme and Zs. Weiner. On 1-blocking sets in $\mathrm{PG}(n, q), n \geq 3$. *Designs, Codes, and Cryptography*, 21(1–3):235–251, October 2000. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/272570`.

**Seress:2001:ALD**

[475] Akos Seress. All lambda-designs with $\lambda = 2^p$ are type-1. *Designs, Codes, and Cryptography*, 22(1):5–17, January 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/281063`.

**Cossidente:2001:VVF**

[476] Antonio Cossidente, Domenico Labbate, and Alessandro Siciliano. Veronese varieties over finite fields and their projections. *Designs, Codes, and Cryptography*, 22(1):19–32, January 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/281064`.

**Dubuc:2001:CLS**

[477] Sylvie Dubuc. Characterization of linear structures. *Designs, Codes, and Cryptography*, 22(1):33–45, January 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/281065`.

**Obana:2001:BCS**

[478] Satoshi Obana and Kaoru Kurosawa. Bounds and combinatorial structure of $(k, n)$ multi-receiver $A$-codes. *Designs, Codes, and Cryptography*, 22(1):47–63, January 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/281066`.

**Daemen:2001:LFB**

[479] Joan Daemen, Lars R. Knudsen, and Vincent Rijmen. Linear frameworks for block ciphers. *Designs, Codes, and Cryptography*, 22(1):65–87, January 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/281067`.

**Gulliver:2001:CIB**

[480] T. Aaron Gulliver and Masaaki Harada. Codes over and improvements to the bounds on ternary linear codes. *Designs, Codes, and Cryptography*, 22(1):89–96, January 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/281069`.

**Enge:2001:R**

[481] Andreas Enge and Dieter Jungnickel. Review. *Designs, Codes, and Cryptography*, 22(1):97–99, January 2001.

CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/281070`.

**Matthews:2001:WPM**

[482] Gretchen L. Matthews. Weierstrass pairs and minimum distance of Goppa codes. *Designs, Codes, and Cryptography*, 22(2):107–121, March 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/311739`.

**Winterhof:2001:SEC**

[483] Arne Winterhof. Some estimates for character sums and applications. *Designs, Codes, and Cryptography*, 22(2): 123–131, March 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/311741`.

**Stinson:2001:SAA**

[484] D. R. Stinson. Something about all or nothing (transforms). *Designs, Codes, and Cryptography*, 22(2): 133–138, March 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/311742`.

**Ward:2001:NCG**

[485] Harold N. Ward. The nonexistence of a $[207, 4, 165]$ code over GF(5). *Designs, Codes, and Cryptography*, 22(2): 139–148, March 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/311743`.

**Tanabe:2001:NPA**

[486] Kenichiro Tanabe. A new proof of the Assmus–Mattson theorem for non-binary codes. *Designs, Codes, and Cryptography*, 22(2):149–155, March 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/311745`.

**Dizon-Garciano:2001:SSA**

[487] Agnes V. Dizon-Garciano and Yutaka Hiramine. On Sylow subgroups of Abelian affine difference sets. *Designs, Codes, and Cryptography*, 22(2): 157–163, March 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/311747`.

**Maruta:2001:NAL**

[488] Tatsuya Maruta. On the nonexistence of $q$-ary linear codes of dimension five. *Designs, Codes, and Cryptography*, 22 (2):165–177, March 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/311749`.

**Johnson:2001:TTP**

[489] Norman L. Johnson. Two-transitive parallelisms. *Designs, Codes, and Cryptography*, 22(2):179–189, March 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/311750`.

**Dempwolff:2001:PRG**

[490] U. Dempwolff. Primitive rank 3 groups on symmetric designs. *Designs, Codes, and Cryptography*, 22(2):

191–207, March 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/311752`.

**Sebille:2001:TES**

[491] Michel Sebille. There exists a simple non trivial $t$-design with an arbitrarily large automorphism group for every $t$. *Designs, Codes, and Cryptography*, 22(3):215–219, January 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/318852`.

**Ahlswede:2001:PCR**

[492] R. Ahlswede, H. K. Aydinian, and L. H. Khachatrian. On perfect codes and related concepts. *Designs, Codes, and Cryptography*, 22(3):221–237, January 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/318853`.

**Scheidler:2001:CQF**

[493] R. Scheidler. Cryptography in quadratic function fields. *Designs, Codes, and Cryptography*, 22(3):239–264, January 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/318854`.

**Kurosawa:2001:CBA**

[494] Kaoru Kurosawa and Satoshi Obana. Combinatorial bounds on authentication codes with arbitration. *Designs, Codes, and Cryptography*, 22(3):265–281, January 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/318855`.

**Jha:2001:ADM**

[495] Vikram Jha and Norman L. Johnson. Almost Desarguesian maximal partial spreads. *Designs, Codes, and Cryptography*, 22(3):283–304, January 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/318856`.

**Davydov:2001:NCC**

[496] Alexander A. Davydov. New constructions of covering codes. *Designs, Codes, and Cryptography*, 22(3):305–316, January 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/318857`.

**Brincat:2001:URS**

[497] Karl Brincat. On the use of RSA as a secret key cryptosystem. *Designs, Codes, and Cryptography*, 22(3):317–329, January 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/318858`.

**Heden:2001:MPS**

[498] Olof Heden. A maximal partial spread of size 45 in PG$(3, 7)$. *Designs, Codes, and Cryptography*, 22(3):331–334, January 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/318859`.

**Shparlinski:2001:LCP**

[499] Igor Shparlinski. On the linear complexity of the power generator. *Designs, Codes, and Cryptography*, 23

(1):5–10, May 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/321868`.

**Betsumiya:2001:BOO**

[500] Koichi Betsumiya and Masaaki Harada. Binary optimal odd formally self-dual codes. *Designs, Codes, and Cryptography*, 23(1):11–22, May 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/321870`.

**Wadayama:2001:ULB**

[501] Tadashi Wadayama, Toru Hada, Koichiro Wakasugi, and Masao Kasahara. Upper and lower bounds on maximum nonlinearity of $n$-input $m$-output Boolean function. *Designs, Codes, and Cryptography*, 23(1):23–34, May 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/321873`.

**Raposa:2001:STB**

[502] Blessilda P. Raposa. Some triple block intersection numbers of Paley 2-designs of QN-type. *Designs, Codes, and Cryptography*, 23(1):35–52, May 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/321874`.

**Enge:2001:EEA**

[503] Andreas Enge. The extended Euclidian algorithm on polynomials, and the computational efficiency of hyperelliptic cryptosystems. *Designs, Codes, and Cryptography*, 23(1):53–74, May 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/321875`.

**Iiams:2001:NCG**

[504] J. E. Iiams. A note on certain 2-groups with Hadamard difference sets. *Designs, Codes, and Cryptography*, 23 (1):75–80, May 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/321876`.

**Mouaha:2001:AAC**

[505] Christophe Mouaha and Gerhard Schiffels. All $q^m$-ary cyclic codes with cyclic $q$-ary image are known. *Designs, Codes, and Cryptography*, 23 (1):81–98, May 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/321877`.

**Yin:2001:CCP**

[506] Jianxing Yin. A combinatorial construction for perfect deletion-correcting codes. *Designs, Codes, and Cryptography*, 23(1):99–110, May 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/321878`.

**Honkala:2001:BMR**

[507] I. Honkala and A. Klapper. Bounds for the multicovering radii of Reed–Muller codes with applications to stream ciphers. *Designs, Codes, and Cryptography*, 23(2):131–146, July 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/333260`.

**Shparlinski:2001:SPS**

[508] Igor Shparlinski. On some properties of the shrinking generator. *Designs, Codes, and Cryptography*, 23(2): 147–156, July 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/333261`.

**Helleseth:2001:NFT**

[509] Tor Helleseth, P. Vijay Kumar, and Halvard Martinsen. A new family of ternary sequences with ideal two-level autocorrelation function. *Designs, Codes, and Cryptography*, 23(2): 157–166, July 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/333262`.

**Gulliver:2001:OTL**

[510] T. Aaron Gulliver and Nikolai Senkevitch. Optimal ternary linear rate 1/2 codes. *Designs, Codes, and Cryptography*, 23(2):167–172, July 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/333263`.

**OConnor:2001:SRE**

[511] Luke O'Connor. On string replacement exponentiation. *Designs, Codes, and Cryptography*, 23(2):173–184, July 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/333264`.

**Cooperstein:2001:HSK**

[512] B. N. Cooperstein. Hyperplane sections of Kantor's unitary ovoids. *Designs, Codes, and Cryptography*, 23(2): 185–196, July 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/333265`.

**Edel:2001:LCS**

[513] Yves Edel and Jürgen Bierbrauer. Large caps in small spaces. *Designs, Codes, and Cryptography*, 23(2): 197–212, July 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/333266`.

**Akiyama:2001:CSR**

[514] Kenzi Akiyama. On certain Schur rings of dimension 4. *Designs, Codes, and Cryptography*, 23(2):213–222, July 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/333267`.

**Krasikov:2001:DDB**

[515] Ilia Krasikov and Simon Litsyn. On the distance distributions of BCH codes and their duals. *Designs, Codes, and Cryptography*, 23(2):223–232, July 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/333268`.

**Buratti:2001:PCD**

[516] Marco Buratti and Fulvio Zuanni. Perfect Cayley designs as generalizations of perfect Mendelsohn designs. *Designs, Codes, and Cryptography*, 23(2): 233–248, July 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/333269`.

**Thas:2001:CTG**

[517] J. A. Thas. Characterizations of translation generalized quadrangles. *Designs, Codes, and Cryptography*, 23(2): 249–258, July 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/333270`.

**Koukouvinos:2001:VMI**

[518] C. Koukouvinos, M. Mitrouli, and Jennifer Seberry. Values of minors of $(1, -1)$ incidence matrices of SBIBDs and their application to the growth problem. *Designs, Codes, and Cryptography*, 23(3):267–282, August 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/336640`.

**Howgrave-Graham:2001:LAD**

[519] N. A. Howgrave-Graham and N. P. Smart. Lattice attacks on digital signature schemes. *Designs, Codes, and Cryptography*, 23(3):283–290, August 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/336641`.

**Sane:2001:PJT**

[520] Sharad Sane. A proof of the Jungnickel-Tonchev conjecture on quasi-multiple quasi-symmetric designs. *Designs, Codes, and Cryptography*, 23(3):291–296, August 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/336642`.

**Joye:2001:HCS**

[521] Marc Joye, Jean-Jacques Quisquater, and Tsuyoshi Takagi. How to choose secret parameters for RSA-type cryptosystems over elliptic curves. *Designs, Codes, and Cryptography*, 23(3): 297–316, August 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/336643`.

**Arasu:2001:DS**

[522] K. T. Arasu and Yu Qing Chen. A difference set in $(\mathbf{Z}/4\mathbf{Z})^3 \times \mathbf{Z}/5\mathbf{Z}$. *Designs, Codes, and Cryptography*, 23(3): 317–324, August 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/336644`.

**Betsumiya:2001:CFS**

[523] Koichi Betsumiya and Masaaki Harada. Classification of formally self-dual even codes of lengths up to 16. *Designs, Codes, and Cryptography*, 23(3):325–332, August 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/336645`.

**Bogdanova:2001:ECC**

[524] Galina T. Bogdanova, Andries E. Brouwer, Stoian N. Kapralov, and Patric R. J. Östergård. Error-correcting codes over an alphabet of four elements. *Designs, Codes, and Cryptography*, 23(3):333–342, August 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/336646`.

**Abdukhalikov:2001:AIC**

[525] Kanat S. Abdukhalikov. Affine invariant and cyclic codes over $p$-adic numbers and finite rings. *Designs, Codes, and Cryptography*, 23(3):343–370, August 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/336647`.

**Hughes:2001:STG**

[526] G. Hughes. Structure theorems for group ring codes with an application to self-dual codes. *Designs, Codes, and Cryptography*, 24(1):5–14, September 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/350095`.

**Chen:2001:TSH**

[527] Houshou Chen and John T. Coffey. Trellis structure and higher weights of extremal self-dual codes. *Designs, Codes, and Cryptography*, 24(1):15–36, September 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/350097`.

**Kovacs:2001:INS**

[528] István Kovács. On the internal nuclei of sets in PG$(n, q)$, $q$ is odd. *Designs, Codes, and Cryptography*, 24(1):37–42, September 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/350098`.

**Boner:2001:MWD**

[529] Chris Boner. Maximal weight divisors of projective Reed–Muller codes. *Designs, Codes, and Cryptography*, 24(1):43–47, September 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/350100`.

**Ng:2001:CMI**

[530] Siaw-Lynn Ng and Michael Walker. On the composition of matroids and ideal secret sharing schemes. *Designs, Codes, and Cryptography*, 24(1):49–67, September 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/350102`.

**Wu:2001:GSS**

[531] D. Wu and L. Zhu. Generalized Steiner systems with a prime power. *Designs, Codes, and Cryptography*, 24(1):69–80, September 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/350103`.

**Veron:2001:TDS**

[532] P. Véron. True dimension of some binary quadratic trace Goppa codes. *Designs, Codes, and Cryptography*, 24(1):81–97, September 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/350104`.

**Nebe:2001:ICG**

[533] Gabriele Nebe, E. M. Rains, and N. J. A. Sloane. The invariants of the Clifford groups. *Designs, Codes, and Cryptography*, 24(1):99–122, September 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/350105`.

**Bokler:2001:MBS**

[534] Martin Bokler. Minimal blocking sets in projective spaces of square order. *Designs, Codes, and Cryptography*, 24 (2):131–144, October 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/353899`.

**Khandani:2001:SMS**

[535] Amir K. Khandani and M. Esmaeili. Successive minimization of the state complexity of the self-dual lattices using Korkin–Zolotarev reduced basis. *Designs, Codes, and Cryptography*, 24 (2):145–158, October 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/353900`.

**Blunck:2001:ECT**

[536] Sönke Blunck. On the existence and construction of tight fourth order quadrature rules for the sphere. *Designs, Codes, and Cryptography*, 24(2): 159–169, October 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/353901`.

**Baliga:2001:CCL**

[537] A. Baliga. Cocyclic codes of length 40. *Designs, Codes, and Cryptography*, 24 (2):171–179, October 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/353903`.

**Lam:2001:WD**

[538] Kwok Yan Lam and Francesco Sica. The weight distribution of. *Designs, Codes, and Cryptography*, 24(2):181–191, October 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/353904`.

**Honkala:2001:CIS**

[539] Iiro Honkala, Tero Laihonen, and Sanna Ranto. On codes identifying sets of vertices in Hamming spaces. *Designs, Codes, and Cryptography*, 24(2): 193–204, October 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/353906`.

**Ball:2001:APP**

[540] Simeon Ball, Ray Hill, Ivan Landjev, and Harold Ward. On $(q^2 + q + 2, q + 2)$-arcs in the projective plane. *Designs, Codes, and Cryptography*, 24(2): 205–224, October 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/353907`.

**Janko:2001:EBT**

[541] Zvonimir Janko, Hadi Kharaghani, and Vladimir D. Tonchev. The existence of a Bush-type Hadamard matrix of order 324 and two new infinite classes of symmetric designs. *Designs, Codes, and Cryptography*, 24(2): 225–232, October 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/353908`.

**Ballico:2001:CPS**

[542] E. Ballico and A. Cossidente. Curves in projective spaces and almost MDS codes. *Designs, Codes, and Cryptography*, 24(2):233–237, October 2001.

CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/353909`.

**Hagita:2001:BBG**

[543] Mariko Hagita and Bernhard Schmidt. Bijections between group rings preserving character sums. *Designs, Codes, and Cryptography*, 24(3):243–254, December 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/356534`.

**Blundo:2001:ISV**

[544] Carlo Blundo, Annalisa De Bonis, and Alfredo De Santis. Improved schemes for visual cryptography. *Designs, Codes, and Cryptography*, 24(3):255–278, December 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/356535`.

**Shparlinski:2001:LCN**

[545] Igor E. Shparlinski and Joseph H. Silverman. On the linear complexity of the Naor–Reingold pseudo-random function from elliptic curves. *Designs, Codes, and Cryptography*, 24(3):279–289, December 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/356536`.

**Lam:2001:DF**

[546] Clement Lam and Ying Miao. Difference families. *Designs, Codes, and Cryptography*, 24(3):291–304, December 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/356538`.

**Tapia-Recillas:2001:UBN**

[547] H. Tapia-Recillas and G. Vega. An upper bound on the number of iterations for transforming a Boolean function of degree greater or equal than 4 to a function of degree 3. *Designs, Codes, and Cryptography*, 24(3):305–312, December 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/356540`.

**Aydin:2001:SGQ**

[548] Nuh Aydin, Irfan Siap, and Dijen K. Ray-Chaudhuri. The structure of 1-generator quasi-twisted codes and new linear codes. *Designs, Codes, and Cryptography*, 24(3):313–326, December 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/356541`.

**Mao:2001:VPE**

[549] Wenbo Mao. Verifiable partial escrow of integer factors. *Designs, Codes, and Cryptography*, 24(3):327–342, December 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/356542`.

**Kim:2001:TRL**

[550] Jeong-Heon Kim and Hong-Yeop Song. Trace representation of Legendre sequences. *Designs, Codes, and Cryptography*, 24(3):343–348, December 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/356544`.

**Bouyuklieva:2002:AOF**

[551] Stefka Bouyuklieva. On the automorphisms of order 2 with fixed points for the extremal self-dual codes of length. *Designs, Codes, and Cryptography*, 25 (1):5–13, January 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/382780`.

**Eisen:2002:TVC**

[552] Philip A. Eisen and Douglas R. Stinson. Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels. *Designs, Codes, and Cryptography*, 25(1):15–61, January 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/382781`.

**Winterhof:2002:PID**

[553] Arne Winterhof. Polynomial interpolation of the discrete logarithm. *Designs, Codes, and Cryptography*, 25(1): 63–72, January 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/382782`.

**Bannai:2002:SDA**

[554] Etsuko Bannai and Mitsuhiro Sawano. Symmetric designs attached to four-weight spin models. *Designs, Codes, and Cryptography*, 25(1):73–90, January 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/382783`.

**Brozovic:2002:CIM**

[555] D. Brozovic, C. Ho, and A. Munemasa. A correction to "Incidence Matrices and Collineations of Finite Projective Planes" by Chat Yin Ho, Designs, Codes and Cryptography, 18 (1999), 159–162. *Designs, Codes, and Cryptography*, 25(1):91–93, January 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/382784`. See [417].

**Blackmore:2002:LBS**

[556] T. Blackmore and G. H. Norton. Lower bounds on the state complexity of geometric Goppa codes. *Designs, Codes, and Cryptography*, 25(1): 95–115, January 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/382785`.

**Arasu:2002:CCH**

[557] K. T. Arasu, Warwick de Launey, and S. L. Ma. On circulant complex Hadamard matrices. *Designs, Codes, and Cryptography*, 25(2):123–142, February 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp007.lwwonline.com/content/getfile/4630/40/1/abstract.htm; http://ipsapp007.lwwonline.com/content/getfile/4630/40/1/fulltext.pdf`.

**Ferret:2002:MLC**

[558] S. Ferret and L. Storme. Minihypers and linear codes meeting the Griesmer bound: Improvements to results of Hamada, Helleseth and Maekawa. *Designs, Codes, and Cryptography*, 25 (2):143–162, February 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://`

ipsapp007.lwwonline.com/content/getfile/4630/40/2/abstract.htm; http://ipsapp007.lwwonline.com/content/getfile/4630/40/2/fulltext.pdf.

**Georgiou:2002:ODT**

[559] Stelios Georgiou, Masaaki Harada, and Christos Koukouvinos. Orthogonal designs and type II codes over $\mathbf{Z}_{2k}$. *Designs, Codes, and Cryptography*, 25 (2):163–174, February 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.lwwonline.com/content/getfile/4630/40/3/abstract.htm; http://ipsapp007.lwwonline.com/content/getfile/4630/40/3/fulltext.pdf.

**Cabello:2002:SSS**

[560] Sergio Cabello, Carles Padró, and Germán Sáez. Secret sharing schemes with detection of cheaters for a general access structure. *Designs, Codes, and Cryptography*, 25(2):175–188, February 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.lwwonline.com/content/getfile/4630/40/4/abstract.htm; http://ipsapp007.lwwonline.com/content/getfile/4630/40/4/fulltext.pdf.

**Bierbrauer:2002:TCC**

[561] Jürgen Bierbrauer. The theory of cyclic codes and a generalization to additive codes. *Designs, Codes, and Cryptography*, 25(2):189–206, February 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.lwwonline.com/content/getfile/4630/40/5/abstract.htm; http://ipsapp007.lwwonline.com/content/getfile/4630/40/5/fulltext.pdf.

**Guajardo:2002:ITI**

[562] Jorge Guajardo and Christof Paar. Itoh–Tsujii inversion in standard basis and its application in cryptography and codes. *Designs, Codes, and Cryptography*, 25(2):207–216, February 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.lwwonline.com/content/getfile/4630/40/6/abstract.htm; http://ipsapp007.lwwonline.com/content/getfile/4630/40/6/fulltext.pdf.

**Biehl:2002:SSB**

[563] Ingrid Biehl, Johannes Buchmann, Safuat Hamdy, and Andreas Meyer. A signature scheme based on the intractability of computing roots. *Designs, Codes, and Cryptography*, 25 (3):223–236, March 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/41/1/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/41/1/fulltext.pdf.

**Giulietti:2002:CAA**

[564] Massimo Giulietti, Fernanda Pambianco, Fernando Torres, and Emanuela Ughi. On complete arcs arising from plane curves. *Designs, Codes, and Cryptography*, 25(3):237–246, March 2002. CODEN DC-

CREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/41/2/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/41/2/fulltext.pdf.

**Thas:2002:TCN**

[565] Koen Thas. A theorem concerning nets arising from generalized quadrangles with a regular point. *Designs, Codes, and Cryptography*, 25 (3):247–253, March 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/41/3/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/41/3/fulltext.pdf.

**Martinez:2002:RVA**

[566] Luis Martínez and Antonio Vera-López. Ring-valued assignments to the points of a $t$-design. *Designs, Codes, and Cryptography*, 25(3):255–262, March 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/41/4/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/41/4/fulltext.pdf.

**Carlet:2002:CSB**

[567] C. Carlet and Yu. Tarannikov. Covering sequences of Boolean functions and their cryptographic significance. *Designs, Codes, and Cryptography*, 25 (3):263–279, March 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/41/5/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/41/5/fulltext.pdf.

**Padro:2002:LKP**

[568] Carles Padró, Ignacio Gracia, Sebastià Martín Molleví, and Paz Morillo. Linear key predistribution schemes. *Designs, Codes, and Cryptography*, 25 (3):281–298, March 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/41/6/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/41/6/fulltext.pdf.

**Polhill:2002:CNP**

[569] John B. Polhill. Constructions of nested partial difference sets with Galois rings. *Designs, Codes, and Cryptography*, 25(3):299–309, March 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/41/7/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/41/7/fulltext.pdf.

**Ballico:2002:HVS**

[570] Edoardo Ballico and Antonio Cossidente. Hermitian Veronesean schemes. *Designs, Codes, and Cryptography*, 25 (3):311–317, March 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/41/8/abstract.htm;

http://ipsapp008.lwwonline.com/content/getfile/4630/41/8/fulltext.pdf.

**Colbourn:2002:PHR**

[571] Charles J. Colbourn, Douglas R. Stinson, and G. H. John van Rees. Preface: In honour of Ronald C. Mullin. *Designs, Codes, and Cryptography*, 26(1–3):5–6, June–July–August 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/42/1/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/42/1/fulltext.pdf.

**Abel:2002:EFH**

[572] R. Julian R. Abel, F. E. Bennett, and G. Ge. The existence of four HMOLS with equal sized holes. *Designs, Codes, and Cryptography*, 26(1–3):7–31, June–July–August 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/42/2/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/42/2/fulltext.pdf.

**Abel:2002:BIB**

[573] R. Julian R. Abel, Iliya Bluskov, and Malcolm Greig. Balanced incomplete block designs with block size 9 and $\lambda = 2, 4, 8$. *Designs, Codes, and Cryptography*, 26(1–3):33–59, June–July–August 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/42/3/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/42/3/fulltext.pdf.

**Bilous:2002:EBS**

[574] R. T. Bilous and G. H. J. van Rees. An enumeration of binary self-dual codes of length 32. *Designs, Codes, and Cryptography*, 26(1–3):61–86, June–July–August 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/42/4/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/42/4/fulltext.pdf.

**Blake:2002:SDS**

[575] Ian F. Blake and Theodoulos Garefalakis. On the security of the digital signature algorithm. *Designs, Codes, and Cryptography*, 26(1–3):87–96, June–July–August 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/42/5/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/42/5/fulltext.pdf.

**Blundo:2002:CBU**

[576] C. Blundo, B. Masucci, D. R. Stinson, and R. Wei. Constructions and bounds for unconditionally secure non-interactive commitment schemes. *Designs, Codes, and Cryptography*, 26(1–3):97–110, June–July–August 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://

ipsapp008.lwwonline.com/content/getfile/4630/42/6/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/42/6/fulltext.pdf.

**Buratti:2002:CDB**

[577] Marco Buratti. Cyclic designs with block size 4 and related optimal optical orthogonal codes. *Designs, Codes, and Cryptography*, 26(1–3):111–125, June–July–August 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/42/7/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/42/7/fulltext.pdf.

**Cao:2002:KPD**

[578] H. Cao and L. Zhu. Kirkman packing designs KPD$(3, 5*, v)$. *Designs, Codes, and Cryptography*, 26(1–3):127–138, June–July–August 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/42/8/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/42/8/fulltext.pdf.

**Charnes:2002:HBF**

[579] Chris Charnes, Martin Rötteler, and Thomas Beth. Homogeneous bent functions, invariants, and designs. *Designs, Codes, and Cryptography*, 26(1–3):139–154, June–July–August 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/42/9/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/42/9/fulltext.pdf.

**Chang:2002:GCD**

[580] Yanxun Chang and Ying Miao. General constructions for double group divisible designs and double frames. *Designs, Codes, and Cryptography*, 26(1–3):155–168, June–July–August 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/42/10/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/42/10/fulltext.pdf.

**Colbourn:2002:EKS**

[581] Charles J. Colbourn, E. R. Lamken, Alan C. H. Ling, and W. H. Mills. The existence of Kirkman squares — doubly resolvable $(v, 3, 1)$-BIBDs. *Designs, Codes, and Cryptography*, 26(1–3):169–196, June–July–August 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/42/11/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/42/11/fulltext.pdf.

**Ding:2002:SPG**

[582] Peng Ding and Jennifer D. Key. Subcodes of the projective generalized Reed–Muller codes spanned by minimum-weight vectors. *Designs, Codes, and Cryptography*, 26(1–3):197–211, June–July–August 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/

getfile/4630/42/12/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/42/12/fulltext.pdf.

**deResmini:2002:AOA**

[583] Marialuisa J. de Resmini, Dina Ghinelli, and Dieter Jungnickel. Arcs and ovals from Abelian groups. *Designs, Codes, and Cryptography*, 26(1–3):213–228, June–July–August 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/42/13/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/42/13/fulltext.pdf.

**Drmota:2002:RPW**

[584] Michael Drmota and Daniel Panario. A rigorous proof of the Waterloo algorithm for the discrete logarithm problem. *Designs, Codes, and Cryptography*, 26(1–3):229–241, June–July–August 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/42/14/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/42/14/fulltext.pdf.

**Franek:2002:LSI**

[585] F. Franek, M. J. Grannell, T. S. Griggs, and A. Rosa. On large sets of $v - 1$ L-intersecting Steiner triple systems of order $v$. *Designs, Codes, and Cryptography*, 26(1–3):243–256, June–July–August 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/42/15/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/42/15/fulltext.pdf.

**Fuji-Hara:2002:NGS**

[586] Ryoh Fuji-Hara and Ying Miao. A note on geometric structures of linear ordered orthogonal arrays and (T,M,S)-nets of low strength. *Designs, Codes, and Cryptography*, 26(1–3):257–263, June–July–August 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/42/16/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/42/16/fulltext.pdf.

**Ge:2002:GDD**

[587] G. Ge and R. S. Rees. On group-divisible designs with block size four and group-type gum1. *Designs, Codes, and Cryptography*, 27(1–2):5–24, October–November 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/43/1/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/43/1/fulltext.pdf.

**Greig:2002:FLS**

[588] Malcolm Greig. Finite linear spaces II. *Designs, Codes, and Cryptography*, 27(1–2):25–47, October–November 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/

getfile/4630/43/2/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/43/2/fulltext.pdf.

**Gronau:2002:ODC**

[589] Hans-Dietrich O. F. Gronau, Martin Grüttmüller, Sven Hartmann, Uwe Leck, and Volker Leck. On orthogonal double covers of graphs. *Designs, Codes, and Cryptography*, 27(1–2):49–91, October–November 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/43/3/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/43/3/fulltext.pdf.

**Jacobson:2002:MAE**

[590] M. J. Jacobson, Jr. and H. C. Williams. Modular arithmetic on elements of small norm in quadratic fields. *Designs, Codes, and Cryptography*, 27(1–2):93–110, October–November 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/43/4/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/43/4/fulltext.pdf.

**Lam:2002:NBN**

[591] Clement Lam and Vladimir D. Tonchev. A new bound on the number of designs with classical affine parameters. *Designs, Codes, and Cryptography*, 27(1–2):111–117, October–November 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/43/5/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/43/5/fulltext.pdf.

**Mathon:2002:PST**

[592] Rudolf Mathon and Anne Penfold Street. Partitioning sets of triples into small planes. *Designs, Codes, and Cryptography*, 27(1–2):119–130, October–November 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/43/6/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/43/6/fulltext.pdf.

**Ostergaard:2002:EDT**

[593] Patric R. J. Östergård and Petteri Kaski. Enumeration of $2-(9,3,\lambda)$ designs and their resolutions. *Designs, Codes, and Cryptography*, 27(1–2):131–137, October–November 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/43/7/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/43/7/fulltext.pdf.

**Phelps:2002:RAP**

[594] Kevin T. Phelps and Mercè Villanueva. Ranks of $q$-ary 1-perfect codes. *Designs, Codes, and Cryptography*, 27(1–2):139–144, October–November 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/

getfile/4630/43/8/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/43/8/fulltext.pdf.

**Shalaby:2002:EPD**

[595] Nabil Shalaby, Jianmin Wang, and Jianxing Yin. Existence of perfect 4-deletion-correcting codes with length six. *Designs, Codes, and Cryptography*, 27(1–2):145–156, October–November 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/43/9/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/43/9/fulltext.pdf.

**Simmons:2002:PEB**

[596] Gustavus J. Simmons. Parity encoding of binary sequences. *Designs, Codes, and Cryptography*, 27(1–2):157–164, October–November 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/43/10/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/43/10/fulltext.pdf.

**Stevens:2002:PAP**

[597] Brett Stevens and Eric Mendelsohn. Packing arrays and packing designs. *Designs, Codes, and Cryptography*, 27(1–2):165–176, October–November 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/43/11/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/43/11/fulltext.pdf.

**Phelps:2002:PCR**

[598] Kevin T. Phelps and Mercè Villanueva. On perfect codes: Rank and kernel. *Designs, Codes, and Cryptography*, 27 (3):183–194, December 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/44/1/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/44/1/fulltext.pdf.

**Jha:2002:TFT**

[599] Vikram Jha and Norman L. Johnson. Transversal-free translation nets. *Designs, Codes, and Cryptography*, 27(3): 195–205, December 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/44/2/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/44/2/fulltext.pdf.

**Tzeng:2002:NAV**

[600] Wen-Guey Tzeng and Chi-Ming Hu. A new approach for visual cryptography. *Designs, Codes, and Cryptography*, 27 (3):207–227, December 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/44/3/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/44/3/fulltext.pdf.

**Murphy:2002:KDB**

[601] S. Murphy and M. J. B. Robshaw. Key-dependent S-boxes and differential cryptanalysis. *Designs, Codes, and Cryptography*, 27(3):229–255, December 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/44/4/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/44/4/fulltext.pdf.

**Ostergaard:2002:DCS**

[602] Patric R. J. Östergård. A $2-(22,8,4)$ design cannot have a $2-(10,4,4)$ subdesign. *Designs, Codes, and Cryptography*, 27(3):257–260, December 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/44/5/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/44/5/fulltext.pdf.

**Ashikhmin:2002:BCR**

[603] A. Ashikhmin and A. Barg. Bounds on the covering radius of linear codes. *Designs, Codes, and Cryptography*, 27 (3):261–269, December 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/44/6/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/44/6/fulltext.pdf.

**Fu:2002:SCB**

[604] Fang-Wei Fu and Victor K.-W. Wei. Self-complementary balanced codes and quasi-symmetric designs. *Designs, Codes, and Cryptography*, 27(3): 271–279, December 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/44/7/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/44/7/fulltext.pdf.

**Horadam:2002:NCC**

[605] K. J. Horadam and P. Udaya. A new construction of central relative $(p^a, p^a, p^a, 1)$-difference sets. *Designs, Codes, and Cryptography*, 27(3):281–295, December 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/44/8/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/44/8/fulltext.pdf.

**Ostergaard:2002:CSH**

[606] Patric R. J. Östergård. Classifying subspaces of Hamming spaces. *Designs, Codes, and Cryptography*, 27(3): 297–305, December 2002. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.lwwonline.com/content/getfile/4630/44/9/abstract.htm; http://ipsapp008.lwwonline.com/content/getfile/4630/44/9/fulltext.pdf.

**Pointcheval:2003:NMC**

[607] David Pointcheval and Guillaume Poupard. A new $\mathcal{NP}$-complete problem and public-key identification. *Designs, Codes, and Cryptography*, 28(1):5–31, January 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/45/1/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/45/1/fulltext.pdf.

**Agou:2003:SPR**

[608] Simon Joseph Agou, Marc Deléglise, and Jean-Louis Nicolas. Short polynomial representations for square roots modulo $p$. *Designs, Codes, and Cryptography*, 28(1):33–44, January 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/45/2/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/45/2/fulltext.pdf.

**Moore:2003:LDS**

[609] Emily H. Moore and Harriet Pollatsek. Looking for difference sets in groups with dihedral images. *Designs, Codes, and Cryptography*, 28(1):45–50, January 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/45/3/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/45/3/fulltext.pdf.

**Govaerts:2003:PCM**

[610] P. Govaerts and L. Storme. On a particular class of minihypers and its applications. I. the result for general $q$. *Designs, Codes, and Cryptography*, 28(1):51–63, January 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/45/4/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/45/4/fulltext.pdf.

**Abatangelo:2003:DDT**

[611] V. Abatangelo and B. Larato. Doubly $\beta$-derived translation planes. *Designs, Codes, and Cryptography*, 28(1):65–74, January 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/45/5/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/45/5/fulltext.pdf.

**Arasu:2003:NFC**

[612] K. T. Arasu and Kevin J. Player. A new family of cyclic difference sets with Singer parameters in characteristic three. *Designs, Codes, and Cryptography*, 28(1):75–91, January 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/45/6/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/45/6/fulltext.pdf.

**Hou:2003:BRF**

[613] Xiang dong Hou. On binary resilient functions. *Designs, Codes, and Cryptography*, 28(1):93–112, January 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (elec-

tronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/45/7/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/45/7/fulltext.pdf.

**Law:2003:EPA**

[614] Laurie Law, Alfred Menezes, Minghua Qu, Jerry Solinas, and Scott Vanstone. An efficient protocol for authenticated key agreement. *Designs, Codes, and Cryptography*, 28(2):119–134, March 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/46/1/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/46/1/fulltext.pdf.

**Konyagin:2003:LCD**

[615] Sergei Konyagin, Tanja Lange, and Igor Shparlinski. Linear complexity of the discrete logarithm. *Designs, Codes, and Cryptography*, 28(2):135–146, March 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/46/2/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/46/2/fulltext.pdf.

**Mavron:2003:QSD**

[616] V. C. Mavron, T. P. McDonough, and M. S. Shrikhande. Quasi-symmetric designs with good blocks and intersection number one. *Designs, Codes, and Cryptography*, 28(2):147–162, March 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/46/3/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/46/3/fulltext.pdf.

**Bouyuklieva:2003:ESD**

[617] Stefka Bouyuklieva and Masaaki Harada. Extremal self-dual $[50, 25, 10]$ codes with automorphisms of order 3 and quasi-symmetric $2-(49, 9, 6)$ designs. *Designs, Codes, and Cryptography*, 28(2):163–169, March 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/46/4/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/46/4/fulltext.pdf.

**Betsumiya:2003:ESD**

[618] Koichi Betsumiya, T. Aaron Gulliver, and Masaaki Harada. Extremal self-dual codes over $\mathbf{F}_2 \times \mathbf{F}_2$. *Designs, Codes, and Cryptography*, 28(2):171–186, March 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/46/5/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/46/5/fulltext.pdf.

**Xu:2003:SDS**

[619] Sheng bo Xu, Jeroen Doumen, and Henk van Tilborg. On the security of digital signature schemes based on error-correcting codes. *Designs, Codes, and Cryptography*, 28(2):187–199, March 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/46/6/abstract.htm; http:/

/ipsapp007.kluweronline.com/content/getfile/4630/46/6/fulltext.pdf.

**Nikova:2003:IDB**

[620] Svetla Nikova and Ventzislav Nikov. Improvement of the Delsarte bound for $\theta$-designs when it is not the best bound possible. *Designs, Codes, and Cryptography*, 28(2):201–222, March 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/46/7/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/46/7/fulltext.pdf.

**Guillermo:2003:PAU**

[621] Mida Guillermo, Keith M. Martin, and Christine M. O'Keefe. Providing anonymity in unconditionally secure secret sharing schemes. *Designs, Codes, and Cryptography*, 28(3):227–245, April 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/47/1/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/47/1/fulltext.pdf.

**Shin:2003:DGC**

[622] Dong-Joon Shin, P. Vijay Kumar, and Tor Helleseth. 3-designs from the $Z_4$-Goethals codes via a new Kloosterman sum identity. *Designs, Codes, and Cryptography*, 28(3):247–263, April 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/47/2/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/47/2/fulltext.pdf.

**Helleseth:2003:HDD**

[623] Tor Helleseth, Torleiv Kløve, and Vladimir I. Levenshtein. Hypercubic 4 and 5-designs from double-error-correcting BCH codes. *Designs, Codes, and Cryptography*, 28(3):265–282, April 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/47/3/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/47/3/fulltext.pdf.

**Masson:2003:DRS**

[624] David Masson. Designs and representation of the symmetric group. *Designs, Codes, and Cryptography*, 28(3):283–302, April 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/47/4/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/47/4/fulltext.pdf.

**Huber:2003:TRM**

[625] Klaus Huber. Taking $p$th roots modulo polynomials over finite fields. *Designs, Codes, and Cryptography*, 28(3):303–311, April 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/47/5/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/47/5/fulltext.pdf.

**Blokhuis:2003:FG**

[626] A. Blokhuis, J. W. P. Hirschfeld, D. Jungnickel, and J. A. Thas. Finite geometries. *Designs, Codes, and Cryptography*, 29(1–3):5, May–June–July 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp007.kluweronline.com/content/getfile/4630/48/1/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/48/1/fulltext.pdf`.

**Aguglia:2003:CSH**

[627] A. Aguglia, A. Cossidente, and G. L. Ebert. Complete spans on Hermitian varieties. *Designs, Codes, and Cryptography*, 29(1–3):7–15, May–June–July 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp007.kluweronline.com/content/getfile/4630/48/2/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/48/2/fulltext.pdf`.

**Ahlswede:2003:FVH**

[628] R. Ahlswede, H. Aydinian, and L. H. Khachatrian. Forbidden $(0, 1)$-vectors in hyperplanes of $\mathbf{R}^n$: The restricted case. *Designs, Codes, and Cryptography*, 29(1–3):17–28, May–June–July 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp007.kluweronline.com/content/getfile/4630/48/3/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/48/3/fulltext.pdf`.

**Ahlswede:2003:CDB**

[629] Rudolf Ahlswede and Levon Khachatrian. Cone dependence — a basic combinatorial concept. *Designs, Codes, and Cryptography*, 29(1–3):29–40, May–June–July 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp007.kluweronline.com/content/getfile/4630/48/4/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/48/4/fulltext.pdf`.

**Bader:2003:SBS**

[630] Laura Bader, Nicola Durante, Maska Law, Guglielmo Lunardon, and Tim Penttila. Symmetries of BLT-sets. *Designs, Codes, and Cryptography*, 29(1–3):41–50, May–June–July 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp007.kluweronline.com/content/getfile/4630/48/5/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/48/5/fulltext.pdf`.

**Beth:2003:NCD**

[631] Thomas Beth, Christopher Charnes, Markus Grassl, Gernot Alber, Aldo Delgado, and Michael Mussinger. A new class of designs which protect against quantum jumps. *Designs, Codes, and Cryptography*, 29(1–3):51–70, May–June–July 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp007.kluweronline.com/content/getfile/4630/48/6/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/48/6/fulltext.pdf`.

**Bierbrauer:2003:PPC**

[632] Jürgen Bierbrauer, Stefano Marcug-

ini, and Fernanda Pambianco. Projective planes, coverings and a network problem. *Designs, Codes, and Cryptography*, 29(1–3):71–89, May–June–July 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp007.kluweronline.com/content/getfile/4630/48/7/abstract.htm`; `http://ipsapp007.kluweronline.com/content/getfile/4630/48/7/fulltext.pdf`.

**Blokhuis:2003:STG**

[633] Aart Blokhuis, Tamás Szőnyi, and Zsuzsa Weiner. On sets without tangents in Galois planes of even order. *Designs, Codes, and Cryptography*, 29(1–3):91–98, May–June–July 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp007.kluweronline.com/content/getfile/4630/48/8/abstract.htm`; `http://ipsapp007.kluweronline.com/content/getfile/4630/48/8/fulltext.pdf`.

**Edel:2003:LCA**

[634] Yves Edel and Jürgen Bierbrauer. The largest cap in AG$(4, 4)$ and its uniqueness. *Designs, Codes, and Cryptography*, 29(1–3):99–104, May–June–July 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp007.kluweronline.com/content/getfile/4630/48/9/abstract.htm`; `http://ipsapp007.kluweronline.com/content/getfile/4630/48/9/fulltext.pdf`.

**Ferret:2003:RMP**

[635] S. Ferret and L. Storme. Results on maximal partial spreads in PG$(3, p^3)$ and on related minihypers. *Designs, Codes, and Cryptography*, 29(1–3):105–122, May–June–July 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp007.kluweronline.com/content/getfile/4630/48/10/abstract.htm`; `http://ipsapp007.kluweronline.com/content/getfile/4630/48/10/fulltext.pdf`.

**Gacs:2003:MPS**

[636] András Gács and Tamás Szőnyi. On maximal partial spreads in PG$(n, q)$. *Designs, Codes, and Cryptography*, 29(1–3):123–129, May–June–July 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp007.kluweronline.com/content/getfile/4630/48/11/abstract.htm`; `http://ipsapp007.kluweronline.com/content/getfile/4630/48/11/fulltext.pdf`.

**Gacs:2003:AT**

[637] András Gács and Zsuzsa Weiner. On $(q + t, t)$-arcs of type $(0, 2, t)$. *Designs, Codes, and Cryptography*, 29(1–3):131–139, May–June–July 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp007.kluweronline.com/content/getfile/4630/48/12/abstract.htm`; `http://ipsapp007.kluweronline.com/content/getfile/4630/48/12/fulltext.pdf`.

**Govaerts:2003:SNM**

[638] P. Govaerts, D. Jungnickel, L. Storme, and J. A. Thas. Some new maximal sets of mutually orthogonal Latin squares. *Designs, Codes, and Cryptography*, 29(1–3):141–147, May–June–July 2003. CODEN DCCREC. ISSN

0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/48/13/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/48/13/fulltext.pdf.

**Kyureghyan:2003:LCS**

[639] Gohar M. Kyureghyan and Alexander Pott. On the linear complexity of the Sidelnikov–Lempel–Cohn–Eastman sequences. *Designs, Codes, and Cryptography*, 29(1–3):149–164, May–June–July 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/48/14/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/48/14/fulltext.pdf. See correction [2442].

**Landjev:2003:OCF**

[640] I. Landjev, A. Rousseva, T. Maruta, and R. Hill. On optimal codes over the field with five elements. *Designs, Codes, and Cryptography*, 29(1–3):165–175, May–June–July 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/48/15/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/48/15/fulltext.pdf.

**Leemans:2003:RWP**

[641] Dimitri Leemans. The residually weakly primitive geometries of $M_{22}$. *Designs, Codes, and Cryptography*, 29(1–3):177–178, May–June–July 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/48/16/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/48/16/fulltext.pdf.

**Luyckx:2003:SQE**

[642] D. Luyckx and J. A. Thas. On 1-systems of $Q(6, q)$, $q$ even. *Designs, Codes, and Cryptography*, 29(1–3):179–197, May–June–July 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/48/17/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/48/17/fulltext.pdf.

**vanMaldeghem:2003:SRS**

[643] Hendrik van Maldeghem. Some remarks on Steiner systems. *Designs, Codes, and Cryptography*, 29(1–3):199–213, May–June–July 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/48/18/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/48/18/fulltext.pdf.

**Metsch:2003:CFH**

[644] Klaus Metsch. On the characterization of the folded halved cubes by their intersection arrays. *Designs, Codes, and Cryptography*, 29(1–3):215–225, May–June–July 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/48/19/abstract.htm; http:

//ipsapp007.kluweronline.com/content/getfile/4630/48/19/fulltext.pdf.

**Thas:2003:SGQ**

[645] Koen Thas. Symmetry in generalized quadrangles. *Designs, Codes, and Cryptography*, 29(1–3):227–245, May–June–July 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/48/20/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/48/20/fulltext.pdf.

**Tonchev:2003:NMC**

[646] Vladimir D. Tonchev. A note on MDS codes, $n$-arcs and complete designs. *Designs, Codes, and Cryptography*, 29(1–3):247–250, May–June–July 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/48/21/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/48/21/fulltext.pdf.

**Ng:2003:RFS**

[647] Siaw-Lynn Ng. A representation of a family of secret sharing matroids. *Designs, Codes, and Cryptography*, 30(1):5–19, August 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/49/1/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/49/1/fulltext.pdf.

**Axenovich:2003:EBS**

[648] Maria Axenovich and Zoltán Füredi. Exact bounds on the sizes of covering codes. *Designs, Codes, and Cryptography*, 30(1):21–38, August 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/49/2/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/49/2/fulltext.pdf.

**Liu:2003:PPA**

[649] Shengli Liu, Henk C. A. Van Tilborg, and Marten Van Dijk. A practical protocol for advantage distillation and information reconciliation. *Designs, Codes, and Cryptography*, 30(1):39–62, August 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/49/3/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/49/3/fulltext.pdf.

**Mellinger:2003:GRB**

[650] Keith E. Mellinger. A geometric relationship between equivalent spreads. *Designs, Codes, and Cryptography*, 30(1):63–71, August 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/49/4/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/49/4/fulltext.pdf.

**Ding:2003:MWK**

[651] Cunsheng Ding, Mordecai Golin, and Torleiv Kløve. Meeting the Welch

and Karystinos-Pados bounds on DS-CDMA binary signature sets. *Designs, Codes, and Cryptography*, 30(1):73–84, August 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/49/5/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/49/5/fulltext.pdf.

**Bluher:2003:CT**

[652] Antonia W. Bluher. On $x^6 + x + a$ in characteristic three. *Designs, Codes, and Cryptography*, 30(1):85–95, August 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/49/6/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/49/6/fulltext.pdf.

**Bouyukliev:2003:SNR**

[653] Iliya Bouyukliev and Juriaan Simonis. Some new results on optimal codes over $F^5$. *Designs, Codes, and Cryptography*, 30(1):97–111, August 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/49/7/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/49/7/fulltext.pdf.

**Ling:2003:ASQ**

[654] San Ling and Patrick Solé. On the algebraic structure of quasi-cyclic codes II: Chain rings. *Designs, Codes, and Cryptography*, 30(1):113–130, August 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/49/8/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/49/8/fulltext.pdf.

**Kharaghani:2003:CSB**

[655] H. Kharaghani. On a class of symmetric balanced generalized weighing matrices. *Designs, Codes, and Cryptography*, 30(2):139–149, September 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/50/1/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/50/1/fulltext.pdf.

**Dalan:2003:NET**

[656] Daniel B. Dalan. New extremal type I codes of lengths 40, 42, and 44. *Designs, Codes, and Cryptography*, 30(2):151–157, September 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/50/2/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/50/2/fulltext.pdf.

**Sala:2003:UBD**

[657] Massimiliano Sala. Upper bounds on the dual distance of BCH$(255, k)$. *Designs, Codes, and Cryptography*, 30(2):159–168, September 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/50/3/abstract.htm; http://ipsapp007.kluweronline.

com/content/getfile/4630/50/3/fulltext.pdf.

**Tanabe:2003:CDC**

[658] Kenichiro Tanabe. A criterion for designs in $Z_4$-codes on the symmetrized weight enumerator. *Designs, Codes, and Cryptography*, 30(2):169–185, September 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/50/4/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/50/4/fulltext.pdf.

**Kim:2003:DAC**

[659] Jon-Lark Kim and Vera Pless. Designs in additive codes over GF(4). *Designs, Codes, and Cryptography*, 30(2):187–199, September 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/50/5/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/50/5/fulltext.pdf.

**Nguyen:2003:IEC**

[660] Phong Q. Nguyen and Igor E. Shparlinski. The insecurity of the elliptic curve digital signature algorithm with partially known nonces. *Designs, Codes, and Cryptography*, 30(2):201–217, September 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/50/6/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/50/6/fulltext.pdf.

**Cardinali:2003:SSF**

[661] I. Cardinali, O. Polverino, and R. Trombetti. On the sporadic semifield flock. *Designs, Codes, and Cryptography*, 30(2):219–226, September 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/50/7/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/50/7/fulltext.pdf.

**Sarkar:2003:CSB**

[662] Palash Sarkar and Paul J. Schellenberg. Construction of symmetric balanced squares with blocksize more than one. *Designs, Codes, and Cryptography*, 30(3):235–280, November 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/51/1/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/51/1/fulltext.pdf.

**Huhnlein:2003:TPN**

[663] Detlef Hühnlein, Michael J. Jacobson, Jr., and Damian Weber. Towards practical non-interactive public-key cryptosystems using non-maximal imaginary quadratic orders. *Designs, Codes, and Cryptography*, 30(3):281–299, November 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/51/2/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/51/2/fulltext.pdf.

**Nocon:2003:CST**

[664] Ederlina G. Nocon. On the construction of some type II codes over $Z_4 \times Z_4$. *Designs, Codes, and Cryptography*, 30(3):301–323, November 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/51/3/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/51/3/fulltext.pdf.

**Chandler:2003:CRD**

[665] David B. Chandler and Qing Xiang. Cyclic relative difference sets and their $p$-ranks. *Designs, Codes, and Cryptography*, 30(3):325–343, November 2003. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/51/4/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/51/4/fulltext.pdf.

**Edel:2004:EGP**

[666] Yves Edel. Extensions of generalized product caps. *Designs, Codes, and Cryptography*, 31(1):5–14, January 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/59/1/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/59/1/fulltext.pdf.

**Barat:2004:MBSa**

[667] J. Barát, A. Del Fra, S. Innamorati, and L. Storme. Minimal blocking sets in PG(2, 8) and maximal partial spreads in PG(3, 8). *Designs, Codes, and Cryptography*, 31(1):15–26, January 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/59/2/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/59/2/fulltext.pdf.

**Schaathun:2004:LBG**

[668] Hans Georg Schaathun. A lower bound on the greedy weights of product codes. *Designs, Codes, and Cryptography*, 31(1):27–42, January 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/59/3/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/59/3/fulltext.pdf.

**Glynn:2004:OGC**

[669] David G. Glynn. On the orthogonality of geometric codes. *Designs, Codes, and Cryptography*, 31(1):43–50, January 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/59/4/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/59/4/fulltext.pdf.

**Golic:2004:CAA**

[670] Jovan Dj. Golić and Renato Menicocci. Correlation analysis of the alternating step generator. *Designs, Codes, and Cryptography*, 31(1):51–74, January 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.

kluweronline.com/content/getfile/4630/59/5/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/59/5/fulltext.pdf.

**Shin:2004:AMT**

[671] Dong-Joon Shin, P. Vijay Kumar, and Tor Helleseth. An Assmus–Mattson-type approach for identifying 3-designs from linear codes over $Z_4$. *Designs, Codes, and Cryptography*, 31(1):75–92, January 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp007.kluweronline.com/content/getfile/4630/59/6/abstract.htm; http://ipsapp007.kluweronline.com/content/getfile/4630/59/6/fulltext.pdf.

**Biehl:2004:EUS**

[672] Ingrid Biehl, Sacher Paulus, and Tsuyoshi Takagi. Efficient undeniable signature schemes based on ideal arithmetic in quadratic orders. *Designs, Codes, and Cryptography*, 31 (2):99–123, February 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/60/A/1/abstract.htm.

**Trung:2004:CTC**

[673] Tran Van Trung and Sosina Martirosyan. On a class of traceability codes. *Designs, Codes, and Cryptography*, 31(2):125–132, February 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/60/A/2/abstract.htm.

**Rajola:2004:APF**

[674] S. Rajola and M. Scafati Tallini. Affine planes and flag linear spaces. *Designs, Codes, and Cryptography*, 31 (2):133–137, February 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/60/A/3/abstract.htm.

**Gulliver:2004:MWC**

[675] T. Aaron Gulliver and Masaaki Harada. On the minimum weight of codes over $F_5$ constructed from certain conference matrices. *Designs, Codes, and Cryptography*, 31 (2):139–145, February 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/60/A/4/abstract.htm.

**Stanica:2004:BFF**

[676] Pantelimon Stănică and Soo Hak Sung. Boolean functions with five controllable cryptographic properties. *Designs, Codes, and Cryptography*, 31 (2):147–157, February 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/60/A/5/abstract.htm.

**Dempwolff:2004:ARG**

[677] U. Dempwolff. Affine rank 3 groups on symmetric designs. *Designs, Codes, and Cryptography*, 31(2):159–168, February 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http:/

/ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/60/A/6/abstract.htm.

**OSullivan:2004:KAC**

[678] Michael E. O'Sullivan. On Koetter's algorithm and the computation of error values. *Designs, Codes, and Cryptography*, 31(2):169–188, February 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/60/A/7/abstract.htm.

**Drake:2004:OHD**

[679] David A. Drake and Kevin Keating. Ovals and hyperovals in Desarguesian nets. *Designs, Codes, and Cryptography*, 31(3):195–212, March 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/61/A/1/abstract.htm.

**Sin:2004:RIM**

[680] Peter Sin. The $p$-rank of the incidence matrix of intersecting linear subspaces. *Designs, Codes, and Cryptography*, 31(3):213–220, March 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/61/A/2/abstract.htm.

**Klein:2004:POC**

[681] Andreas Klein. Partial ovoids in classical finite polar spaces. *Designs, Codes, and Cryptography*, 31(3):221–226, March 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/61/A/3/abstract.htm.

**Klapper:2004:RSA**

[682] Andrew Klapper and Jinzhong Xu. Register synthesis for algebraic feedback shift registers based on non-primes. *Designs, Codes, and Cryptography*, 31(3):227–250, March 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/61/A/4/abstract.htm.

**Brown:2004:SFO**

[683] Matthew R. Brown, Christine M. O'Keefe, S. E. Payne, Tim Penttila, and Gordon F. Royle. Spreads of $T_2(o)$, $\alpha$-flocks and ovals. *Designs, Codes, and Cryptography*, 31(3):251–282, March 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/61/A/5/abstract.htm.

**Metsch:2004:SPS**

[684] Klaus Metsch. Small point sets that meet all generators of $W(2n+1,q)$. *Designs, Codes, and Cryptography*, 31(3):283–288, March 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/61/A/6/abstract.htm.

**Rinaldi:2004:KDP**

[685] Gloria Rinaldi. Key distribution patterns using tangent circle structures.

*Designs, Codes, and Cryptography*, 31 (3):289–300, March 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/61/A/7/abstract.htm`.

**Muller:2004:CSR**

[686] Siguna Müller. On the computation of square roots in finite fields. *Designs, Codes, and Cryptography*, 31 (3):301–312, March 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/61/A/8/abstract.htm`.

**Avgustinovich:2004:CSP**

[687] Sergey V. Avgustinovich, Olof Heden, and Faina I. Solov'eva. The classification of some perfect codes. *Designs, Codes, and Cryptography*, 31 (3):313–318, March 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/61/A/9/abstract.htm`.

**Anonymous:2004:P**

[688] Anonymous. Preface. *Designs, Codes, and Cryptography*, 32(1–3):5–6, May–July 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/62/A/1/abstract.htm`. Special Issue: Proceedings of the Third Pythagorean Conference.

**Anonymous:2004:LP**

[689] Anonymous. List of participants. *Designs, Codes, and Cryptography*, 32 (1–3):7–8, May–July 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/62/A/2/abstract.htm`. Special Issue: Proceedings of the Third Pythagorean Conference.

**Ball:2004:SS**

[690] Simeon Ball, John Bamberg, Michel Lavrauw, and Tim Penttila. Symplectic spreads. *Designs, Codes, and Cryptography*, 32(1–3):9–14, May–July 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/62/A/3/abstract.htm`. Special Issue: Proceedings of the Third Pythagorean Conference.

**Blundo:2004:DSH**

[691] Carlo Blundo, Paolo D'Arco, Alfredo De Santis, and Massimiliano Listo. Design of self-healing key distribution schemes. *Designs, Codes, and Cryptography*, 32(1–3): 15–44, May–July 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/62/A/4/abstract.htm`. Special Issue: Proceedings of the Third Pythagorean Conference.

**Brown:2004:AG**

[692] Julia M. N. Brown. On the action of the groups $\mathrm{GL}(n+1,q)$, $\mathrm{PGL}(n+1,q)$, $\mathrm{SL}(n+1,q)$ and

PSL$(n+1,q)$ on PG$(n,q^t)$. *Designs, Codes, and Cryptography*, 32(1–3):45–50, May–July 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/62/A/5/abstract.htm`. Special Issue: Proceedings of the Third Pythagorean Conference.

**Chu:2004:CPC**

[693] Wensong Chu, Charles J. Colbourn, and Peter Dukes. Constructions for permutation codes in powerline communications. *Designs, Codes, and Cryptography*, 32(1–3): 51–64, May–July 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/62/A/6/abstract.htm`. Special Issue: Proceedings of the Third Pythagorean Conference.

**Colbourn:2004:CFF**

[694] Charles J. Colbourn, Alan C. H. Ling, and Violet R. Syrotiuk. Cover-free families and topology-transparent scheduling for MANETs. *Designs, Codes, and Cryptography*, 32(1–3): 65–95, May–July 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/62/A/7/abstract.htm`. Special Issue: Proceedings of the Third Pythagorean Conference.

**Cossidente:2004:RSC**

[695] A. Cossidente and M. J. de Resmini. Remarks on Singer cyclic groups and their normalizers. *Designs, Codes, and Cryptography*, 32(1–3): 97–102, May–July 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/62/A/8/abstract.htm`. Special Issue: Proceedings of the Third Pythagorean Conference.

**DeClerck:2004:GDS**

[696] F. De Clerck and M. Delanote. On $(0,\alpha)$-geometries and dual semipartial geometries fully embedded in an affine space. *Designs, Codes, and Cryptography*, 32(1–3):103–110, May–July 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/62/A/9/abstract.htm`. Special Issue: Proceedings of the Third Pythagorean Conference.

**deFeyter:2004:POS**

[697] Nikias de Feyter. Planar oval sets in Desarguesian planes of even order. *Designs, Codes, and Cryptography*, 32(1–3):111–119, May–July 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/62/A/10/abstract.htm`. Special Issue: Proceedings of the Third Pythagorean Conference.

**Deng:2004:LLL**

[698] D. Deng, D. R. Stinson, and R. Wei. The Lovász local lemma and its applications to some combinatorial arrays. *Designs, Codes, and Cryptography*, 32(1–3):121–134, May–July 2004. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/62/A/11/abstract.htm`. Special Issue: Proceedings of the Third Pythagorean Conference.

**DeSantis:2004:AMB**

[699] A. De Santis and B. Masucci. Anonymous membership broadcast schemes. *Designs, Codes, and Cryptography*, 32(1–3):135–151, May–July 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/62/A/12/abstract.htm`. Special Issue: Proceedings of the Third Pythagorean Conference.

**DeWinter:2004:SRS**

[700] S. De Winter and J. A. Thas. SPG-reguli satisfying the polar property and a new semipartial geometry. *Designs, Codes, and Cryptography*, 32(1–3):153–166, May–July 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/62/A/13/abstract.htm`. Special Issue: Proceedings of the Third Pythagorean Conference.

**Drake:2004:NSD**

[701] David A. Drake and Wendy Myrvold. Nets of small degree without ovals. *Designs, Codes, and Cryptography*, 32(1–3):167–183, May–July 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/62/A/14/abstract.htm`. Special Issue: Proceedings of the Third Pythagorean Conference.

**Eslami:2004:EDT**

[702] Z. Eslami, G. B. Khosrovshahi, and M. M. Noori. Enumeration of $t$-designs through intersection matrices. *Designs, Codes, and Cryptography*, 32(1–3):185–191, May–July 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/62/A/15/abstract.htm`. Special Issue: Proceedings of the Third Pythagorean Conference.

**Georgiou:2004:SOS**

[703] S. Georgiou and C. Koukouvinos. Self-orthogonal and self-dual codes constructed via combinatorial designs and Diophantine equations. *Designs, Codes, and Cryptography*, 32(1–3): 193–206, May–July 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/62/A/16/abstract.htm`. Special Issue: Proceedings of the Third Pythagorean Conference.

**Vasco:2004:STP**

[704] M. I. González Vasco, D. Hofheinz, C. Martínez, and R. Steinwandt. On the security of two public key cryptosystems using non-Abelian groups. *Designs, Codes, and Cryptography*, 32(1–3):207–216, May–July 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/62/A/17/abstract.htm`.

Special Issue: Proceedings of the Third Pythagorean Conference.

**Grosek:2004:NPL**

[705] Otokar Grošek, Peter Horák, and Tran van Trung. On non-polynomial Latin squares. *Designs, Codes, and Cryptography*, 32(1–3):217–226, May–July 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/62/A/18/abstract.htm`. Special Issue: Proceedings of the Third Pythagorean Conference.

**Ionin:2004:RHM**

[706] Yury J. Ionin. Regular Hadamard matrices generating infinite families of symmetric designs. *Designs, Codes, and Cryptography*, 32(1–3): 227–233, May–July 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/62/A/19/abstract.htm`. Special Issue: Proceedings of the Third Pythagorean Conference.

**Khosrovshahi:2004:SID**

[707] G. B. Khosrovshahi and B. Tayfeh-Rezaie. Some indecomposable $t$-designs. *Designs, Codes, and Cryptography*, 32(1–3):235–238, May–July 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/62/A/20/abstract.htm`. Special Issue: Proceedings of the Third Pythagorean Conference.

**Korchmaros:2004:HOF**

[708] G. Korchmáros and A. Sonnino. Hyperbolic ovals in finite planes. *Designs, Codes, and Cryptography*, 32(1–3):239–249, May–July 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/62/A/21/abstract.htm`. Special Issue: Proceedings of the Third Pythagorean Conference.

**Kuccukccifcci:2004:MCH**

[709] Selda Kücçükccıfccı and C. C. Lindner. Minimum covering for hexagon triple systems. *Designs, Codes, and Cryptography*, 32(1–3):251–265, May–July 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/62/A/22/abstract.htm`. Special Issue: Proceedings of the Third Pythagorean Conference.

**Labbate:2004:ACB**

[710] Domenico Labbate. Amalgams of cubic bipartite graphs. *Designs, Codes, and Cryptography*, 32(1–3): 267–275, May–July 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/62/A/23/abstract.htm`. Special Issue: Proceedings of the Third Pythagorean Conference.

**Laue:2004:RD**

[711] Reinhard Laue. Resolvable $t$-designs. *Designs, Codes, and Cryp-*

*tography*, 32(1–3):277–301, May–July 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/62/A/24/abstract.htm`. Special Issue: Proceedings of the Third Pythagorean Conference.

**Ma:2004:BCF**

[712] X. Ma and R. Wei. On a bound of cover-free families. *Designs, Codes, and Cryptography*, 32(1–3): 303–321, May–July 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/62/A/25/abstract.htm`. Special Issue: Proceedings of the Third Pythagorean Conference.

**Martirosyan:2004:CA**

[713] Sosina Martirosyan and Tran van Trung. On $t$-covering arrays. *Designs, Codes, and Cryptography*, 32(1–3):323–339, May–July 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/62/A/26/abstract.htm`. Special Issue: Proceedings of the Third Pythagorean Conference.

**Mellinger:2004:LCT**

[714] Keith E. Mellinger. LDPC codes from triangle-free line sets. *Designs, Codes, and Cryptography*, 32(1–3): 341–350, May–July 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/62/A/27/abstract.htm`. Special Issue: Proceedings of the Third Pythagorean Conference.

**Offer:2004:SOT**

[715] Alan Offer and Hendrik Van Maldeghem. Spreads and ovoids translation with respect to disjoint flags. *Designs, Codes, and Cryptography*, 32(1–3): 351–367, May–July 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/62/A/28/abstract.htm`. Special Issue: Proceedings of the Third Pythagorean Conference.

**Seidel:2004:PSA**

[716] Tanya E. Seidel, Daniel Socek, and Michal Sramka. Parallel symmetric attack on NTRU using nondeterministic lattice reduction. *Designs, Codes, and Cryptography*, 32(1–3):369–379, May–July 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/62/A/29/abstract.htm`. Special Issue: Proceedings of the Third Pythagorean Conference.

**Shaw:2004:QG**

[717] R. Shaw and N. A. Gordon. The quintic Grassmannian $G_{1,4,2}$ in PG$(9, 2)$. *Designs, Codes, and Cryptography*, 32(1–3):381–396, May–July 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/62/A/30/abstract.htm`. Special Issue: Proceed-

ings of the Third Pythagorean Conference.

**Barat:2004:MBSb**

[718] János Barát and Leo Storme. Multiple blocking sets in $\mathrm{PG}(n, q), n > 3$. *Designs, Codes, and Cryptography*, 33(1):5–21, August 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/63/A/1/abstract.htm`.

**No:2004:RCP**

[719] Jong-Seon No, Dong-Joon Shin, and Tor Helleseth. On the $p$-ranks and characteristic polynomials of cyclic difference sets. *Designs, Codes, and Cryptography*, 33 (1):23–37, August 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/63/A/2/abstract.htm`.

**Helleseth:2004:PSC**

[720] Tor Helleseth and Johannes Mykkeltveit. A proof of Simmons' Conjecture. *Designs, Codes, and Cryptography*, 33 (1):39–43, August 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/63/A/3/abstract.htm`.

**Dougherty:2004:MDC**

[721] Steven T. Dougherty and Keisuke Shiromoto. Maximum distance codes in $\mathrm{Mat}_{n,s}(Z_k)$ with a non-Hamming metric and uniform distributions. *Designs, Codes, and Cryptography*, 33 (1):45–61, August 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/63/A/4/abstract.htm`.

**Drake:2004:NEM**

[722] David A. Drake and Wendy Myrvold. The non-existence of maximal sets of four mutually orthogonal Latin squares of order 8. *Designs, Codes, and Cryptography*, 33 (1):63–69, August 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/63/A/5/abstract.htm`.

**Ward:2004:SUQ**

[723] Harold N. Ward. A sequence of unique quaternary Griesmer codes. *Designs, Codes, and Cryptography*, 33 (1):71–85, August 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/63/A/6/abstract.htm`.

**Martinez-Perez:2004:WHP**

[724] Conchita Martínez-Pérez and Wolfgang Willems. On the weight hierarchy of product codes. *Designs, Codes, and Cryptography*, 33(2):95–108, September 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/64/A/1/abstract.htm`.

**Meidl:2004:HMB**

[725] Wilfried Meidl. How many bits have to be changed to decrease the linear complexity? *Designs, Codes, and Cryptography*, 33(2):109–122, September 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/64/A/2/abstract.htm`.

**Goresky:2004:PCP**

[726] Mark Goresky and Andrew Klapper. Periodicity and correlation properties of $d$-FCSR sequences. *Designs, Codes, and Cryptography*, 33(2):123–148, September 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/64/A/3/abstract.htm`.

**Harada:2004:CRT**

[727] Masaaki Harada, Michio Ozeki, and Kenichiro Tanabe. On the covering radius of ternary extremal self-dual codes. *Designs, Codes, and Cryptography*, 33(2):149–158, September 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/64/A/4/abstract.htm`.

**Hayden:2004:EFP**

[728] J. L. Hayden. Eigenvalues of finite projective planes with an Abelian Cartesian group. *Designs, Codes, and Cryptography*, 33(2):159–172, September 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/64/A/5/abstract.htm`.

**Guerra:2004:LCA**

[729] Lucio Guerra and Rita Vincenti. On the linear codes arising from Schubert varieties. *Designs, Codes, and Cryptography*, 33(2):173–180, September 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/64/A/6/abstract.htm`.

**Diestelkamp:2004:PIO**

[730] Wiebke S. Diestelkamp. Parameter inequalities for orthogonal arrays with mixed levels. *Designs, Codes, and Cryptography*, 33(3):187–197, November 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/65/A/1/abstract.htm`.

**No:2004:NCD**

[731] Jong-Seon No. New cyclic difference sets with Singer parameters constructed from $d$-homogeneous functions. *Designs, Codes, and Cryptography*, 33(3):199–213, November 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/65/A/2/abstract.htm`.

**Vasco:2004:TUD**

[732] María Isabel González Vasco, Consuelo Martínez, and Rainer Steinwandt. Towards a uniform description of several group based cryptographic primitives. *Designs, Codes, and Cryptography*, 33 (3):215–226, November 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/65/A/3/abstract.htm`.

**Ding:2004:TCA**

[733] Cunsheng Ding and Xiaojian Tian. Three constructions of authentication codes with perfect secrecy. *Designs, Codes, and Cryptography*, 33(3): 227–239, November 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/65/A/4/abstract.htm`.

**Blundo:2004:LAA**

[734] Carlo Blundo, Sebastià Martín, Barbara Masucci, and CarlEs Padró. A linear algebraic approach to metering schemes. *Designs, Codes, and Cryptography*, 33(3):241–260, November 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/65/A/5/abstract.htm`.

**Menezes:2004:SSS**

[735] Alfred Menezes and Nigel Smart. Security of signature schemes in a multi-user setting. *Designs, Codes, and Cryptography*, 33(3):261–274, November 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/65/A/6/abstract.htm`.

**Yucas:2004:SRI**

[736] Joseph L. Yucas and Gary L. Mullen. Self-reciprocal irreducible polynomials over finite fields. *Designs, Codes, and Cryptography*, 33(3):275–281, November 2004. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://ipsapp008.kluweronline.com/IPS/content/ext/x/J/4630/I/65/A/7/abstract.htm`.

**Maruta:2005:MSS**

[737] Tatsuya Maruta, Ivan N. Landjev, and Assya Rousseva. On the minimum size of some minihypers and related linear codes. *Designs, Codes, and Cryptography*, 34(1):5–15, January 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Marti-Farre:2005:SSS**

[738] Jaume Martí-Farré and Carles Padró. Secret sharing schemes with three or four minimal qualified subsets. *Designs, Codes, and Cryptography*, 34(1): 17–34, January 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Ozbudak:2005:EPO**

[739] Ferruh Özbudak. Elements of prescribed order, prescribed traces and systems of rational functions over finite fields. *Designs, Codes, and Cryptography*, 34(1):35–54, January 2005.

CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Braun:2005:SCA**

[740] Michael Braun, Adalbert Kerber, and Reinhard Laue. Systematic construction of $q$-analogs of $t-(v,k,\lambda)$-designs. *Designs, Codes, and Cryptography*, 34 (1):55–70, January 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Harada:2005:SNG**

[741] Masaaki Harada, Clement Lam, and Vladimir D. Tonchev. Symmetric $(4,4)$-nets and generalized Hadamard matrices over groups of order 4. *Designs, Codes, and Cryptography*, 34(1): 71–87, January 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Dey:2005:LCC**

[742] Bikash Kumar Dey and B. Sundar Rajan. $F_q$-linear cyclic codes over $F_q^m$: DFT approach. *Designs, Codes, and Cryptography*, 34(1):89–116, January 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Ge:2005:GDD**

[743] Gennian Ge and Alan C. H. Ling. Group divisible designs with block size four and group type $g^u m^1$ with minimum $m$. *Designs, Codes, and Cryptography*, 34(1):117–126, January 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Blokhuis:2005:P**

[744] Aart Blokhuis and Willem Haemers. Preface. *Designs, Codes, and Cryptography*, 34(2–3):135, February 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**VanDam:2005:CDC**

[745] Edwin R. Van Dam. The combinatorics of Dom de Caen. *Designs, Codes, and Cryptography*, 34(2–3):137–148, February 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**DeCaen:2005:DRC**

[746] D. De Caen and D. Fon-Der-Flaass. Distance regular covers of complete graphs from latin squares. *Designs, Codes, and Cryptography*, 34(2–3):149–153, February 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Coolsaet:2005:CAP**

[747] K. Coolsaet and J. Degraer. A computer-assisted proof of the uniqueness of the Perkel graph. *Designs, Codes, and Cryptography*, 34(2–3):155–171, February 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Sejeong:2005:SIR**

[748] Bang Sejeong and J. H. Koolen. Some interlacing results for the eigenvalues of distance-regular graphs. *Designs, Codes, and Cryptography*, 34(2–3):173–186, February 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Hirasaka:2005:MTA**

[749] Hirasaka. On meta-thin association schemes. *Designs, Codes, and Cryptography*, 34(2–3):187–201, February 2005.

CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Shaw:2005:CFW**

[750] Ron Shaw, Johannes G. Maks, and Neil A. Gordon. The classification of flats in which are external to the Grassmannian. *Designs, Codes, and Cryptography*, 34(2–3):203–227, February 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Cvetkovic:2005:GLE**

[751] Dragos Cvetković, Peter Rowlinson, and Slobodan K. Simić. Graphs with least eigenvalue $-2$: a new proof of the 31 forbidden subgraphs theorem. *Designs, Codes, and Cryptography*, 34(2–3):229–240, February 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Curtin:2005:ACG**

[752] Brian Curtin. Algebraic characterizations of graph regularity conditions. *Designs, Codes, and Cryptography*, 34 (2–3):241–248, February 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Muzychuk:2005:SPB**

[753] Mikhail Muzychuk and István Kovács. A solution of a problem of A. E. Brouwer. *Designs, Codes, and Cryptography*, 34(2–3):249–264, February 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Seress:2005:SFN**

[754] Ákos Seress. Square-free non-Cayley numbers. on vertex-transitive non-Cayley graphs of square-free order. *Designs, Codes, and Cryptography*, 34(2–3):265–281, February 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Thas:2005:SCF**

[755] Joseph A. Thas and Hendrik Van Maldeghem. Some characterizations of finite Hermitian Veroneseans. *Designs, Codes, and Cryptography*, 34(2–3):283–293, February 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Baker:2005:HFC**

[756] R. D. Baker, G. L. Ebert, and Tim Penttila. Hyperbolic fibrations and $q$-clans. *Designs, Codes, and Cryptography*, 34(2–3):295–305, February 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Terwilliger:2005:TLT**

[757] Paul Terwilliger. Two linear transformations each tridiagonal with respect to an eigenbasis of the other; comments on the parameter array. *Designs, Codes, and Cryptography*, 34(2–3):307–332, February 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Cuypers:2005:NTS**

[758] Hans Cuypers. A note on the tight spherical 7-design in and 5-design in. *Designs, Codes, and Cryptography*, 34 (2–3):333–337, February 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Metsch:2005:BSH**

[759] Klaus Metsch. Blocking structures of Hermitian varieties. *Designs,*

*Codes, and Cryptography*, 34(2–3):339–360, February 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Golic:2005:VAF**

[760] Jovan Dj. Golić and Philip Hawkes. Vectorial approach to fast correlation attacks. *Designs, Codes, and Cryptography*, 35(1):5–19, April 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Mcsorley:2005:DATa**

[761] John P. Mcsorley, N. C. K. Phillips, W. D. Wallis, et al. Double arrays, triple arrays and balanced grids. *Designs, Codes, and Cryptography*, 35 (1):21–45, April 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Tzeng:2005:PKT**

[762] Wen-Guey Tzeng and Zhi-Jia Tzeng. A public-key traitor tracing scheme with revocation using dynamic shares. *Designs, Codes, and Cryptography*, 35 (1):47–61, April 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Berger:2005:HMS**

[763] Thierry P. Berger and Pierre Loidreau. How to mask the structure of codes for a cryptographic use. *Designs, Codes, and Cryptography*, 35(1):63–79, April 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Milenkovic:2005:SWE**

[764] Olgica Milenkovic. Support weight enumerators and coset weight distributions of isodual codes. *Designs, Codes, and Cryptography*, 35(1):81–109, April 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Hess:2005:LCM**

[765] Florian Hess and Igor E. Shparlinski. On the linear complexity and multidimensional distribution of congruential generators over elliptic curves. *Designs, Codes, and Cryptography*, 35(1): 111–117, April 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Brown:2005:GGC**

[766] Daniel R. L. Brown. Generic groups, collision resistance, and ECDSA. *Designs, Codes, and Cryptography*, 35(1): 119–152, April 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Bialota:2005:MAG**

[767] Rafał Białota and Grzegorz Kawa. Modified alternating $\vec{k}$ generators. *Designs, Codes, and Cryptography*, 35(2): 159–174, May 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Maruta:2005:ETL**

[768] Tatsuya Maruta. Extendability of ternary linear codes. *Designs, Codes, and Cryptography*, 35(2):175–190, May 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Xia:2005:NMC**

[769] Mingyuan Xia, Tianbing Xia, and Jennifer Seberry. A new method for constructing Williamson matrices. *Designs, Codes, and Cryptography*, 35(2):

191–209, May 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Carvalho:2005:GCW**

[770] Cícero Carvalho and Fernando Torres. On Goppa codes and Weierstrass gaps at several points. *Designs, Codes, and Cryptography*, 35(2):211–225, May 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Trung:2005:NCI**

[771] Tran Van Trung and Sosina Martirosyan. New constructions for IPP codes. *Designs, Codes, and Cryptography*, 35(2):227–239, May 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Ostergaard:2005:NRC**

[772] Patric R. J. Östergård, Jörn Quistorff, and Alfred Wassermann. New results on codes with covering radius 1 and minimum distance 2. *Designs, Codes, and Cryptography*, 35(2):241–250, May 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Lisonek:2005:FCC**

[773] Petr Lisonek and Mahadad Khatirinejad. A family of complete caps in PG$(n, 2)$. *Designs, Codes, and Cryptography*, 35(3):259–270, June 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Haanpaa:2005:NRD**

[774] Harri Haanpää and Petteri Kaski. The near resolvable $2 - (13, 4, 3)$ designs and thirteen-player whist tournaments. *Designs, Codes, and Cryptography*, 35 (3):271–285, June 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Gennian:2005:RMP**

[775] G. E. Gennian, C. W. H. Lam, Alan C. H. Ling, et al. Resolvable maximum packings with quadruples. *Designs, Codes, and Cryptography*, 35(3): 287–302, June 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Ionin:2005:RCN**

[776] Yury J. Ionin and Hadi Kharaghani. A recursive construction for new symmetric designs. *Designs, Codes, and Cryptography*, 35(3):303–310, June 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Cimato:2005:OCT**

[777] Stelvio Cimato, Roberto De Prisco, and Alfredo De Santis. Optimal colored threshold visual cryptography schemes. *Designs, Codes, and Cryptography*, 35 (3):311–335, June 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Luyckx:2005:TSQ**

[778] D. Luyckx and J. A. Thas. Trialities and 1-systems of $Q^+(7, q)$. *Designs, Codes, and Cryptography*, 35(3): 337–352, June 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Barwick:2005:GAR**

[779] S. G. Barwick, Wen-Ai Jackson, and Keith M. Martin. A general approach to robust Web metering. *Designs, Codes, and Cryptography*, 36

(1):5–27, July 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=36&issue=1&spage=5.

**Galati:2005:NES**

[780] John C. Galati. On the non-existence of semiregular relative difference sets in groups with all Sylow subgroups cyclic. *Designs, Codes, and Cryptography*, 36(1):29–31, July 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=36&issue=1&spage=29.

**Ciet:2005:ECC**

[781] Mathieu Ciet and Marc Joye. Elliptic curve cryptosystems in the presence of permanent and transient faults. *Designs, Codes, and Cryptography*, 36(1):33–43, July 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=36&issue=1&spage=33.

**Bracken:2005:CSD**

[782] Carl Bracken and Gary Mcguire. Characterization of SDP designs that yield certain spin models. *Designs, Codes, and Cryptography*, 36 (1):45–52, July 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=36&issue=1&spage=45.

**Lin:2005:GPW**

[783] Iuon-Chang Lin, Min-Shiang Hwang, and Chin-Chen Chang. The general pay-word: a micro-payment scheme based on $n$-dimension one-way hash chain. *Designs, Codes, and Cryptography*, 36(1):53–67, July 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=36&issue=1&spage=53.

**Lofvenberg:2005:BFC**

[784] J. Löfvenberg. Binary fingerprinting codes. *Designs, Codes, and Cryptography*, 36(1):69–81, July 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=36&issue=1&spage=69.

**Ji:2005:EGS**

[785] L. Ji, D. Wu, and L. Zhu. Existence of generalized Steiner systems $\mathrm{GS}(2, 4, \nu, 2)$. *Designs, Codes, and Cryptography*, 36(1):83–99, July 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=36&issue=1&spage=83.

**Eisfeld:2005:SSM**

[786] J. Eisfeld, L. Storme, and P. Sziklai. On the spectrum of the sizes of maximal partial line spreads in $\mathrm{PG}(2\mathrm{n}, \mathrm{q}), \mathrm{n} \geq 3$. *Designs, Codes, and Cryptography*, 36(1):101–110, July 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http:

//www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=36&issue=1&spage=101.

**DeKaey:2005:MGC**

[787] J. De Kaey. On a more general characterisation of Steiner systems. *Designs, Codes, and Cryptography*, 36 (2):117–129, August 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=36&issue=2&spage=117.

**Langevin:2005:NSI**

[788] P. Langevin and J.-P. Zanotti. Nonlinearity of some invariant Boolean functions. *Designs, Codes, and Cryptography*, 36(2):131–146, August 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=36&issue=2&spage=131.

**Chiera:2005:TIC**

[789] F. L. Chiera. Type II codes over $\mathbf{Z}/2k\mathbf{Z}$, invariant rings and theta series. *Designs, Codes, and Cryptography*, 36 (2):147–158, August 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=36&issue=2&spage=147.

**Zhou:2005:BPD**

[790] Shenglin Zhou. Block primitive $2-(v,k,1)$ designs admitting a Ree group of characteristic two. *Designs, Codes, and Cryptography*, 36 (2):159–169, August 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=36&issue=2&spage=159.

**Leung:2005:FDM**

[791] Ka Hin Leung and Bernhard Schmidt. The field descent method. *Designs, Codes, and Cryptography*, 36(2):171–188, August 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=36&issue=2&spage=171.

**Carlet:2005:CIF**

[792] Claude Carlet. Concatenating indicators of flats for designing cryptographic functions. *Designs, Codes, and Cryptography*, 36(2):189–202, August 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=36&issue=2&spage=189.

**Jha:2005:LSL**

[793] Vikram Jha. Local Schur's lemma and commutative semifields. *Designs, Codes, and Cryptography*, 36 (2):203–216, August 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=36&issue=2&spage=203.

**Gupta:2005:LCM**

[794] Manish K. Gupta, Mahesh C. Bhandari, and Arbind K. Lal. On linear codes over $\mathbf{Z}_2^s$. *Designs, Codes, and Cryptography*, 36(3):227–244, September 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=36&issue=3&spage=227`.

**Brown:2005:HCC**

[795] Ezra Brown, Bruce T. Myers, and Jerome A. Solinas. Hyperelliptic curves with compact parameters. *Designs, Codes, and Cryptography*, 36(3): 245–261, September 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=36&issue=3&spage=245`.

**Martin:2005:DED**

[796] Keith M. Martin, Rei Safavi-Naini, Huaxiong Wang, and Peter R. Wild. Distributing the encryption and decryption of a block cipher. *Designs, Codes, and Cryptography*, 36(3): 263–287, September 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=36&issue=3&spage=263`.

**Cheon:2005:NCA**

[797] E. J. Cheon, T. Kato, and S. J. Kim. Nonexistence of $[n, 5, d]_q$ codes attaining the Griesmer bound for $q^4 - 2q^2 - 2q + 1 \leq d \leq q^4 - 2q^2 - q$. *Designs, Codes, and Cryptography*, 36(3): 289–299, September 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=36&issue=3&spage=289`.

**Nieto:2005:PKC**

[798] Juan Manuel Gonzalez Nieto, Colin Boyd, and Ed Dawson. A public key cryptosystem based on a subgroup membership problem. *Designs, Codes, and Cryptography*, 36(3): 301–316, September 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=36&issue=3&spage=301`.

**Veron:2005:PCT**

[799] P. Véron. Proof of conjectures on the true dimension of some binary Goppa codes. *Designs, Codes, and Cryptography*, 36(3):317–325, September 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=36&issue=3&spage=317`.

**Ostergaard:2005:TNF**

[800] Patric R. J. Östergård. Two new four-error-correcting binary codes. *Designs, Codes, and Cryptography*, 36(3): 327–329, September 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=36&issue=3&spage=327`.

**Cohen:2005:FFE**

[801] Stephen D. Cohen. Finite field elements with specified order and traces. *Designs, Codes, and Cryptography*, 36 (3):331–340, September 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=36&issue=3&spage=331`.

**Anonymous:2005:VTC**

[802] Anonymous. Volume table of contents: Volume 36. *Designs, Codes, and Cryptography*, 36(3):341–342, September 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=36&issue=3&spage=341`.

**Golemac:2005:OSD**

[803] Anka Golemac, Tanja Vucicić, and Josko Mandić. One $(96, 20, 4)$-symmetric design and related non-abelian difference sets. *Designs, Codes, and Cryptography*, 37(1):5–13, October 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=37&issue=1&spage=5`.

**vanZanten:2005:CLA**

[804] A. J. van Zanten and I. Nengah Suparta. On the construction of linear $q$-ary lexicodes. *Designs, Codes, and Cryptography*, 37(1):15–29, October 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=37&issue=1&spage=15`.

**Langevin:2005:NLP**

[805] Philippe Langevin and Pascal Véron. On the non-linearity of power functions. *Designs, Codes, and Cryptography*, 37(1):31–43, October 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=37&issue=1&spage=31`.

**Keri:2005:BCC**

[806] Gerzson Kéri and Patric R. J. Östergård. Bounds for covering codes over large alphabets. *Designs, Codes, and Cryptography*, 37 (1):45–60, October 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=37&issue=1&spage=45`.

**Davydov:2005:CSC**

[807] Alexander A. Davydov, Giorgio Faina, and Fernanda Pambianco. Constructions of small complete caps in binary projective spaces. *Designs, Codes, and Cryptography*, 37(1):61–80, October 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=37&issue=1&spage=61`.

**Malone-Lee:2005:SNI**

[808] John Malone-Lee. Signcryption with non-interactive non-repudiation. *Designs, Codes, and Cryptography*, 37 (1):81–109, October 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=37&issue=1&spage=81`.

**Homma:2005:TDM**

[809] Masaaki Homma and Seon Jeong Kim. Toward the determination of the minimum distance of two–point codes on a Hermitian curve. *Designs, Codes, and Cryptography*, 37 (1):111–132, October 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=37&issue=1&spage=111`.

**Brezing:2005:ECS**

[810] Friederike Brezing and Annegret Weng. Elliptic curves suitable for pairing based cryptography. *Designs, Codes, and Cryptography*, 37(1):133–141, October 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=37&issue=1&spage=133`.

**Tayfeh-Rezaie:2005:ELS**

[811] B. Tayfeh-Rezaie. On the existence of large sets of $t$-designs of prime sizes. *Designs, Codes, and Cryptography*, 37 (1):143–149, October 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=37&issue=1&spage=143`.

**Ahlswede:2005:FVH**

[812] R. Ahlswede, H. Aydinian, and L. H. Khachatrian. Forbidden (0,1)-vectors in hyperplanes of $\mathbf{R}^n$: The unrestricted case. *Designs, Codes, and Cryptography*, 37(1):151–167, October 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=37&issue=1&spage=151`.

**Ang:2005:SWM**

[813] Miin Huey Ang and Siu Lun Ma. Symmetric weighing matrices constructed using group matrices. *Designs, Codes, and Cryptography*, 37(2): 195–210, November 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=37&issue=2&spage=195`.

**Bierbrauer:2005:FBN**

[814] Jürgen Bierbrauer and Yves Edel. A family of binary $(t, m, s)$-nets of strength 5. *Designs, Codes, and Cryptography*, 37(2):211–214, November 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=37&issue=2&spage=211`.

**Belyavskaya:2005:CCSa**

[815] G. B. Belyavskaya, V. I. Izbash, and G. L. Mullen. Check character systems using quasigroups: I. *Designs, Codes, and Cryptography*, 37(2): 215–227, November 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=37&issue=2&spage=215`.

**Safavi-naini:2005:MH**

[816] R. Safavi-naini and C. Charnes. MRD hashing. *Designs, Codes, and Cryptography*, 37(2):229–242, November 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=37&issue=2&spage=229`.

**Phelps:2005:KKA**

[817] K. T. Phelps, J. Rifà, and M. Villanueva. Kernels and $p$-kernels of $p^r$-ary 1-perfect codes. *Designs, Codes, and Cryptography*, 37(2):243–261, November 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=37&issue=2&spage=243`.

**DeBruyn:2005:SNP**

[818] Bart De Bruyn. Slim near polygons. *Designs, Codes, and Cryptography*, 37 (2):263–280, November 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=37&issue=2&spage=263`.

**Yin:2005:CDP**

[819] Jianxing Yin. Cyclic difference packing and covering arrays. *Designs, Codes, and Cryptography*, 37(2):281–292, November 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=37&issue=2&spage=281`.

**Suetake:2005:CST**

[820] Chihiro Suetake. The classification of symmetric transversal designs $\mathrm{STD}_4[12;3]$'s. *Designs, Codes, and Cryptography*, 37(2):293–304, November 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=37&issue=2&spage=293`.

**Spera:2005:AGC**

[821] Antonino Giorgio Spera. Asymptotically good codes from generalized algebraic–geometry codes. *Designs, Codes, and Cryptography*, 37(2): 305–312, November 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=37&issue=2&spage=305`.

**Mcsorley:2005:DATb**

[822] John P. Mcsorley. Double arrays, triple arrays and balanced grids with $v = r + c - 1$. *Designs,*

*Codes, and Cryptography*, 37(2):313–318, November 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=37&issue=2&spage=313`.

**Barwick:2005:OMT**

[823] S. G. Barwick and Wen-Ai Jackson. An optimal multisecret threshold scheme construction. *Designs, Codes, and Cryptography*, 37(3):367–389, December 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=37&issue=3&spage=367`.

**Dorofeev:2005:MGR**

[824] A. Ya. Dorofeev, L. S. Kazarin, V. M. Sidelnikov, and M. E. Tuzhilin. Matrix groups related to the quaternion group and spherical orbit codes. *Designs, Codes, and Cryptography*, 37(3):391–404, December 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=37&issue=3&spage=391`.

**Belyavskaya:2005:CCSb**

[825] G. B. Belyavskaya, V. I. Izbash, and G. L. Mullen. Check character systems using quasigroups: II. *Designs, Codes, and Cryptography*, 37(3):405–419, December 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=37&issue=3&spage=405`.

**Cheon:2005:MLS**

[826] E. J. Cheon, T. Kato, and S. J. Kim. On the minimum length of some linear codes of dimension 5. *Designs, Codes, and Cryptography*, 37(3):421–434, December 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=37&issue=3&spage=421`.

**Wispelaere:2005:CGH**

[827] A. Wispelaere and H. Maldeghem. Codes from generalized hexagons. *Designs, Codes, and Cryptography*, 37(3):435–448, December 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=37&issue=3&spage=435`.

**Carlet:2005:PCB**

[828] Claude Carlet and Joseph L. Yucas. Piecewise constructions of bent and almost optimal Boolean functions. *Designs, Codes, and Cryptography*, 37(3):449–464, December 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=37&issue=3&spage=449`.

**Gulliver:2005:NEF**

[829] T. Aaron Gulliver, Masaaki Harada, Takuji Nishimura, and Patric R. J. Östergård. Near-extremal formally self-dual even codes of lengths 24 and 32.

*Designs, Codes, and Cryptography*, 37 (3):465–471, December 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=37&issue=3&spage=465`.

**Matthews:2005:WSC**

[830] Gretchen L. Matthews. Weierstrass semigroups and codes from a quotient of the Hermitian curve. *Designs, Codes, and Cryptography*, 37(3): 473–492, December 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=37&issue=3&spage=473`.

**Ahmadi:2005:NTO**

[831] Omran Ahmadi and Alfred Menezes. On the number of trace-one elements in polynomial bases for $\mathbf{F}_2^n$. *Designs, Codes, and Cryptography*, 37(3): 493–507, December 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=37&issue=3&spage=493`.

**Bohli:2005:WKM**

[832] Jens-Matthias Bohli, Rainer Steinwandt, María Isabel González Vasco, and Consuelo Martínez. Weak keys in $\mathrm{MST}_1$. *Designs, Codes, and Cryptography*, 37(3):509–524, December 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=37&issue=3&spage=509`.

**Harada:2006:SOD**

[833] Masaaki Harada. Self-orthogonal $3-(56,12,65)$ designs and extremal doubly-even self-dual codes of length 56. *Designs, Codes, and Cryptography*, 38(1):5–16, January 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=38&issue=1&spage=5`.

**Ozen:2006:LCR**

[834] Mehmet Ozen and Irfan Siap. Linear codes over $\mathbf{F}_q[u]/(u^s)$ with respect to the Rosenbloom–Tsfasman metric. *Designs, Codes, and Cryptography*, 38 (1):17–29, January 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=38&issue=1&spage=17`.

**Alderson:2006:MCA**

[835] T. L. Alderson. $(6,3)$-MDS codes over an alphabet of size 4. *Designs, Codes, and Cryptography*, 38 (1):31–40, January 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=38&issue=1&spage=31`.

**Coron:2006:ICA**

[836] Jean-Sébastien Coron, David Naccache, Yvo Desmedt, Andrew Odlyzko, and Julien P. Stern. Index calculation attacks on RSA signa-

ture and encryption. *Designs, Codes, and Cryptography*, 38(1):41–53, January 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=38&issue=1&spage=41.

**Homma:2006:TPCa**

[837] Masaaki Homma and Seon Jeong Kim. The two-point codes on a Hermitian curve with the designed minimum distance. *Designs, Codes, and Cryptography*, 38(1):55–81, January 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=38&issue=1&spage=55.

**Ji:2006:ADL**

[838] L. Ji. Asymptotic determination of the last packing number of quadruples. *Designs, Codes, and Cryptography*, 38 (1):83–95, January 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=38&issue=1&spage=83.

**Dougherty:2006:HWT**

[839] Steven T. Dougherty, T. Aaron. Gulliver, and Manabu Oura. Higher weights for ternary and quaternary self-dual codes. *Designs, Codes, and Cryptography*, 38(1):97–112, January 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=38&issue=1&spage=97.

**Lavrauw:2006:SPO**

[840] Michel Lavrauw. Sublines of prime order contained in the set of internal points of a conic. *Designs, Codes, and Cryptography*, 38(1):113–123, January 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=38&issue=1&spage=113.

**Heden:2006:FRP**

[841] Olof Heden. A full rank perfect code of length 31. *Designs, Codes, and Cryptography*, 38(1):125–129, January 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=38&issue=1&spage=125.

**Ball:2006:OPQ**

[842] Simeon Ball, Patrick Govaerts, and Leo Storme. On ovoids of parabolic quadrics. *Designs, Codes, and Cryptography*, 38(1):131–145, January 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=38&issue=1&spage=131.

**Meidl:2006:SNL**

[843] Wilfried Meidl and Arne Winterhof. Some notes on the linear complexity of Sidel'nikov–Lempel–Cohn–Eastman sequences. *Designs,*

*Codes, and Cryptography*, 38(2):159–178, February 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=38&issue=2&spage=159`.

**deClerck:2006:DRR**

[844] Frank de Clerck, Stefaan de Winter, Elisabeth Kuijken, and Cristina Tonesi. Distance-regular $(0, \alpha)$-reguli. *Designs, Codes, and Cryptography*, 38 (2):179–194, February 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=38&issue=2&spage=179`.

**Cauchie:2006:CCH**

[845] Sara Cauchie. A characterization of the complement of a hyperbolic quadric in PG$(3, q)$, for $q$ odd. *Designs, Codes, and Cryptography*, 38 (2):195–208, February 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=38&issue=2&spage=195`.

**Scott:2006:GMM**

[846] Michael Scott and Paulo S. L. M. Barreto. Generating more MNT elliptic curves. *Designs, Codes, and Cryptography*, 38(2):209–217, February 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=38&issue=2&spage=209`.

**Horng:2006:CVC**

[847] Gwoboa Horng, Tzungher Chen, and Du shiau Tsai. Cheating in visual cryptography. *Designs, Codes, and Cryptography*, 38(2):219–236, February 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=38&issue=2&spage=219`.

**Juels:2006:FVS**

[848] Ari Juels and Madhu Sudan. A fuzzy vault scheme. *Designs, Codes, and Cryptography*, 38(2):237–257, February 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=38&issue=2&spage=237`.

**Stinson:2006:SOT**

[849] D. R. Stinson. Some observations on the theory of cryptographic hash functions. *Designs, Codes, and Cryptography*, 38(2):259–277, February 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=38&issue=2&spage=259`.

**Khoo:2006:NCS**

[850] Khoongming Khoo, Guang Gong, and Douglas R. Stinson. A new characterization of semi-bent and bent functions on finite fields*. *Designs, Codes, and Cryptography*, 38(2):279–295, February 2006. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=38&issue=2&spage=279.

**Merchant:2006:EMH**

[851] Eric Merchant. Exponentially many Hadamard designs. *Designs, Codes, and Cryptography*, 38(2):297–308, February 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=38&issue=2&spage=297.

**Kamiya:2006:QCC**

[852] Norifumi Kamiya and Marc P. C. Fossorier. Quasi-cyclic codes from a finite affine plane. *Designs, Codes, and Cryptography*, 38(3):311–329, March 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=38&issue=3&spage=311.

**Rosendahl:2006:GNT**

[853] Petri Rosendahl. A generalization of Niho's Theorem. *Designs, Codes, and Cryptography*, 38(3):331–336, March 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=38&issue=3&spage=331.

**Ling:2006:ASQ**

[854] San Ling, Harald Niederreiter, and Patrick Solé. On the algebraic structure of quasi-cyclic codes IV: Repeated roots. *Designs, Codes, and Cryptography*, 38(3):337–361, March 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=38&issue=3&spage=337.

**Grolmusz:2006:COC**

[855] Vince Grolmusz. Co-orthogonal codes. *Designs, Codes, and Cryptography*, 38 (3):363–372, March 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=38&issue=3&spage=363.

**Wang:2006:NCO**

[856] Jinhua Wang. A new class of optimal 3-splitting authentication codes. *Designs, Codes, and Cryptography*, 38 (3):373–381, March 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=38&issue=3&spage=373.

**Weng:2006:LMA**

[857] Annegret Weng. A low-memory algorithm for point counting on Picard curves. *Designs, Codes, and Cryptography*, 38(3):383–393, March 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=38&issue=3&spage=383.

**Ahmadi:2006:SRI**

[858] Omran Ahmadi. Self-reciprocal irreducible pentanomials over $\mathbf{F}_2$. *Designs, Codes, and Cryptography*, 38 (3):395–397, March 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=38&issue=3&spage=395`.

**Arazi:2006:CCT**

[859] Benjamin Arazi. Communication-computation trade-off in executing ECDSA in a contactless Smartcard. *Designs, Codes, and Cryptography*, 38 (3):399–415, March 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=38&issue=3&spage=399`.

**Dover:2006:SSH**

[860] Jeremy Dover. Subregular spreads of Hermitian unitals. *Designs, Codes, and Cryptography*, 39(1):5–15, April 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=39&issue=1&spage=5`.

**Khatirinejad:2006:CCC**

[861] Mahdad Khatirinejad and Petr Lisonek. Classification and constructions of complete caps in binary spaces. *Designs, Codes, and Cryptography*, 39 (1):17–31, April 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=39&issue=1&spage=17`.

**Cossidente:2006:AGP**

[862] A. Cossidente and A. Siciliano. The automorphism group of plane algebraic curves with Singer automorphisms. *Designs, Codes, and Cryptography*, 39(1):33–37, April 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=39&issue=1&spage=33`.

**Feng:2006:EZC**

[863] Tao Feng and Yanxun Chang. Existence of Z-cyclic 3PTWh($p$) for any prime $p \equiv 1 \pmod 4$. *Designs, Codes, and Cryptography*, 39 (1):39–49, April 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=39&issue=1&spage=39`.

**Garciano:2006:RDS**

[864] Agnes D. Garciano, Yutaka Hiramine, and Takeo Yokonuma. On relative difference sets in dihedral groups. *Designs, Codes, and Cryptography*, 39(1):51–63, April 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=39&issue=1&spage=51`.

**Dougherty:2006:CAI**

[865] Steven T. Dougherty and Young Ho Park. Codes over the $p$-adic inte-

gers. *Designs, Codes, and Cryptography*, 39(1):65–80, April 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=39&issue=1&spage=65`.

**DeWinter:2006:GQA**

[866] S. De Winter and K. Thas. Generalized quadrangles with an Abelian Singer group. *Designs, Codes, and Cryptography*, 39(1):81–87, April 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=39&issue=1&spage=81`.

**Masucci:2006:SMS**

[867] Barbara Masucci. Sharing multiple secrets: Models, schemes and analysis. *Designs, Codes, and Cryptography*, 39(1):89–111, April 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=39&issue=1&spage=89`.

**Shparlinski:2006:RMP**

[868] Igor E. Shparlinski. On RSA moduli with prescribed bit patterns. *Designs, Codes, and Cryptography*, 39 (1):113–122, April 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=39&issue=1&spage=113`.

**Dougherty:2006:CCE**

[869] Steven T. Dougherty and San Ling. Cyclic codes over $\mathbf{Z}_4$ of even length. *Designs, Codes, and Cryptography*, 39(2):127–153, May 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=39&issue=2&spage=127`.

**Aly:2006:LCP**

[870] Hassan Aly and Arne Winterhof. On the linear complexity profile of nonlinear congruential pseudorandom number generators with Dickson polynomials. *Designs, Codes, and Cryptography*, 39(2):155–162, May 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=39&issue=2&spage=155`.

**Giudici:2006:CCW**

[871] Michael Giudici. Codes with a certain weight-preserving transitive group of automorphisms. *Designs, Codes, and Cryptography*, 39(2):163–172, May 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=39&issue=2&spage=163`.

**Chen:2006:SSD**

[872] Kejun Chen and Ruizhong Wei. Super-simple $(\nu, 5, 5)$ designs. *Designs, Codes, and Cryptography*, 39 (2):173–187, May 2006. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=39&issue=2&spage=173.

**Ciet:2006:TIM**

[873] Mathieu Ciet, Marc Joye, Kristin Lauter, and Peter L. Montgomery. Trading inversions for multiplications in elliptic curve cryptography. *Designs, Codes, and Cryptography*, 39 (2):189–206, May 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=39&issue=2&spage=189.

**Bini:2006:CRF**

[874] Gilberto Bini. $A$-codes from rational functions over Galois rings. *Designs, Codes, and Cryptography*, 39 (2):207–214, May 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=39&issue=2&spage=207.

**Guneri:2006:IGH**

[875] Cem Güneri and Ferruh Özbudak. Improvements on generalized Hamming weights of some trace codes. *Designs, Codes, and Cryptography*, 39 (2):215–231, May 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=39&issue=2&spage=215.

**Piret:2006:LRR**

[876] Gilles Piret. Luby–Rackoff revisited: On the use of permutations as inner functions of a Feistel scheme. *Designs, Codes, and Cryptography*, 39 (2):233–245, May 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=39&issue=2&spage=233.

**Crnkovic:2006:SRH**

[877] Dean Crnković. A series of regular Hadamard matrices. *Designs, Codes, and Cryptography*, 39(2):247–251, May 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=39&issue=2&spage=247.

**VanDijk:2006:SEU**

[878] Marten Van Dijk, Dwaine Clarke, Blaise Gassend, G. Edward Suh, and Srinivas Devadas. Speeding up exponentiation using an untrusted computational resource. *Designs, Codes, and Cryptography*, 39(2):253–273, May 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=39&issue=2&spage=253.

**Darafsheh:2006:DGE**

[879] M. R. Darafsheh. Designs from the group $\mathrm{PSL}_2(q)$, $q$ even. *Designs, Codes, and Cryptography*, 39 (3):311–316, June 2006. CODEN

DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=39&issue=3&spage=311.

**Avgustinovich:2006:IPP**

[880] Sergey V. Avgustinovich, Olof Heden, and Faina I. Solov'eva. On intersection problem for perfect binary codes. *Designs, Codes, and Cryptography*, 39(3):317–322, June 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=39&issue=3&spage=317.

**DeBeule:2006:BAG**

[881] Jan De Beule and Leo Storme. Blocking all generators of $Q^+(2n+1,3)$, $n \geq 4$. *Designs, Codes, and Cryptography*, 39(3):323–333, June 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=39&issue=3&spage=323.

**Chang:2006:NAD**

[882] Jen-Chun Chang. New algorithms of distance-increasing mappings from binary vectors to permutations by swaps. *Designs, Codes, and Cryptography*, 39(3):335–345, June 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=39&issue=3&spage=335.

**Maffre:2006:WKT**

[883] Samuel Maffre. A weak key test for braid based cryptography. *Designs, Codes, and Cryptography*, 39(3):347–373, June 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=39&issue=3&spage=347.

**Homma:2006:TPCb**

[884] Masaaki Homma and Seon Jeong Kim. The two-point codes with the designed distance on a Hermitian curve in even characteristic. *Designs, Codes, and Cryptography*, 39(3):375–386, June 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=39&issue=3&spage=375.

**OBrien:2006:BCD**

[885] Katie M. O'Brien and Patrick Fitzpatrick. Bounds on codes derived by counting components in Varshamov graphs. *Designs, Codes, and Cryptography*, 39(3):387–396, June 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=39&issue=3&spage=387.

**Aguglia:2006:BSC**

[886] Angela Aguglia and Massimo Giulietti. Blocking sets of certain line sets related to a conic. *Designs, Codes, and Cryptography*, 39(3):397–

405, June 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=39&issue=3&spage=397.

**Homma:2006:CDM**

[887] Masaaki Homma and Seon Jeong Kim. The complete determination of the minimum distance of two-point codes on a Hermitian curve. *Designs, Codes, and Cryptography*, 40 (1):5–24, July 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=40&issue=1&spage=5.

**Grabner:2006:NOB**

[888] Peter J. Grabner and Clemens Heuberger. On the number of optimal base 2 representations of integers. *Designs, Codes, and Cryptography*, 40(1):25–39, July 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=40&issue=1&spage=25.

**Dalai:2006:BTC**

[889] Deepak Kumar Dalai, Subhamoy Maitra, and Sumanta Sarkar. Basic theory in construction of Boolean functions with maximum possible annihilator immunity. *Designs, Codes, and Cryptography*, 40(1): 41–58, July 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=40&issue=1&spage=41.

**Rodier:2006:ANB**

[890] François Rodier. Asymptotic nonlinearity of Boolean functions. *Designs, Codes, and Cryptography*, 40 (1):59–70, July 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=40&issue=1&spage=59.

**Carlet:2006:ASH**

[891] Claude Carlet, Cunsheng Ding, and Harald Niederreiter. Authentication schemes from highly nonlinear functions. *Designs, Codes, and Cryptography*, 40(1):71–79, July 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=40&issue=1&spage=71.

**Koga:2006:BPR**

[892] Hiroki Koga and Etsuyo Ueda. Basic properties of the $(t, n)$-threshold visual secret sharing scheme with perfect reconstruction of black pixels. *Designs, Codes, and Cryptography*, 40(1):81–102, July 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=40&issue=1&spage=81.

**Herranz:2006:DRS**

[893] Javier Herranz and Germán Sáez. Distributed ring signatures from general dual access structures. *De-*

*signs, Codes, and Cryptography*, 40 (1):103–120, July 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=40&issue=1&spage=103`.

**Evans:2006:LSO**

[894] Anthony B. Evans. Latin squares without orthogonal mates. *Designs, Codes, and Cryptography*, 40 (1):121–130, July 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=40&issue=1&spage=121`.

**Wanless:2006:ELS**

[895] Ian M. Wanless and Bridget S. Webb. The existence of Latin squares without orthogonal mates. *Designs, Codes, and Cryptography*, 40(1):131–135, July 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=40&issue=1&spage=131`.

**Huang:2006:CPA**

[896] Yen-Ying Huang, Shi-Chun Tsai, and Hsin-Lung Wu. On the construction of permutation arrays via mappings from binary vectors to permutations. *Designs, Codes, and Cryptography*, 40 (2):139–155, August 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=40&issue=2&spage=139`.

**Ding:2006:COC**

[897] Cunsheng Ding and Jianxing Yin. A construction of optimal constant composition codes. *Designs, Codes, and Cryptography*, 40(2):157–165, August 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=40&issue=2&spage=157`.

**Chang:2006:CED**

[898] Yanxun Chang and Cunsheng Ding. Constructions of external difference families and disjoint difference families. *Designs, Codes, and Cryptography*, 40(2):167–185, August 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=40&issue=2&spage=167`.

**Osuna:2006:TST**

[899] Octavio Páez Osuna. There are 1239 Steiner triple systems STS(31) of 2-rank 27. *Designs, Codes, and Cryptography*, 40(2):187–190, August 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=40&issue=2&spage=187`.

**Long:2006:GCA**

[900] Shoulun Long, Josef Pieprzyk, Huaxiong Wang, and Duncan S. Wong. Generalised cumulative arrays in secret sharing. *Designs, Codes, and Cryptography*, 40(2):191–209, August 2006. CODEN DCCREC.

ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=40&issue=2&spage=191.

**Abel:2006:EPM**

[901] R. J. R. Abel and F. E. Bennett. The existence of $(\nu, 6, \lambda)$-perfect Mendelsohn designs with $\lambda > 1$. *Designs, Codes, and Cryptography*, 40 (2):211–224, August 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=40&issue=2&spage=211.

**Grannell:2006:FUM**

[902] Mike J. Grannell, Terry S. Griggs, and Anne Penfold Street. A flaw in the use of minimal defining sets for secret sharing schemes. *Designs, Codes, and Cryptography*, 40 (2):225–236, August 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=40&issue=2&spage=225.

**Faldum:2006:EPB**

[903] Andreas Faldum, Julio Lafuente, Gustavo Ochoa, and Wolfgang Willems. Error probabilities for bounded distance decoding. *Designs, Codes, and Cryptography*, 40(2):237–252, August 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=40&issue=2&spage=237.

**Bose:2006:OVC**

[904] Mausumi Bose and Rahul Mukerjee. Optimal $(2, n)$ visual cryptographic schemes. *Designs, Codes, and Cryptography*, 40(3):255–267, September 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=40&issue=3&spage=255.

**McKay:2006:NTL**

[905] Brendan D. McKay, Jeanette C. McLeod, and Ian M. Wanless. The number of transversals in a Latin square. *Designs, Codes, and Cryptography*, 40(3):269–284, September 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=40&issue=3&spage=269.

**Wolf:2006:SST**

[906] Christopher Wolf, An Braeken, and Bart Preneel. On the security of stepwise triangular systems. *Designs, Codes, and Cryptography*, 40(3): 285–302, September 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=40&issue=3&spage=285.

**Ge:2006:GDA**

[907] Gennian Ge, Ying Miao, and L. Zhu. GOB designs for authentication codes with arbitration. *Designs, Codes, and Cryptography*, 40(3):303–317,

September 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=40&issue=3&spage=303.

**Heden:2006:CPC**

[908] Olof Heden and Martin Hessler. On the classification of perfect codes: side class structures. *Designs, Codes, and Cryptography*, 40(3):319–333, September 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=40&issue=3&spage=319.

**Glynn:2006:PDG**

[909] David G. Glynn, Johannes G. Maks, and Rey Casse. The polynomial degree of the Grassmannian $G(1, n, q)$ of lines in finite projective space $\mathrm{PG}(n, q)$. *Designs, Codes, and Cryptography*, 40 (3):335–341, September 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=40&issue=3&spage=335.

**Droms:2006:LCG**

[910] Sean V. Droms, Keith E. Mellinger, and Chris Meyer. LDPC codes generated by conics in the classical projective plane. *Designs, Codes, and Cryptography*, 40(3):343–356, September 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=40&issue=3&spage=343.

**Horak:2006:FDQ**

[911] Peter Horak and Bader F. AlBdaiwi. Fast decoding of quasi-perfect Lee distance codes. *Designs, Codes, and Cryptography*, 40(3):357–367, September 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=40&issue=3&spage=357.

**Aly:2006:ELC**

[912] Hassan Aly and Arne Winterhof. On the $k$-error linear complexity over $\mathbf{F}_p$ of Legendre and Sidelnikov sequences. *Designs, Codes, and Cryptography*, 40 (3):369–374, September 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=40&issue=3&spage=369.

**Safavi-Naini:2006:SSS**

[913] Rei Safavi-Naini and Huaxiong Wang. Secret sharing schemes with partial broadcast channels. *Designs, Codes, and Cryptography*, 41(1):5–22, October 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=41&issue=1&spage=5.

**Moncel:2006:CCI**

[914] Julien Moncel. Constructing codes identifying sets of vertices. *Designs, Codes, and Cryptography*, 41

(1):23–31, October 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=41&issue=1&spage=23.

**Colbourn:2006:RTC**

[915] Charles J. Colbourn, Sosina S. Martirosyan, Tran Van Trung, and Robert A. Walker. Roux-type constructions for covering arrays of strengths three and four. *Designs, Codes, and Cryptography*, 41(1):33–57, October 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=41&issue=1&spage=33.

**Bouyukliev:2006:PTW**

[916] Iliya Bouyukliev, Veerle Fack, Wolfgang Willems, and Joost Winne. Projective two-weight codes with small parameters and their corresponding graphs. *Designs, Codes, and Cryptography*, 41(1):59–78, October 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=41&issue=1&spage=59.

**Keevash:2006:RCP**

[917] Peter Keevash and Cheng Yeaw Ku. A random construction for permutation codes and the covering radius. *Designs, Codes, and Cryptography*, 41 (1):79–86, October 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=41&issue=1&spage=79.

**Grolmusz:2006:PCP**

[918] Vince Grolmusz. Pairs of codes with prescribed Hamming distances and coincidences. *Designs, Codes, and Cryptography*, 41(1):87–99, October 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=41&issue=1&spage=87.

**Bouyuklieva:2006:NCO**

[919] Stefka Bouyuklieva and Patric R. J. Östergård. New constructions of optimal self-dual binary codes of length 54. *Designs, Codes, and Cryptography*, 41(1):101–109, October 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=41&issue=1&spage=101.

**Arasu:2006:CWM**

[920] K. T. Arasu, Ka Hin Leung, Siu Lun Ma, Ali Nabavi, and D. K. Ray-Chaudhuri. Circulant weighing matrices of weight $2^{2t}$. *Designs, Codes, and Cryptography*, 41(1):111–123, October 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=41&issue=1&spage=111.

**Jha:2006:SPA**

[921] Vikram Jha and Norman L. Johnson. Subregular planes admitting elations. *Designs, Codes, and Cryptography*, 41 (2):125–145, November 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=41&issue=2&spage=125`.

**Muniz:2006:IEH**

[922] Marcelo Muniz. Isometric embeddings of $\mathbf{Z}_p^k$ in the Hamming space $\mathbf{F}_p^N$ and $\mathbf{Z}_p^k$-linear codes. *Designs, Codes, and Cryptography*, 41(2):147–152, November 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=41&issue=2&spage=147`.

**Bailey:2006:UBB**

[923] Robert F. Bailey. Uncoverings-by-bases for base-transitive permutation groups. *Designs, Codes, and Cryptography*, 41 (2):153–176, November 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=41&issue=2&spage=153`.

**Cao:2006:CCO**

[924] Zhenfu Cao, Gennian Ge, and Ying Miao. Combinatorial characterizations of one-coincidence frequency-hopping sequences. *Designs, Codes, and Cryptography*, 41(2):177–184, November 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=41&issue=2&spage=177`.

**Miklavic:2006:DTD**

[925] Stefko Miklavic and Primoz Potocnik. Distance-transitive dihedrants. *Designs, Codes, and Cryptography*, 41(2): 185–193, November 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=41&issue=2&spage=185`.

**Bracken:2006:NQS**

[926] Carl Bracken, Gary McGuire, and Harold Ward. New quasi-symmetric designs constructed using mutually orthogonal Latin squares and Hadamard matrices. *Designs, Codes, and Cryptography*, 41(2):195–198, November 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=41&issue=2&spage=195`.

**Galindo:2006:ECP**

[927] C. Galindo and M. Sanchis. Evaluation codes and plane valuations. *Designs, Codes, and Cryptography*, 41(2): 199–219, November 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=41&issue=2&spage=199`.

**Liu:2006:ECS**

[928] Lihua Liu and Hao Shen. Explicit constructions of separating hash families from algebraic curves over finite fields. *Designs, Codes, and Cryptography*, 41 (2):221–233, November 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=41&issue=2&spage=221`.

**Dougherty:2006:SDC**

[929] Steven T. Dougherty, T. Aaron Gulliver, and John Wong. Self-dual codes over $\mathbf{Z}_8$ and $\mathbf{Z}_9$. *Designs, Codes, and Cryptography*, 41(3):235–249, December 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=41&issue=3&spage=235`.

**Hasegawa:2006:SOP**

[930] Takehiro Hasegawa, Shoichi Kondo, and Hidekazu Kurusu. A sequence of one-point codes from a tower of function fields. *Designs, Codes, and Cryptography*, 41(3):251–267, December 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=41&issue=3&spage=251`.

**Shen:2006:ERG**

[931] Jun Shen and Hao Shen. Embeddings of resolvable group divisible designs with block size 3. *Designs, Codes, and Cryptography*, 41(3):269–298, December 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=41&issue=3&spage=269`.

**Kwon:2006:SPR**

[932] Soonhak Kwon, Chang Hoon Kim, and Chun Pyo Hong. Sparse polynomials, redundant bases, Gauss periods, and efficient exponentiation of primitive elements for small characteristic finite fields. *Designs, Codes, and Cryptography*, 41(3):299–306, December 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=41&issue=3&spage=299`.

**Miri:2006:ART**

[933] Ali Miri, Monica Nevins, and Terasan Niyomsataya. Applications of representation theory to wireless communications. *Designs, Codes, and Cryptography*, 41(3):307–318, December 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=41&issue=3&spage=307`.

**Bracken:2006:NCS**

[934] Carl Bracken. New classes of self-complementary codes and quasi-symmetric designs. *Designs, Codes, and Cryptography*, 41(3):319–323, December 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http:`

//www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=41&issue=3&spage=319.

**Vontobel:2006:UDM**

[935] Pascal O. Vontobel and Ashwin Ganesan. On universally decodable matrices for space-time coding. *Designs, Codes, and Cryptography*, 41(3): 325–342, December 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=41&issue=3&spage=325.

**Ozbudak:2006:SCS**

[936] Ferruh Özbudak and Zülfükar Saygi. Some constructions of systematic authentication codes using Galois rings. *Designs, Codes, and Cryptography*, 41 (3):343–357, December 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=41&issue=3&spage=343.

**Blunck:2007:LDD**

[937] Andrea Blunck, Hans Havlicek, and Corrado Zanella. Lifting of divisible designs. *Designs, Codes, and Cryptography*, 42(1):1–14, January 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=42&issue=1&spage=1.

**Lee:2007:RWD**

[938] Chong-Dao Lee, Yaotsu Chang, and Trieu-Kien Truong. A result on the weight distributions of binary quadratic residue codes. *Designs, Codes, and Cryptography*, 42(1):15–20, January 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=42&issue=1&spage=15.

**Roelse:2007:DCP**

[939] Peter Roelse. The design of composite permutations with applications to DES-like S-boxes. *Designs, Codes, and Cryptography*, 42 (1):21–42, January 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=42&issue=1&spage=21.

**Ebeid:2007:BSD**

[940] Nevine Ebeid and M. Anwar Hasan. On binary signed digit representations of integers. *Designs, Codes, and Cryptography*, 42(1):43–65, January 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=42&issue=1&spage=43.

**Litsyn:2007:ILB**

[941] Simon Litsyn and Beniamin Mounits. Improved lower bounds on sizes of single-error correcting codes. *Designs, Codes, and Cryptography*, 42 (1):67–72, January 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.

asp?genre=article&issn=0925-1022&volume=42&issue=1&spage=67.

**Kim:2007:SWC**

[942] Jon-Lark Kim, Keith E. Mellinger, and Leo Storme. Small weight codewords in LDPC codes defined by (dual) classical generalized quadrangles. *Designs, Codes, and Cryptography*, 42 (1):73–92, January 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=42&issue=1&spage=73.

**Chigira:2007:ESD**

[943] Naoki Chigira, Masaaki Harada, and Masaaki Kitazume. Extremal self-dual codes of length 64 through neighbors and covering radii. *Designs, Codes, and Cryptography*, 42(1):93–101, January 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=42&issue=1&spage=93.

**Cossidente:2007:VET**

[944] Antonio Cossidente and Giuseppe Marino. Veronese embedding and two-character sets. *Designs, Codes, and Cryptography*, 42(1):103–107, January 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=42&issue=1&spage=103.

**Hu:2007:CSN**

[945] Bessie C. Hu, Duncan S. Wong, Zhenfeng Zhang, and Xiaotie Deng. Certificateless signature: a new security model and an improved generic construction. *Designs, Codes, and Cryptography*, 42(2):109–126, February 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=42&issue=2&spage=109.

**Bierbrauer:2007:DAL**

[946] Jürgen Bierbrauer. A direct approach to linear programming bounds for codes and tms-nets. *Designs, Codes, and Cryptography*, 42(2):127–143, February 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=42&issue=2&spage=127.

**Gharge:2007:QAS**

[947] Sanjeevani Gharge and Sharad Sane. Quasi-affine symmetric designs. *Designs, Codes, and Cryptography*, 42 (2):145–166, February 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=42&issue=2&spage=145.

**Salomon:2007:RMC**

[948] Amir J. Salomon and Ofer Amrani. Reed–Muller codes and Barnes–Wall lattices: Generalized multilevel constructions and representation over GF($2^q$). *Designs,*

*Codes, and Cryptography*, 42(2):167–180, February 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=42&issue=2&spage=167.

**Meidl:2007:REL**

[949] Wilfried Meidl and Ayineedi Venkateswarlu. Remarks on the $k$-error linear complexity of $p^n$-periodic sequences. *Designs, Codes, and Cryptography*, 42 (2):181–193, February 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=42&issue=2&spage=181.

**Paterson:2007:SWD**

[950] Maura Paterson. Sliding-window dynamic frameproof codes. *Designs, Codes, and Cryptography*, 42(2):195–212, February 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=42&issue=2&spage=195.

**Gonzalez:2007:SSB**

[951] S. González, C. Martínez, and I. F. Rúa. Symplectic spread-based generalized Kerdock codes. *Designs, Codes, and Cryptography*, 42(2):213–226, February 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=42&issue=2&spage=213.

**Tonien:2007:CDC**

[952] Dongvu Tonien and Reihaneh Safavi-Naini. Construction of deletion correcting codes using generalized Reed–Solomon codes and their subcodes. *Designs, Codes, and Cryptography*, 42 (2):227–237, February 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=42&issue=2&spage=227.

**Barreto:2007:EPC**

[953] Paulo S. L. M. Barreto, Steven D. Galbraith, Colm Ó'hÉigeartaigh, and Michael Scott. Efficient pairing computation on supersingular Abelian varieties. *Designs, Codes, and Cryptography*, 42(3):239–271, March 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=42&issue=3&spage=239.

**Abualrub:2007:CCR**

[954] Taher Abualrub and Irfan Siap. Cyclic codes over the rings $Z_2 + uZ_2$ and $Z_2 + uZ_2 + u^2Z_2$. *Designs, Codes, and Cryptography*, 42 (3):273–287, March 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=42&issue=3&spage=273.

**Byrne:2007:LPB**

[955] Eimear Byrne, Marcus Greferath, and Michael E. O'Sullivan. The linear programming bound for codes

over finite Frobenius rings. *Designs, Codes, and Cryptography*, 42 (3):289–301, March 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=42&issue=3&spage=289`. See errata [1003].

**Pepe:2007:LCH**

[956] Valentina Pepe. LDPC codes from the Hermitian curve. *Designs, Codes, and Cryptography*, 42(3):303–315, March 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=42&issue=3&spage=303`.

**Paterson:2007:SDF**

[957] Maura Paterson. Sequential and dynamic frameproof codes. *Designs, Codes, and Cryptography*, 42(3):317–326, March 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=42&issue=3&spage=317`.

**Vega:2007:NCW**

[958] Gerardo Vega and Jacques Wolfmann. New classes of 2-weight cyclic codes. *Designs, Codes, and Cryptography*, 42 (3):327–334, March 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=42&issue=3&spage=327`.

**Westerback:2007:MPP**

[959] Thomas Westerbäck. Maximal partial packings of $Z_2^n$ with perfect codes. *Designs, Codes, and Cryptography*, 42 (3):335–355, March 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=42&issue=3&spage=335`.

**Kelly:2007:CIS**

[960] Shane Kelly. Constructions of intriguing sets of polar spaces from field reduction and derivation. *Designs, Codes, and Cryptography*, 43 (1):1–8, April 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=43&issue=1&spage=1`.

**Fu:2007:CBC**

[961] Fang-Wei Fu and Shu-Tao Xia. The characterization of binary constant weight codes meeting the bound of Fu and Shen. *Designs, Codes, and Cryptography*, 43(1):9–20, April 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=43&issue=1&spage=9`.

**DeFeyter:2007:CGE**

[962] Nikias De Feyter. Classification of $(0, 2)$-geometries embedded in $\mathrm{AG}(3, q)$. *Designs, Codes, and Cryptography*, 43(1):21–32, April 2007. CODEN DCCREC. ISSN 0925-1022

(print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=43&issue=1&spage=21.

**Caggegi:2007:DTI**

[963] Andrea Caggegi and Giovanni Falcone. On $2-(n^2, 2n, 2n-1)$ designs with three intersection numbers. *Designs, Codes, and Cryptography*, 43(1):33–40, April 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=43&issue=1&spage=33.

**Giese:2007:DDD**

[964] Sabine Giese and Ralph-Hardo Schulz. Divisible designs with dual translation group. *Designs, Codes, and Cryptography*, 43(1):41–45, April 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=43&issue=1&spage=41.

**Izu:2007:LDA**

[965] Tetsuya Izu, Jun Kogure, Takeshi Koshiba, and Takeshi Shimoyama. Low-density attack revisited. *Designs, Codes, and Cryptography*, 43 (1):47–59, April 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=43&issue=1&spage=47.

**Kiayias:2007:CPR**

[966] Aggelos Kiayias and Moti Yung. Cryptanalyzing the polynomial-reconstruction based public-key system under optimal parameter choice. *Designs, Codes, and Cryptography*, 43(2–3): 61–78, June 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=43&issue=2&spage=61.

**Jedwab:2007:TNB**

[967] Jonathan Jedwab and Matthew G. Parker. There are no Barker arrays having more than two dimensions. *Designs, Codes, and Cryptography*, 43 (2–3):79–84, June 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=43&issue=2&spage=79.

**Gashkov:2007:GAF**

[968] I. Gashkov, J. A. O. Ekberg, and D. Taub. A geometric approach to finding new lower bounds of $A(n, d, w)$. *Designs, Codes, and Cryptography*, 43(2–3):85–91, June 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=43&issue=2&spage=85.

**Jang:2007:BHM**

[969] Ji-Woong Jang, Jong-Seon No, and Habong Chung. Butson Hadamard matrices with partially cyclic core. *Designs, Codes, and Cryptography*, 43 (2–3):93–101, June 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.

asp?genre=article&issn=0925-1022&volume=43&issue=2&spage=93.

**Arhin:2007:SDM**

[970] John Arhin. On the structure of 1-designs with at most two block intersection numbers. *Designs, Codes, and Cryptography*, 43(2–3): 103–114, June 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=43&issue=2&spage=103.

**Ji:2007:CLSa**

[971] Lijun Ji. A construction for large sets of disjoint Kirkman triple systems. *Designs, Codes, and Cryptography*, 43 (2–3):115–122, June 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=43&issue=2&spage=115.

**Cheon:2007:MLS**

[972] E. J. Cheon and T. Maruta. On the minimum length of some linear codes. *Designs, Codes, and Cryptography*, 43 (2–3):123–135, June 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=43&issue=2&spage=123.

**Bras-Amoros:2007:AGC**

[973] Maria Bras-Amorós. Algebraic-geometry codes, one-point codes, and evaluation codes. *Designs, Codes, and Cryptography*, 43(2–3): 137–145, June 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=43&issue=2&spage=137.

**Yildiz:2007:WML**

[974] Bahattin Yildiz. Weights modulo $p^e$ of linear codes over rings. *Designs, Codes, and Cryptography*, 43 (2–3):147–165, June 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=43&issue=2&spage=147.

**Jackson:2007:PAA**

[975] Wen-Ai Jackson and S. Murphy. Projective aspects of the AES inversion. *Designs, Codes, and Cryptography*, 43 (2–3):167–179, June 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=43&issue=2&spage=167.

**Ghinelli:2007:P**

[976] Dina Ghinelli, James Hirschfeld, and Dieter Jungnickel. Preface. *Designs, Codes, and Cryptography*, 44 (1–3):1–2, September 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=44&issue=1&spage=1.

**Thas:2007:USS**

[977] J. A. Thas. The uniqueness of 1-systems of $W_5(q)$ satisfying the BLT-

property, with $q$ odd. *Designs, Codes, and Cryptography*, 44(1–3):3–10, September 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=44&issue=1&spage=3`.

**Cameron:2007:DGG**

[978] P. J. Cameron and A. Rudvalis. A design and a geometry for the group $\mathrm{Fi}_{22}$. *Designs, Codes, and Cryptography*, 44 (1–3):11–14, September 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=44&issue=1&spage=11`.

**Ebert:2007:MPR**

[979] Gary L. Ebert and Keith E. Mellinger. Mixed partitions and related designs. *Designs, Codes, and Cryptography*, 44 (1–3):15–23, September 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=44&issue=1&spage=15`.

**Prince:2007:TPO**

[980] Alan R. Prince. A translation plane of order $19^2$ admitting $\mathrm{SL}(2,5)$, obtained by 12-nest replacement. *Designs, Codes, and Cryptography*, 44(1–3):25–30, September 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=44&issue=1&spage=25`.

**Pasini:2007:CTP**

[981] Antonio Pasini. A characterization of truncated projective geometries as flag-transitive $\mathrm{PG}^*.\mathrm{PG}$-geometries. *Designs, Codes, and Cryptography*, 44(1–3):31–38, September 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=44&issue=1&spage=31`.

**Lunardon:2007:SSF**

[982] Guglielmo Lunardon. Simplectic spreads and finite semifields. *Designs, Codes, and Cryptography*, 44(1–3):39–48, September 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=44&issue=1&spage=39`.

**Weng:2007:PPG**

[983] Guobiao Weng, Weisheng Qiu, Zeying Wang, and Qing Xiang. Pseudo-Paley graphs and skew Hadamard difference sets from presemifields. *Designs, Codes, and Cryptography*, 44(1–3):49–62, September 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=44&issue=1&spage=49`.

**Ball:2007:HKK**

[984] Simeon Ball and Michel Lavrauw. On the Hughes–Kleinfeld and Knuth's semifields two-dimensional over a weak nucleus. *Designs, Codes, and Cryptography*, 44(1–3):63–67,

September 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=44&issue=1&spage=63.

**Biliotti:2007:TPO**

[985] M. Biliotti, V. Jha, N. L. Johnson, and A. Montinaro. Translation planes of order $q^2$ admitting a two-transitive orbit of length $q + 1$ on the line at infinity. *Designs, Codes, and Cryptography*, 44 (1–3):69–86, September 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=44&issue=1&spage=69.

**Dewar:2007:DTP**

[986] Michael Dewar, Lucia Moura, Daniel Panario, Brett Stevens, and Qiang Wang. Division of trinomials by pentanomials and orthogonal arrays. *Designs, Codes, and Cryptography*, 45 (1):1–17, October 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=45&issue=1&spage=1.

**Rodriguez-Henriquez:2007:PIT**

[987] Francisco Rodríguez-Henríquez, Guillermo Morales-Luna, Nazar A. Saqib, and Nareli Cruz-Cortés. Parallel Itoh–Tsujii multiplicative inversion algorithm for a special class of trinomials. *Designs, Codes, and Cryptography*, 45(1):19–37, October 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=45&issue=1&spage=19.

**Ji:2007:CLSb**

[988] Lijun Ji. Constructions for large sets of $L$-intersecting Steiner triple systems. *Designs, Codes, and Cryptography*, 45 (1):39–49, October 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=45&issue=1&spage=39.

**Esmaeili:2007:PPB**

[989] Morteza Esmaeili and Morteza Hivadi. $G$-projectable and $\Lambda$-projectable binary linear block codes. *Designs, Codes, and Cryptography*, 45(1):51–64, October 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=45&issue=1&spage=51.

**Xiong:2007:OCI**

[990] Yu Xiong, Jun Ma, and Hao Shen. On optimal codes with $w$-identifiable parent property. *Designs, Codes, and Cryptography*, 45 (1):65–90, October 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=45&issue=1&spage=65.

**Seuranen:2007:NLB**

[991] Esa Antero Seuranen. New lower bounds for multiple coverings. *Designs, Codes, and Cryptography*, 45

(1):91–94, October 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=45&issue=1&spage=91.

**Barwick:2007:SAL**

[992] Susan G. Barwick and Wen-Ai Jackson. A sequence approach to linear perfect hash families. *Designs, Codes, and Cryptography*, 45(1):95–121, October 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=45&issue=1&spage=95.

**Landjev:2007:WVR**

[993] I. Landjev and L. Storme. A weighted version of a result of Hamada on minihypers and on linear codes meeting the Griesmer bound. *Designs, Codes, and Cryptography*, 45(1):123–138, October 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=45&issue=1&spage=123.

**Zhang:2007:ECP**

[994] Xiande Zhang and Gennian Ge. Existence of $Z$-cyclic 3PDTWh($p$) for prime $p \equiv 1 \pmod 4$. *Designs, Codes, and Cryptography*, 45(1):139–155, October 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=45&issue=1&spage=139.

**Ge:2007:KFH**

[995] Gennian Ge, Rolf Rees, and Nabil Shalaby. Kirkman frames having hole type $h^u m^1$ for small $h$. *Designs, Codes, and Cryptography*, 45(2):157–184, November 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=45&issue=2&spage=157.

**Cao:2007:CGS**

[996] Haitao Cao, Lijun Ji, and Lie Zhu. Constructions for generalized Steiner systems GS$(3, 4, v, 2)$. *Designs, Codes, and Cryptography*, 45(2):185–197, November 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=45&issue=2&spage=185.

**Gutierrez:2007:ISP**

[997] Jaime Gutierrez and Álvar Ibeas. Inferring sequences produced by a linear congruential generator on elliptic curves missing high-order bits. *Designs, Codes, and Cryptography*, 45(2):199–212, November 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=45&issue=2&spage=199.

**Asamov:2007:SAL**

[998] Tsvetan Asamov and Nuh Aydin. A search algorithm for linear codes: progressive dimension growth. *Designs, Codes, and Cryptography*, 45(2):

213–217, November 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=45&issue=2&spage=213.

**Martinez-Moro:2007:RRM**

[999] E. Martínez-Moro and I. F. Rúa. On repeated-root multivariable codes over a finite chain ring. *Designs, Codes, and Cryptography*, 45(2):219–227, November 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=45&issue=2&spage=219.

**Shaw:2007:AF**

[1000] Ron Shaw. The $\psi$-associate $X^{\#}$ of a flat $X$ in PG$(n, 2)$. *Designs, Codes, and Cryptography*, 45(2):229–246, November 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=45&issue=2&spage=229.

**Kim:2007:CMS**

[1001] Jon-Lark Kim and Yoonjin Lee. Construction of MDS self-dual codes over Galois rings. *Designs, Codes, and Cryptography*, 45(2):247–258, November 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=45&issue=2&spage=247.

**Mengyan:2007:NPN**

[1002] Csaba Mengyán. On the number of pairwise non-isomorphic minimal blocking sets in PG$(2, q)$. *Designs, Codes, and Cryptography*, 45(2):259–267, November 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=45&issue=2&spage=259.

**Byrne:2007:ELP**

[1003] Eimear Byrne, Marcus Greferath, and Michael E. O'Sullivan. Errata for "The linear programming bound for codes over finite Frobenius rings". *Designs, Codes, and Cryptography*, 45(2):269–270, November 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=45&issue=2&spage=269. See [955].

**Ebeid:2007:ARI**

[1004] Nevine Maurice Ebeid and M. Anwar Hasan. On $\tau$-adic representations of integers. *Designs, Codes, and Cryptography*, 45(3):271–296, December 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=45&issue=3&spage=271.

**Ling:2007:CBL**

[1005] San Ling and Ferruh Özbudak. Constructions and bounds on linear error-block codes. *Designs,*

*Codes, and Cryptography*, 45(3):297–316, December 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=45&issue=3&spage=297.

**Ko:2007:TGS**

[1006] Ki Hyoung Ko, Jang Won Lee, and Tony Thomas. Towards generating secure keys for braid cryptography. *Designs, Codes, and Cryptography*, 45(3):317–333, December 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=45&issue=3&spage=317.

**Russeva:2007:BSD**

[1007] Radka Russeva and Nikolay Yankov. On binary self-dual codes of lengths 60, 62, 64 and 66 having an automorphism of order 9. *Designs, Codes, and Cryptography*, 45(3):335–346, December 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=45&issue=3&spage=335.

**Stinson:2007:GMF**

[1008] D. R. Stinson. Generalized mix functions and orthogonal equitable rectangles. *Designs, Codes, and Cryptography*, 45(3):347–357, December 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=45&issue=3&spage=347.

**Carvalho:2007:CCT**

[1009] Cícero Carvalho and Takao Kato. Codes from curves with total inflection points. *Designs, Codes, and Cryptography*, 45(3):359–364, December 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=45&issue=3&spage=359.

**Hana:2007:SC**

[1010] Gert Monstad Hana and Trygve Johnsen. Scroll codes. *Designs, Codes, and Cryptography*, 45(3):365–377, December 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=45&issue=3&spage=365.

**Momihara:2007:NSC**

[1011] Koji Momihara. Necessary and sufficient conditions for tight equi-difference conflict-avoiding codes of weight three. *Designs, Codes, and Cryptography*, 45(3):379–390, December 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=45&issue=3&spage=379.

**Wang:2007:NCO**

[1012] Jinhua Wang. A new class of optimal 3-splitting authentication codes. *Designs, Codes, and Cryptography*, 45

(3):391, December 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=45&issue=3&spage=391.

**Wang:2008:EPA**

[1013] Jinhua Wang and Hao Shen. Existence of $(v, K_{1(3)} \cup \{w^*\})$-PBDs and its applications. *Designs, Codes, and Cryptography*, 46(1):1–16, January 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=46&issue=1&spage=1.

**Skachek:2008:PAF**

[1014] Vitaly Skachek and Ron M. Roth. Probabilistic algorithm for finding roots of linearized polynomials. *Designs, Codes, and Cryptography*, 46 (1):17–23, January 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=46&issue=1&spage=17.

**Fack:2008:SWC**

[1015] Veerle Fack, Szabolcs L. Fancsali, L. Storme, Geetrui Van de Voorde, and Joost Winne. Small weight codewords in the codes arising from Desarguesian projective planes. *Designs, Codes, and Cryptography*, 46 (1):25–43, January 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=46&issue=1&spage=25.

**Heden:2008:PAC**

[1016] Olof Heden. On perfect $p$-ary codes of length $p + 1$. *Designs, Codes, and Cryptography*, 46(1):45–56, January 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=46&issue=1&spage=45.

**Meidl:2008:RCL**

[1017] Wilfried Meidl. Reducing the calculation of the linear complexity of $u2^v$-periodic binary sequences to Games–Chan algorithm. *Designs, Codes, and Cryptography*, 46(1):57–65, January 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=46&issue=1&spage=57.

**Zhang:2008:CPS**

[1018] Weiming Zhang and Shiqu Li. A coding problem in steganography. *Designs, Codes, and Cryptography*, 46 (1):67–81, January 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=46&issue=1&spage=67.

**Davis:2008:PNF**

[1019] James A. Davis and Laurent Poinsot. $G$-perfect nonlinear functions. *Designs, Codes, and Cryptography*, 46 (1):83–96, January 2008. CODEN

DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=46&issue=1&spage=83.

**Martirosyan:2008:ECP**

[1020] Sosina Martirosyan and Tran van Trung. Explicit constructions for perfect hash families. *Designs, Codes, and Cryptography*, 46(1):97–112, January 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=46&issue=1&spage=97.

**Ding:2008:CAD**

[1021] Cunsheng Ding and Tao Feng. Codebooks from almost difference sets. *Designs, Codes, and Cryptography*, 46(1):113–126, January 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=46&issue=1&spage=113.

**Johnson:2008:RSP**

[1022] Norman L. Johnson. $m$th-root subgeometry partitions. *Designs, Codes, and Cryptography*, 46(2):127–136, February 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=46&issue=2&spage=127.

**Skoric:2008:STF**

[1023] Boris Skorić, Stefan Katzenbeisser, and Mehmet U. Celik. Symmetric Tardos fingerprinting codes for arbitrary alphabet sizes. *Designs, Codes, and Cryptography*, 46(2):137–166, February 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=46&issue=2&spage=137.

**Abatangelo:2008:ENM**

[1024] Vito Abatangelo and Bambina Larato. Elliptic near-MDS codes over $\mathbf{F}_5$. *Designs, Codes, and Cryptography*, 46(2):167–174, February 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=46&issue=2&spage=167.

**Britz:2008:DSS**

[1025] Thomas Britz and Keisuke Shiromoto. Designs from subcode supports of linear codes. *Designs, Codes, and Cryptography*, 46(2):175–189, February 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=46&issue=2&spage=175.

**Keri:2008:CRE**

[1026] Gerzson Kéri. The covering radius of extreme binary 2-surjective codes. *Designs, Codes, and Cryptography*, 46(2):191–198, February 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=46&issue=2&spage=191.

**Montinaro:2008:RU**

[1027] Alessandro Montinaro. On the Ree Unital. *Designs, Codes, and Cryptography*, 46(2):199–209, February 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=46&issue=2&spage=199`.

**Yin:2008:GBT**

[1028] Jianxing Yin, Jie Yan, and Chengmin Wang. Generalized balanced tournament designs and related codes. *Designs, Codes, and Cryptography*, 46 (2):211–230, February 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=46&issue=2&spage=211`.

**Cossidente:2008:GST**

[1029] Antonio Cossidente, Nicola Durante, Giuseppe Marino, Tim Penttila, and Alessandro Siciliano. The geometry of some two-character sets. *Designs, Codes, and Cryptography*, 46 (2):231–241, February 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=46&issue=2&spage=231`.

**Potechin:2008:MC**

[1030] Aaron Potechin. Maximal caps in AG$(6, 3)$. *Designs, Codes, and Cryptography*, 46(3):243–259, March 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=46&issue=3&spage=243`.

**Donati:2008:ITS**

[1031] Giorgio Donati and Nicola Durante. On the intersection of two subgeometries of PG$(n, q)$. *Designs, Codes, and Cryptography*, 46(3):261–267, March 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=46&issue=3&spage=261`.

**Bierbrauer:2008:CB**

[1032] Jürgen Bierbrauer and Gohar M. Kyureghyan. Crooked binomials. *Designs, Codes, and Cryptography*, 46 (3):269–301, March 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=46&issue=3&spage=269`.

**Cuaresma:2008:HFJ**

[1033] Maria Cristeta Cuaresma, Michael Giudici, and Cheryl E. Praeger. Homogeneous factorisations of Johnson graphs. *Designs, Codes, and Cryptography*, 46(3):303–327, March 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=46&issue=3&spage=303`.

**Ustaoglu:2008:OSE**

[1034] Berkant Ustaoglu. Obtaining a secure and efficient key agreement proto-

col from (H)MQV and NAXOS. *Designs, Codes, and Cryptography*, 46 (3):329–342, March 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=46&issue=3&spage=329.

**Holzmann:2008:WMO**

[1035] W. H. Holzmann, H. Kharaghani, and B. Tayfeh-Rezaie. Williamson matrices up to order 59. *Designs, Codes, and Cryptography*, 46(3):343–352, March 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=46&issue=3&spage=343.

**Kolokotronis:2008:CPN**

[1036] Nicholas Kolokotronis. Cryptographic properties of nonlinear pseudorandom number generators. *Designs, Codes, and Cryptography*, 46(3):353–363, March 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=46&issue=3&spage=353.

**Polhill:2008:NNL**

[1037] John Polhill. New negative Latin square type partial difference sets in nonelementary abelian 2-groups and 3-groups. *Designs, Codes, and Cryptography*, 46(3):365–377, March 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=46&issue=3&spage=365.

**Blokhuis:2008:FG**

[1038] A. Blokhuis, J. W. P. Hirschfeld, D. Jungnickel, and J. A. Thas. Finite geometries. *Designs, Codes, and Cryptography*, 47(1–3):1–2, June 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=47&issue=1&spage=1.

**DeWinter:2008:NIS**

[1039] S. De Winter. Non-isomorphic semipartial geometries. *Designs, Codes, and Cryptography*, 47(1–3):3–9, June 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=47&issue=1&spage=3.

**Blunck:2008:DDT**

[1040] Andrea Blunck, Hans Havlicek, and Corrado Zanella. Divisible designs from twisted dual numbers. *Designs, Codes, and Cryptography*, 47 (1–3):11–20, June 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=47&issue=1&spage=11.

**DeBeule:2008:POP**

[1041] J. De Beule, A. Klein, K. Metsch, and L. Storme. Partial ovoids and partial spreads in Hermitian polar spaces. *Designs, Codes, and Cryptography*, 47(1–3):21–34, June 2008. CODEN

DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=47&issue=1&spage=21.

**Cooperstein:2008:CPH**

[1042] B. N. Cooperstein and B. De Bruyn. The combinatorial properties of the hyperplanes of $\mathrm{DW}(5, q)$ arising from embedding. *Designs, Codes, and Cryptography*, 47(1–3): 35–51, June 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=47&issue=1&spage=35.

**DeWispelaere:2008:RPW**

[1043] A. De Wispelaere and H. Van Maldeghem. Regular partitions of (weak) finite generalized polygons. *Designs, Codes, and Cryptography*, 47 (1–3):53–73, June 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=47&issue=1&spage=53.

**Coolsaet:2008:DER**

[1044] Kris Coolsaet. A 51-dimensional embedding of the Ree–Tits generalized octagon. *Designs, Codes, and Cryptography*, 47(1–3):75–97, June 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=47&issue=1&spage=75.

**Praeger:2008:CLT**

[1045] Cheryl E. Praeger and Shenglin Zhou. Classification of line-transitive point-imprimitive linear spaces with line size at most 12. *Designs, Codes, and Cryptography*, 47(1–3): 99–111, June 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=47&issue=1&spage=99.

**Alderson:2008:CSI**

[1046] T. L. Alderson and A. A. Bruen. Coprimitive sets and inextendable codes. *Designs, Codes, and Cryptography*, 47 (1–3):113–124, June 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=47&issue=1&spage=113.

**Edel:2008:SAG**

[1047] Yves Edel. Sequences in abelian groups $G$ of odd order without zero-sum subsequences of length $\exp(G)$. *Designs, Codes, and Cryptography*, 47 (1–3):125–134, June 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=47&issue=1&spage=125.

**Byrne:2008:RGT**

[1048] Eimear Byrne, Marcus Greferath, and Thomas Honold. Ring geometries, two-weight codes, and strongly regular graphs. *Designs, Codes, and Cryptography*, 48(1):1–16, July 2008. CODEN

DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=48&issue=1&spage=1.

**Deng:2008:ENK**

[1049] Dameng Deng, Rolf Rees, and Hao Shen. On the existence of nearly Kirkman triple systems with subsystems. *Designs, Codes, and Cryptography*, 48(1):17–33, July 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=48&issue=1&spage=17.

**Yuan:2008:ACL**

[1050] Landang Yuan and Qingde Kang. Another construction for large sets of Kirkman triple systems. *Designs, Codes, and Cryptography*, 48(1):35–42, July 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=48&issue=1&spage=35.

**Han:2008:SDC**

[1051] Sunghyu Han and Jon-Lark Kim. On self-dual codes over $\mathbf{F}_5$. *Designs, Codes, and Cryptography*, 48(1):43–58, July 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=48&issue=1&spage=43.

**Ji:2008:IQC**

[1052] L. Ji. 2-idempotent 3-quasigroups with a conjugate invariant subgroup consisting of a single cycle of length four. *Designs, Codes, and Cryptography*, 48(1):59–68, July 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=48&issue=1&spage=59.

**Blinco:2008:VSP**

[1053] A. D. Blinco, S. I. El-Zanati, G. F. Seelinger, P. A. Sissokho, L. E. Spence, and C. Vanden Eynden. On vector space partitions and uniformly resolvable designs. *Designs, Codes, and Cryptography*, 48(1):69–77, July 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=48&issue=1&spage=69.

**Blayer:2008:IVT**

[1054] Oded Blayer and Tamir Tassa. Improved versions of Tardos' fingerprinting scheme. *Designs, Codes, and Cryptography*, 48(1):79–103, July 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=48&issue=1&spage=79.

**Thas:2008:NET**

[1055] Koen Thas. Note on the existence of translation nets. *Designs, Codes, and Cryptography*, 48(1):105–107, July 2008. CODEN

DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=48&issue=1&spage=105.

**Ding:2008:P**

[1056] Cunsheng Ding, Tor Helleseth, and Øyvind Ytrehus. Preface. *Designs, Codes, and Cryptography*, 48 (2):109–110, August 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=48&issue=2&spage=109.

**Liu:2008:RGH**

[1057] Zihui Liu, Wende Chen, and Yuan Luo. The relative generalized Hamming weight of linear $q$-ary codes and their subcodes. *Designs, Codes, and Cryptography*, 48(2):111–123, August 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=48&issue=2&spage=111.

**Xia:2008:UEP**

[1058] Shu-Tao Xia and Fang-Wei Fu. Undetected error probability of $q$-ary constant weight codes. *Designs, Codes, and Cryptography*, 48(2):125–140, August 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=48&issue=2&spage=125.

**Ouahada:2008:BPS**

[1059] Khmaies Ouahada, Theo G. Swart, Hendrik C. Ferreira, and Ling Cheng. Binary permutation sequences as subsets of Levenshtein codes, spectral null codes, run-length limited codes and constant weight codes. *Designs, Codes, and Cryptography*, 48 (2):141–154, August 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=48&issue=2&spage=141.

**Yorgova:2008:BSD**

[1060] Radinka Yorgova and Alfred Wassermann. Binary self-dual codes with automorphisms of order 23. *Designs, Codes, and Cryptography*, 48 (2):155–164, August 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=48&issue=2&spage=155.

**Keri:2008:MSB**

[1061] Gerzson Kéri and Patric R. J. Östergård. On the minimum size of binary codes with length $2R + 4$ and covering radius $R$. *Designs, Codes, and Cryptography*, 48(2):165–169, August 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=48&issue=2&spage=165.

**Gabidulin:2008:ACA**

[1062] Ernst M. Gabidulin. Attacks and counter-attacks on the GPT pub-

lic key cryptosystem. *Designs, Codes, and Cryptography*, 48(2):171–177, August 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=48&issue=2&spage=171`.

**Riera:2008:GST**

[1063] Constanza Riera, Stéphane Jacob, and Matthew G. Parker. From graph states to two-graph states. *Designs, Codes, and Cryptography*, 48 (2):179–206, August 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=48&issue=2&spage=179`.

**vanZanten:2008:SDS**

[1064] A. J. van Zanten and Loeky Haryanto. Sets of disjoint snakes based on a Reed–Muller code and covering the hypercube. *Designs, Codes, and Cryptography*, 48(3):207–229, September 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=48&issue=3&spage=207`.

**Lavrauw:2008:CGI**

[1065] Michel Lavrauw, Leo Storme, and Geertrui Van de Voorde. On the code generated by the incidence matrix of points and hyperplanes in $\mathrm{PG}(n, q)$ and its dual. *Designs, Codes, and Cryptography*, 48(3):231–245, September 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=48&issue=3&spage=231`.

**Hyun:2008:MDS**

[1066] Jong Yoon Hyun and Hyun Kwang Kim. Maximum distance separable poset codes. *Designs, Codes, and Cryptography*, 48(3):247–261, September 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=48&issue=3&spage=247`.

**Prince:2008:FTP**

[1067] Alan R. Prince. Further translation planes of order $19^2$ admitting $\mathrm{SL}(2, 5)$, obtained by nest replacement. *Designs, Codes, and Cryptography*, 48(3): 263–267, September 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=48&issue=3&spage=263`.

**Klein:2008:ARS**

[1068] Andreas Klein. Attacks on the RC4 stream cipher. *Designs, Codes, and Cryptography*, 48(3):269–286, September 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=48&issue=3&spage=269`.

**deVries:2008:ORC**

[1069] Hans Ludwig de Vries. On orthogonal resolutions of the classical

Steiner quadruple system SQS(16). *Designs, Codes, and Cryptography*, 48(3): 287–292, September 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=48&issue=3&spage=287`.

**Gong:2008:SIA**

[1070] Zheng Gong, Xuejia Lai, and Kefei Chen. A synthetic indifferentiability analysis of some block-cipher-based hash functions. *Designs, Codes, and Cryptography*, 48(3): 293–305, September 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=48&issue=3&spage=293`.

**Dempwolff:2008:DSD**

[1071] Ulrich Dempwolff and William M. Kantor. Distorting symmetric designs. *Designs, Codes, and Cryptography*, 48(3): 307–322, September 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=48&issue=3&spage=307`.

**Geil:2008:SWG**

[1072] Olav Geil. On the second weight of generalized Reed–Muller codes. *Designs, Codes, and Cryptography*, 48(3): 323–330, September 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=48&issue=3&spage=323`. See erratum [1707].

**Wang:2008:SCC**

[1073] Jianmin Wang. Some combinatorial constructions for optimal perfect deletion-correcting codes. *Designs, Codes, and Cryptography*, 48(3): 331–347, September 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=48&issue=3&spage=331`.

**Charpin:2008:EMH**

[1074] Pascale Charpin and Tor Helleseth. Editorial: In memory of Hans Dobbertin. *Designs, Codes, and Cryptography*, 49 (1–3):1–2, December 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=49&issue=1&spage=1`.

**Dobbertin:2008:BFE**

[1075] Hans Dobbertin and Gregor Leander. Bent functions embedded into the recursive framework of **Z**-bent functions. *Designs, Codes, and Cryptography*, 49 (1–3):3–22, December 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=49&issue=1&spage=3`.

**Dillon:2008:MDD**

[1076] J. F. Dillon. More DD difference sets. *Designs, Codes, and Cryptography*, 49 (1–3):23–32, December 2008. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=49&issue=1&spage=23.

**Niederreiter:2008:PML**

[1077] Harald Niederreiter and Ayineedi Venkateswarlu. Periodic multisequences with large error linear complexity. *Designs, Codes, and Cryptography*, 49(1–3):33–45, December 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=49&issue=1&spage=33.

**Semaev:2008:SSA**

[1078] Igor Semaev. On solving sparse algebraic equations over finite fields. *Designs, Codes, and Cryptography*, 49(1–3):47–60, December 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=49&issue=1&spage=47.

**Ozbudak:2008:SAC**

[1079] Ferruh Özbudak and Zülfükar Saygi. Systematic authentication codes using additive polynomials. *Designs, Codes, and Cryptography*, 49(1–3):61–77, December 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=49&issue=1&spage=61.

**Horadam:2008:BPN**

[1080] K. J. Horadam and D. G. Farmer. Bundles, presemifields and nonlinear functions. *Designs, Codes, and Cryptography*, 49(1–3):79–94, December 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=49&issue=1&spage=79.

**Sarkar:2008:INP**

[1081] Sumanta Sarkar and Subhamoy Maitra. Idempotents in the neighbourhood of Patterson–Wiedemann functions having Walsh spectra zeros. *Designs, Codes, and Cryptography*, 49(1–3):95–103, December 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=49&issue=1&spage=95.

**Gabidulin:2008:EEC**

[1082] Ernst M. Gabidulin and Nina I. Pilipchuk. Error and erasure correcting algorithms for rank codes. *Designs, Codes, and Cryptography*, 49(1–3):105–122, December 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=49&issue=1&spage=105.

**Paul:2008:NNB**

[1083] Goutam Paul, Siddheshwar Rathi, and Subhamoy Maitra. On non-negligible bias of the first output byte of RC4 towards the first three

bytes of the secret key. *Designs, Codes, and Cryptography*, 49(1–3): 123–134, December 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=49&issue=1&spage=123.

**Kim:2008:SHD**

[1084] Jon-Lark Kim and Patrick Solé. Skew Hadamard designs and their codes. *Designs, Codes, and Cryptography*, 49(1–3):135–145, December 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=49&issue=1&spage=135.

**Raddum:2008:SMR**

[1085] Håvard Raddum and Igor Semaev. Solving Multiple Right Hand Sides linear equations. *Designs, Codes, and Cryptography*, 49(1–3):147–160, December 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=49&issue=1&spage=147.

**Danielsen:2008:ELC**

[1086] Lars Eirik Danielsen and Matthew G. Parker. Edge local complementation and equivalence of binary linear codes. *Designs, Codes, and Cryptography*, 49(1–3):161–170, December 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=49&issue=1&spage=161.

**Farashahi:2008:EBE**

[1087] Reza Rezaeian Farashahi, Ruud Pellikaan, and Andrey Sidorenko. Extractors for binary elliptic curves. *Designs, Codes, and Cryptography*, 49(1–3):171–186, December 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=49&issue=1&spage=171.

**DeBeule:2008:CRA**

[1088] J. De Beule, K. Metsch, and L. Storme. Characterization results on arbitrary non-weighted minihypers and on linear codes meeting the Griesmer bound. *Designs, Codes, and Cryptography*, 49(1–3):187–197, December 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=49&issue=1&spage=187.

**Christopoulou:2008:TON**

[1089] Maria Christopoulou, Theo Garefalakis, Daniel Panario, and David Thomson. The trace of an optimal normal element and low complexity normal bases. *Designs, Codes, and Cryptography*, 49(1–3): 199–215, December 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=49&issue=1&spage=199.

**Czapski:2008:EDE**

[1090] Mariusz Czapski and Maciej Nikodem. Error detection and error correction procedures for the Advanced Encryption Standard. *Designs, Codes, and Cryptography*, 49(1–3):217–232, December 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=49&issue=1&spage=217`.

**Qian:2008:EPK**

[1091] Haifeng Qian, Yuan Zhou, Zhibin Li, Zecheng Wang, and Bing Zhang. Efficient public key encryption with smallest ciphertext expansion from factoring. *Designs, Codes, and Cryptography*, 49(1–3):233–249, December 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=49&issue=1&spage=233`.

**Petrides:2008:CRN**

[1092] George Petrides and Johannes Mykkeltveit. Composition of recursions and nonlinear complexity of periodic binary sequences. *Designs, Codes, and Cryptography*, 49(1–3):251–264, December 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=49&issue=1&spage=251`.

**Danev:2008:FTQ**

[1093] Danyo Danev and Stefan Dodunekov. A family of ternary quasi-perfect BCH codes. *Designs, Codes, and Cryptography*, 49(1–3):265–271, December 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=49&issue=1&spage=265`.

**Brinkmann:2008:CAF**

[1094] Marcus Brinkmann and Gregor Leander. On the classification of APN functions up to dimension five. *Designs, Codes, and Cryptography*, 49(1–3):273–288, December 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=49&issue=1&spage=273`.

**Nojima:2008:SSM**

[1095] Ryo Nojima, Hideki Imai, Kazukuni Kobara, and Kirill Morozov. Semantic security for the McEliece cryptosystem without random oracles. *Designs, Codes, and Cryptography*, 49(1–3):289–305, December 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=49&issue=1&spage=289`.

**Siqueira:2008:FTL**

[1096] Rogério M. Siqueira and Sueli I. R. Costa. Flat tori, lattices and bounds for commutative group codes. *Designs, Codes, and Cryptography*, 49(1–3):307–321, December 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.`

asp?genre=article&issn=0925-1022&volume=49&issue=1&spage=307.

**Fourquet:2008:ILD**

[1097] Rafaël Fourquet and Cédric Tavernier. An improved list decoding algorithm for the second order Reed–Muller codes and its applications. *Designs, Codes, and Cryptography*, 49(1–3): 323–340, December 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=49&issue=1&spage=323.

**Bey:2008:BFS**

[1098] Christian Bey and Gohar M. Kyureghyan. On Boolean functions with the sum of every two of them being bent. *Designs, Codes, and Cryptography*, 49(1–3):341–346, December 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=49&issue=1&spage=341.

**Garaschuk:2008:BKS**

[1099] Kseniya Garaschuk and Petr Lisonek. On binary Kloosterman sums divisible by 3. *Designs, Codes, and Cryptography*, 49(1–3):347–357, December 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=49&issue=1&spage=347.

**Homma:2009:SGH**

[1100] Masaaki Homma and Seon Jeong Kim. The second generalized Hamming weight for two-point codes on a Hermitian curve. *Designs, Codes, and Cryptography*, 50(1):1–40, January 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=50&issue=1&spage=1.

**Schillewaert:2009:CHV**

[1101] J. Schillewaert and J. A. Thas. Characterizations of Hermitian varieties by intersection numbers. *Designs, Codes, and Cryptography*, 50(1):41–60, January 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=50&issue=1&spage=41.

**Yan:2009:COC**

[1102] Jie Yan and Jianxing Yin. A class of optimal constant composition codes from GDRPs. *Designs, Codes, and Cryptography*, 50(1):61–76, January 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=50&issue=1&spage=61.

**Dougherty:2009:MCF**

[1103] Steven T. Dougherty, Jon-Lark Kim, and Hamid Kulosman. MDS codes over finite principal ideal rings. *Designs, Codes, and Cryptography*, 50 (1):77–92, January 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.

asp?genre=article&issn=0925-1022&volume=50&issue=1&spage=77.

**Weng:2009:SRS**

[1104] Guobiao Weng and Lei Hu. Some results on skew Hadamard difference sets. *Designs, Codes, and Cryptography*, 50 (1):93–105, January 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=50&issue=1&spage=93.

**Guo:2009:EGM**

[1105] Weidong Guo and Gennian Ge. The existence of generalized mix functions. *Designs, Codes, and Cryptography*, 50 (1):107–113, January 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=50&issue=1&spage=107.

**Coron:2009:VBF**

[1106] Jean-Sébastien Coron. A variant of Boneh–Franklin IBE with a tight reduction in the random oracle model. *Designs, Codes, and Cryptography*, 50 (1):115–133, January 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=50&issue=1&spage=115.

**Edoukou:2009:CDF**

[1107] Frédéric A. B. Edoukou. Codes defined by forms of degree 2 on non-degenerate Hermitian varieties in $\mathbf{P}^4(\mathbf{F}_q)\mathbf{P}^4(\mathbf{F}_q)$. *Designs, Codes, and Cryptography*, 50 (1):135–146, January 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=50&issue=1&spage=135.

**Park:2009:MIG**

[1108] Young Ho Park. Modular independence and generator matrices for codes over $\mathbf{Z}_m$. *Designs, Codes, and Cryptography*, 50(2):147–162, February 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=50&issue=2&spage=147.

**Xia:2009:JTB**

[1109] Shu-Tao Xia and Fang-Wei Fu. Johnson type bounds on constant dimension codes. *Designs, Codes, and Cryptography*, 50(2):163–172, February 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=50&issue=2&spage=163.

**Hyun:2009:GMI**

[1110] Jong Yoon Hyun. Generalized MacWilliams identities and their applications to perfect binary codes. *Designs, Codes, and Cryptography*, 50 (2):173–185, February 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=50&issue=2&spage=173.

**DeBeule:2009:TSW**

[1111] Jan De Beule, Patrick Govaerts, Anja Hallez, and Leo Storme. Tight sets, weighted $m$-covers, weighted $m$-ovoids, and minihypers. *Designs, Codes, and Cryptography*, 50(2):187–201, February 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=50&issue=2&spage=187`.

**Fu:2009:SOG**

[1112] Wenqing Fu and Tao Feng. On self-orthogonal group ring codes. *Designs, Codes, and Cryptography*, 50 (2):203–214, February 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=50&issue=2&spage=203`.

**Liu:2009:APV**

[1113] Feng Liu, Chuan Kun Wu, and Xi Jun Lin. The alignment problem of visual cryptography schemes. *Designs, Codes, and Cryptography*, 50(2):215–227, February 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=50&issue=2&spage=215`.

**Trinker:2009:SDM**

[1114] Horst Trinker. A simple derivation of the MacWilliams identity for linear ordered codes and orthogonal arrays. *Designs, Codes, and Cryptography*, 50 (2):229–234, February 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=50&issue=2&spage=229`.

**Bierbrauer:2009:FCF**

[1115] Jürgen Bierbrauer. A family of crooked functions. *Designs, Codes, and Cryptography*, 50(2):235–241, February 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=50&issue=2&spage=235`.

**Feng:2009:MVG**

[1116] Keqin Feng, Qunying Liao, and Jing Yang. Maximal values of generalized algebraic immunity. *Designs, Codes, and Cryptography*, 50(2):243–252, February 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=50&issue=2&spage=243`.

**Huang:2009:USC**

[1117] Yiwei Huang and Bernhard Schmidt. Uniqueness of some cyclic projective planes. *Designs, Codes, and Cryptography*, 50(2):253–266, February 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=50&issue=2&spage=253`.

**Chaussade:2009:SCP**

[1118] Lionel Chaussade, Pierre Loidreau, and Felix Ulmer. Skew codes of prescribed distance or rank. *Designs, Codes, and Cryptography*, 50 (3):267–284, March 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=50&issue=3&spage=267`.

**Hiramine:2009:TOM**

[1119] Yutaka Hiramine. A two-to-one map and abelian affine difference sets. *Designs, Codes, and Cryptography*, 50 (3):285–290, March 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=50&issue=3&spage=285`.

**Nagata:2009:NSD**

[1120] Kiyoshi Nagata, Fidel Nemenzo, and Hideo Wada. The number of self-dual codes over $Z_{p^3}$. *Designs, Codes, and Cryptography*, 50(3):291–303, March 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=50&issue=3&spage=291`.

**Galbraith:2009:CPU**

[1121] Steven D. Galbraith and Xibin Lin. Computing pairings using $x$-coordinates only. *Designs, Codes, and Cryptography*, 50(3):305–324, March 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=50&issue=3&spage=305`.

**Piret:2009:PSB**

[1122] Gilles Piret and François-Xavier Standaert. Provable security of block ciphers against linear cryptanalysis: a mission impossible? An experimental review of the practical security approach and the key equivalence hypothesis in linear cryptanalysis. *Designs, Codes, and Cryptography*, 50 (3):325–338, March 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=50&issue=3&spage=325`.

**Li:2009:CAS**

[1123] Yang Li, Lijun Ji, and Jianxing Yin. Covering arrays of strength 3 and 4 from holey difference matrices. *Designs, Codes, and Cryptography*, 50 (3):339–350, March 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=50&issue=3&spage=339`.

**Panario:2009:ERC**

[1124] D. Panario and D. Thomson. Efficient $p$th root computations in finite fields of characteristic $p$. *Designs, Codes, and Cryptography*, 50 (3):351–358, March 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.`

asp?genre=article&issn=0925-1022&volume=50&issue=3&spage=351.

**Davydov:2009:CCS**

[1125] Alexander A. Davydov, Stefano Marcugini, and Fernanda Pambianco. Complete $(q^2 + q + 8)/2$-caps in the spaces $PG(3, q), q \equiv 2(mod 3)$ an odd prime, and a complete 20-cap in $PG(3, 5)$. *Designs, Codes, and Cryptography*, 50(3):359–372, March 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=50&issue=3&spage=359.

**Tian:2009:NCM**

[1126] Tian Tian and Wen-Feng Qi. A note on the crosscorrelation of maximal length FCSR sequences. *Designs, Codes, and Cryptography*, 51 (1):1–8, April 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=51&issue=1&spage=1.

**Cheon:2009:COL**

[1127] E. J. Cheon. A class of optimal linear codes of length one above the Griesmer bound. *Designs, Codes, and Cryptography*, 51(1):9–20, April 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=51&issue=1&spage=9.

**Lyubich:2009:TPD**

[1128] Yu. I. Lyubich. On tight projective designs. *Designs, Codes, and Cryptography*, 51(1):21–31, April 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=51&issue=1&spage=21.

**Meidl:2009:RCS**

[1129] Wilfried Meidl. Remarks on a cyclotomic sequence. *Designs, Codes, and Cryptography*, 51(1):33–43, April 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=51&issue=1&spage=33.

**Petelczyc:2009:CPR**

[1130] Krzysztof Petelczyc and Małgorzata Prazmowska. 103-configurations and projective realizability of multiplied configurations. *Designs, Codes, and Cryptography*, 51(1):45–54, April 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=51&issue=1&spage=45.

**Dougherty:2009:IVC**

[1131] Steven T. Dougherty and Hongwei Liu. Independence of vectors in codes over rings. *Designs, Codes, and Cryptography*, 51(1):55–68, April 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.

asp?genre=article&issn=0925-1022&volume=51&issue=1&spage=55.

**Han:2009:NNE**

[1132] Sunghyu Han and Jon-Lark Kim. The nonexistence of near-extremal formally self-dual codes. *Designs, Codes, and Cryptography*, 51(1):69–77, April 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=51&issue=1&spage=69.

**Abel:2009:E**

[1133] R. Julian R. Abel, Norman J. Finizio, Malcolm Greig, and Luis B. Morales. Existence of $(2,8)$GWhD($v$) and $(4,8)$GWhD($v$) with $v \equiv 0,1 \pmod 8$. *Designs, Codes, and Cryptography*, 51(1):79–97, April 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=51&issue=1&spage=79.

**Poulakis:2009:VDS**

[1134] Dimitrios Poulakis. A variant of Digital Signature Algorithm. *Designs, Codes, and Cryptography*, 51(1):99–104, April 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=51&issue=1&spage=99. See erratum [1293].

**Bouyukliev:2009:DAO**

[1135] Iliya Bouyukliev, Veerle Fack, and Joost Winne. $2-(31,15,7)$, $2-(35,17,8)$ and $2-(36,15,6)$ designs with automorphisms of odd prime order, and their related Hadamard matrices and codes. *Designs, Codes, and Cryptography*, 51(2):105–122, May 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=51&issue=2&spage=105.

**Cossidente:2009:SCH**

[1136] Antonio Cossidente. Some constructions on the Hermitian surface. *Designs, Codes, and Cryptography*, 51(2):123–129, May 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=51&issue=2&spage=123.

**Jungnickel:2009:PQS**

[1137] Dieter Jungnickel and Vladimir D. Tonchev. Polarities, quasi-symmetric designs, and Hamada's conjecture. *Designs, Codes, and Cryptography*, 51(2):131–140, May 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=51&issue=2&spage=131.

**Shaw:2009:CSV**

[1138] Ron Shaw and Neil A. Gordon. The cubic Segre variety in PG$(5,2)$. *Designs, Codes, and Cryptography*, 51(2):141–156, May 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.

asp?genre=article&issn=0925-1022&volume=51&issue=2&spage=141.

**Bamberg:2009:HNG**

[1139] John Bamberg, Frank De Clerck, and Nicola Durante. A hemisystem of a nonclassical generalised quadrangle. *Designs, Codes, and Cryptography*, 51(2):157–165, May 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=51&issue=2&spage=157.

**Collins:2009:UBP**

[1140] Michael J. Collins. Upper bounds for parent-identifying set systems. *Designs, Codes, and Cryptography*, 51 (2):167–173, May 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=51&issue=2&spage=167.

**Feng:2009:DSN**

[1141] Tao Feng. Difference sets with $n = 5p^r$. *Designs, Codes, and Cryptography*, 51(2):175–194, May 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=51&issue=2&spage=175.

**Lee:2009:ERA**

[1142] Jooyoung Lee and Yongjin Yeom. Efficient RFID authentication protocols based on pseudorandom sequence generators. *Designs, Codes, and Cryptography*, 51(2):195–210, May 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=51&issue=2&spage=195.

**Darafsheh:2009:SDC**

[1143] M. R. Darafsheh, A. Iranmanesh, and R. Kahkeshani. Some designs and codes invariant under the groups $S_9$ and $A_8$. *Designs, Codes, and Cryptography*, 51(2):211–223, May 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=51&issue=2&spage=211.

**Cao:2009:OGE**

[1144] H. Cao, J. Dinitz, D. Kreher, D. R. Stinson, and R. Wei. On orthogonal generalized equitable rectangles. *Designs, Codes, and Cryptography*, 51(3):225–230, June 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=51&issue=3&spage=225.

**Smith:2009:GCH**

[1145] Derek H. Smith, Richard P. Ward, and Stephanie Perkins. Gold codes, Hadamard partitions and the security of CDMA systems. *Designs, Codes, and Cryptography*, 51(3):231–243, June 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=51&issue=3&spage=231.

**Adams:2009:MMH**

[1146] Sarah Spence Adams, Matthew Crawford, Caitlin Greeley, Bryce Lee, and Mathav Kishore Murugan. Multilevel and multidimensional Hadamard matrices. *Designs, Codes, and Cryptography*, 51 (3):245–252, June 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=51&issue=3&spage=245`.

**Momihara:2009:SDF**

[1147] Koji Momihara. Strong difference families, difference covers, and their applications for relative difference families. *Designs, Codes, and Cryptography*, 51(3):253–273, June 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=51&issue=3&spage=253`.

**Boumova:2009:PTI**

[1148] Silvia Boumova, Peter Boyvalenkov, Hristina Kulina, and Maya Stoyanova. Polynomial techniques for investigation of spherical designs. *Designs, Codes, and Cryptography*, 51 (3):275–288, June 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=51&issue=3&spage=275`.

**Bernal:2009:IDG**

[1149] José Joaquín Bernal, Ángel del Río, and Juan Jacobo Simón. An intrinsical description of group codes. *Designs, Codes, and Cryptography*, 51 (3):289–300, June 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=51&issue=3&spage=289`.

**Burkhart:2009:FFE**

[1150] Jessica F. Burkhart, Neil J. Calkin, Shuhong Gao, Justine C. Hyde-Volpe, Kevin James, et al. Finite field elements of high order arising from modular curves. *Designs, Codes, and Cryptography*, 51 (3):301–314, June 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=51&issue=3&spage=301`.

**Martin:2009:EBE**

[1151] Thomas Martin, Keith M. Martin, and Peter Wild. Establishing the broadcast efficiency of the Subset Difference Revocation Scheme. *Designs, Codes, and Cryptography*, 51 (3):315–334, June 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=51&issue=3&spage=315`.

**Marti-Farre:2009:ISS**

[1152] Jaume Martí-Farré and Carles Padró. Ideal secret sharing schemes whose minimal qualified subsets have at most three participants. *Designs, Codes, and Cryptography*, 52(1):1–14, July 2009. CODEN DC-

CREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=52&issue=1&spage=1.

**Harn:2009:DIC**

[1153] Lein Harn and Changlu Lin. Detection and identification of cheaters in $(t, n)$ secret sharing scheme. *Designs, Codes, and Cryptography*, 52 (1):15–24, July 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=52&issue=1&spage=15.

**Colbourn:2009:LHF**

[1154] Charles J. Colbourn and Alan C. H. Ling. Linear hash families and forbidden configurations. *Designs, Codes, and Cryptography*, 52(1): 25–55, July 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=52&issue=1&spage=25.

**Grassl:2009:CSD**

[1155] Markus Grassl and T. Aaron Gulliver. On circulant self-dual codes over small fields. *Designs, Codes, and Cryptography*, 52(1):57–81, July 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=52&issue=1&spage=57.

**Liu:2009:GMT**

[1156] Yu-Ru Liu and Craig V. Spencer. A generalization of Meshulam's theorem on subsets of finite abelian groups with no 3-term arithmetic progression. *Designs, Codes, and Cryptography*, 52(1):83–91, July 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=52&issue=1&spage=83.

**Bryant:2009:IPL**

[1157] Darryn Bryant, Judith Egan, Barbara Maenhaut, and Ian M. Wanless. Indivisible plexes in latin squares. *Designs, Codes, and Cryptography*, 52(1):93–105, July 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=52&issue=1&spage=93.

**Wen:2009:OGH**

[1158] Bin Wen, Jianmin Wang, and Jianxing Yin. Optimal grid holey packings with block size 3 and 4. *Designs, Codes, and Cryptography*, 52 (1):107–124, July 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=52&issue=1&spage=107.

**Harada:2009:TEN**

[1159] Masaaki Harada and Akihiro Munemasa. There exists no self-dual $[24, 12, 10]$ code over $\mathbf{F}_5$. *Designs, Codes, and Cryptography*, 52(1):125–

127, July 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=52&issue=1&spage=125.

**Tassa:2009:PSB**

[1160] Tamir Tassa and Jorge L. Villar. On proper secrets, $(t, k)$-bases and linear codes. *Designs, Codes, and Cryptography*, 52(2):129–154, August 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=52&issue=2&spage=129.

**AlBdaiwi:2009:EDP**

[1161] Bader AlBdaiwi, Peter Horak, and Lorenzo Milazzo. Enumerating and decoding perfect linear Lee codes. *Designs, Codes, and Cryptography*, 52 (2):155–162, August 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=52&issue=2&spage=155.

**Polhill:2009:PTP**

[1162] John Polhill. Paley type partial difference sets in non $p$-groups. *Designs, Codes, and Cryptography*, 52 (2):163–169, August 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=52&issue=2&spage=163.

**Cheon:2009:NET**

[1163] E. J. Cheon and T. Maruta. A new extension theorem for 3-weight modulo $q$ linear codes over $\mathbf{F}_q$. *Designs, Codes, and Cryptography*, 52 (2):171–183, August 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=52&issue=2&spage=171.

**Heuberger:2009:UDS**

[1164] Clemens Heuberger and James A. Muir. Unbalanced digit sets and the closest choice strategy for minimal weight integer representations. *Designs, Codes, and Cryptography*, 52 (2):185–208, August 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=52&issue=2&spage=185.

**Dorbec:2009:WCL**

[1165] Paul Dorbec, Sylvain Gravier, Iiro Honkala, and Michel Mollard. Weighted codes in Lee metrics. *Designs, Codes, and Cryptography*, 52(2):209–218, August 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=52&issue=2&spage=209.

**Paterson:2009:RBN**

[1166] Kenneth G. Paterson and Sriramkrishnan Srinivasan. On the relations between non-interactive key distribution, identity-based encryption and

trapdoor discrete log groups. *Designs, Codes, and Cryptography*, 52 (2):219–241, August 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=52&issue=2&spage=219`.

**Prince:2009:PPP**

[1167] Alan R. Prince. Pure partial planes of order 6 with 25 lines. *Designs, Codes, and Cryptography*, 52(2):243–247, August 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=52&issue=2&spage=243`.

**Tian:2009:LPB**

[1168] Tian Tian and Wen-Feng Qi. Linearity properties of binary FCSR sequences. *Designs, Codes, and Cryptography*, 52 (3):249–262, September 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=52&issue=3&spage=249`.

**Curtin:2009:SAS**

[1169] Brian Curtin and Ibtisam Daqqa. The subconstituent algebra of strongly regular graphs associated with a Latin square. *Designs, Codes, and Cryptography*, 52(3):263–274, September 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=52&issue=3&spage=263`.

**Mishima:2009:OCA**

[1170] Miwako Mishima, Hung-Lin Fu, and Shoichi Uruno. Optimal conflict-avoiding codes of length $n \equiv 0 \pmod 1 6$ and weight 3. *Designs, Codes, and Cryptography*, 52(3):275–291, September 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=52&issue=3&spage=275`.

**Caranti:2009:AOS**

[1171] A. Caranti, Francesca Dalla Volta, and M. Sala. An application of the O'Nan–Scott theorem to the group generated by the round functions of an AES-like cipher. *Designs, Codes, and Cryptography*, 52(3): 293–301, September 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=52&issue=3&spage=293`.

**Carlet:2009:FPS**

[1172] Claude Carlet, Xiangyong Zeng, Chunlei Li, and Lei Hu. Further properties of several classes of Boolean functions with optimum algebraic immunity. *Designs, Codes, and Cryptography*, 52(3): 303–338, September 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=52&issue=3&spage=303`.

**Nuida:2009:IDT**

[1173] Koji Nuida, Satoshi Fujitsu, Manabu Hagiwara, Takashi Kitagawa, Hajime

Watanabe, et al. An improvement of discrete Tardos fingerprinting codes. *Designs, Codes, and Cryptography*, 52 (3):339–362, September 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=52&issue=3&spage=339`.

**Kim:2009:GGP**

[1174] Jon-Lark Kim and Xiaoyu Liu. A generalized Gleason–Pierce–Ward theorem. *Designs, Codes, and Cryptography*, 52(3):363–380, September 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=52&issue=3&spage=363`.

**Moody:2009:DHP**

[1175] Dustin Moody. The Diffie–Hellman problem and generalization of Verheul's theorem. *Designs, Codes, and Cryptography*, 52(3):381–390, September 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=52&issue=3&spage=381`.

**Coulter:2009:SSD**

[1176] Robert S. Coulter and Todd Gutekunst. Special subsets of difference sets with particular emphasis on skew Hadamard difference sets. *Designs, Codes, and Cryptography*, 53(1):1–12, October 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=53&issue=1&spage=1`.

**Roy:2009:UDC**

[1177] Aidan Roy and A. J. Scott. Unitary designs and codes. *Designs, Codes, and Cryptography*, 53(1):13–31, October 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=53&issue=1&spage=13`.

**Yang:2009:IAB**

[1178] Siman Yang and Lulu Qi. On improved asymptotic bounds for codes from global function fields. *Designs, Codes, and Cryptography*, 53 (1):33–43, October 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=53&issue=1&spage=33`.

**Owsiejczuk:2009:CGG**

[1179] Andrzej Owsiejczuk and Małgorzata Prazmowska. Combinatorial generalizations of generalized quadrangles of order $(2, 2)$. *Designs, Codes, and Cryptography*, 53(1):45–57, October 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=53&issue=1&spage=45`.

**Alderson:2009:MLC**

[1180] T. L. Alderson and András Gács. On the maximality of linear codes. *De-*

*signs, Codes, and Cryptography*, 53 (1):59–68, October 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=53&issue=1&spage=59.

**Heden:2009:NSC**

[1181] Olof Heden. Necessary and sufficient conditions for the existence of a class of partitions of a finite vector space. *Designs, Codes, and Cryptography*, 53 (2):69–73, November 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=53&issue=2&spage=69.

**Kavuluru:2009:CPB**

[1182] Ramakanth Kavuluru. Characterization of $2^n$-periodic binary sequences with fixed 2-error or 3-error linear complexity. *Designs, Codes, and Cryptography*, 53(2):75–97, November 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=53&issue=2&spage=75.

**Carvalho:2009:AAC**

[1183] Cícero Carvalho and Ercílio Silva. On algebras admitting a complete set of near weights, evaluation codes, and Goppa codes. *Designs, Codes, and Cryptography*, 53(2):99–110, November 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=53&issue=2&spage=99.

**Bras-Amoros:2009:NSR**

[1184] Maria Bras-Amorós. On numerical semigroups and the redundancy of improved codes correcting generic errors. *Designs, Codes, and Cryptography*, 53 (2):111–118, November 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=53&issue=2&spage=111.

**Ball:2009:MBS**

[1185] Simeon Ball and Szabolcs L. Fancsali. Multiple blocking sets in finite projective spaces and improvements to the Griesmer bound for linear codes. *Designs, Codes, and Cryptography*, 53(2):119–136, November 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=53&issue=2&spage=119.

**Tang:2009:NOQ**

[1186] Xiaohu Tang, Tor Helleseth, and Pingzhi Fan. A new optimal quaternary sequence family of length $2(2^n-1)$ obtained from the orthogonal transformation of Families $\mathcal{B}$ and $\mathcal{C}$. *Designs, Codes, and Cryptography*, 53(3):137–148, December 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=53&issue=3&spage=137.

**Mossinghoff:2009:WPB**

[1187] Michael J. Mossinghoff. Wieferich pairs and Barker sequences. *Designs, Codes, and Cryptography*, 53(3): 149–163, December 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=53&issue=3&spage=149`.

**Fanali:2009:MCF**

[1188] Stefania Fanali and Massimo Giulietti. On maximal curves with Frobenius dimension 3. *Designs, Codes, and Cryptography*, 53(3):165–174, December 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=53&issue=3&spage=165`.

**Pinto:2009:CAS**

[1189] Alexandre Pinto, André Souto, Armando Matos, and Luís Antunes. Commitment and authentication systems. *Designs, Codes, and Cryptography*, 53 (3):175–193, December 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=53&issue=3&spage=175`.

**Csirmaz:2009:IRG**

[1190] László Csirmaz. An impossibility result on graph secret sharing. *Designs, Codes, and Cryptography*, 53(3): 195–209, December 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=53&issue=3&spage=195`.

**Cossidente:2010:CST**

[1191] Antonio Cossidente. The classical 1-system of $Q^-(7,q)$ and two-character sets. *Designs, Codes, and Cryptography*, 54(1):1–9, January 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=54&issue=1&spage=1`.

**Liu:2010:NVF**

[1192] Zihui Liu and Wende Chen. Notes on the value function. *Designs, Codes, and Cryptography*, 54(1):11–19, January 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=54&issue=1&spage=11`.

**Zuo:2010:SCM**

[1193] Guoxin Zuo and Mingyuan Xia. A special class of $T$-matrices. *Designs, Codes, and Cryptography*, 54 (1):21–28, January 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=54&issue=1&spage=21`.

**Levy-dit-Vehel:2010:SAW**

[1194] Françoise Levy dit Vehel and Ludovic Perret. Security analysis of word problem-based cryptosystems. *Designs, Codes, and Cryptography*, 54 (1):29–41, January 2010. CODEN

DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=54&issue=1&spage=29.

**Wang:2010:COT**

[1195] Jianmin Wang, Xiuling Shan, and Jianxing Yin. On constructions for optimal two-dimensional optical orthogonal codes. *Designs, Codes, and Cryptography*, 54(1):43–60, January 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=54&issue=1&spage=43.

**Yildiz:2010:LCM**

[1196] Bahattin Yildiz and Suat Karadeniz. Linear codes over $\mathbf{F}_2 + u\mathbf{F}_2 + v\mathbf{F}_2 + uv\mathbf{F}_2$. *Designs, Codes, and Cryptography*, 54(1):61–81, January 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=54&issue=1&spage=61.

**Farashahi:2010:NDE**

[1197] Reza Rezaeian Farashahi and Igor E. Shparlinski. On the number of distinct elliptic curves in some families. *Designs, Codes, and Cryptography*, 54(1):83–99, January 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=54&issue=1&spage=83.

**El-Zanati:2010:MSP**

[1198] S. El-Zanati, H. Jordon, G. Seelinger, P. Sissokho, and L. Spence. The maximum size of a partial 3-spread in a finite vector space over GF(2). *Designs, Codes, and Cryptography*, 54(2):101–107, February 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=54&issue=2&spage=101.

**Huczynska:2010:EFP**

[1199] Sophie Huczynska. Equidistant frequency permutation arrays and related constant composition codes. *Designs, Codes, and Cryptography*, 54(2):109–120, February 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=54&issue=2&spage=109.

**Ma:2010:EDL**

[1200] Changshe Ma, Jian Weng, Yingjiu Li, and Robert Deng. Efficient discrete logarithm based multi-signature scheme in the plain public key model. *Designs, Codes, and Cryptography*, 54(2):121–133, February 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=54&issue=2&spage=121.

**Landjev:2010:SM**

[1201] Ivan Landjev and Leo Storme. A study of $(x(q+1), x; 2, q)$-minihypers. *Designs, Codes, and Cryptography*, 54

(2):135–147, February 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=54&issue=2&spage=135`.

**Bhaintwal:2010:GRM**

[1202] Maheshanand Bhaintwal and Siri Krishan Wasan. Generalized Reed–Muller codes over $\mathbf{Z}_q$. *Designs, Codes, and Cryptography*, 54(2):149–166, February 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=54&issue=2&spage=149`.

**Borges:2010:LCG**

[1203] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà, and M. Villanueva. $\mathbf{Z}_2\mathbf{Z}_4$-linear codes: generator matrices and duality. *Designs, Codes, and Cryptography*, 54(2):167–179, February 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=54&issue=2&spage=167`.

**Drake:2010:PCB**

[1204] Nathan Drake and Gretchen L. Matthews. Parameter choices and a better bound on the list size in the Guruswami–Sudan algorithm for algebraic geometry codes. *Designs, Codes, and Cryptography*, 54(2):181–187, February 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=54&issue=2&spage=181`.

**Bierbrauer:2010:NSP**

[1205] Jürgen Bierbrauer. New semifields, PN and APN functions. *Designs, Codes, and Cryptography*, 54(3):189–200, March 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=54&issue=3&spage=189`.

**Dokovic:2010:NYN**

[1206] Dragomir Z. Đoković. A new Yang number and consequences. *Designs, Codes, and Cryptography*, 54(3):201–204, March 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=54&issue=3&spage=201`.

**Abe:2010:EHE**

[1207] Masayuki Abe, Yang Cui, Hideki Imai, and Eike Kiltz. Efficient hybrid encryption from ID-based encryption. *Designs, Codes, and Cryptography*, 54(3):205–240, March 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=54&issue=3&spage=205`.

**Petelczyc:2010:TFS**

[1208] Krzysztof Petelczyc and Małgorzata Prazmowska. Twisted Fano spaces and their classification, linear completions of systems of triangle perspectives. *Designs, Codes, and Cryptography*, 54

(3):241–251, March 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=54&issue=3&spage=241.

**Davydov:2010:LCC**

[1209] Alexander A. Davydov and Patric R. J. Östergård. Linear codes with covering radius 3. *Designs, Codes, and Cryptography*, 54(3):253–271, March 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=54&issue=3&spage=253.

**Schillewaert:2010:MCR**

[1210] J. Schillewaert, L. Storme, and J. A. Thas. Minimal codewords in Reed–Muller codes. *Designs, Codes, and Cryptography*, 54(3):273–286, March 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=54&issue=3&spage=273.

**Vandendriessche:2010:SLD**

[1211] Peter Vandendriessche. Some low-density parity-check codes derived from finite geometries. *Designs, Codes, and Cryptography*, 54(3):287–297, March 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=54&issue=3&spage=287.

**Zhou:2010:NRL**

[1212] Junling Zhou and Yanxun Chang. New results on large sets of Kirkman triple systems. *Designs, Codes, and Cryptography*, 55(1):1–7, April 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=55&issue=1&spage=1.

**Knarr:2010:PUC**

[1213] Norbert Knarr and Markus Stroppel. Polarities and unitals in the Coulter–Matthews planes. *Designs, Codes, and Cryptography*, 55(1):9–18, April 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=55&issue=1&spage=9.

**Bose:2010:OVC**

[1214] Mausumi Bose and Rahul Mukerjee. Optimal $(k, n)$ visual cryptographic schemes for general $k$. *Designs, Codes, and Cryptography*, 55(1):19–35, April 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=55&issue=1&spage=19.

**Maschietti:2010:GFC**

[1215] Antonio Maschietti. The group fixing a completely regular line-oval. *Designs, Codes, and Cryptography*, 55(1):37–43, April 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http:

//www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=55&issue=1&spage=37.

**Shi:2010:MED**

[1216] Hongsong Shi, Shaoquan Jiang, and Zhiguang Qin. More efficient DDH pseudorandom generators. *Designs, Codes, and Cryptography*, 55(1):45–64, April 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=55&issue=1&spage=45.

**Tian:2010:EVR**

[1217] Tian Tian and Wen-Feng Qi. Expected values for the rational complexity of finite binary sequences. *Designs, Codes, and Cryptography*, 55(1):65–79, April 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=55&issue=1&spage=65.

**Zhang:2010:ERD**

[1218] Xiande Zhang and Gennian Ge. Existence of resolvable $H$-designs with group sizes 2, 3, 4 and 6. *Designs, Codes, and Cryptography*, 55(1):81–101, April 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=55&issue=1&spage=81.

**Mullin:2010:SID**

[1219] Ronald C. Mullin and Rainer Steinwandt. Special issue dedicated to Spyros Magliveras on the occasion of his 70th birthday. *Designs, Codes, and Cryptography*, 55(2–3):103–105, May 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=55&issue=2&spage=103.

**Rossing:2010:SRM**

[1220] C. Rößing and L. Storme. A spectrum result on minimal blocking sets with respect to the planes of $PG(3, q)$, $q$ odd. *Designs, Codes, and Cryptography*, 55(2–3):107–119, May 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=55&issue=2&spage=107.

**DeWispelaere:2010:CGE**

[1221] A. De Wispelaere, J. A. Thas, and H. Van Maldeghem. A characterization of the Grassmann embedding of $H(q)$, with $q$ even. *Designs, Codes, and Cryptography*, 55(2–3):121–130, May 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=55&issue=2&spage=121.

**Jungnickel:2010:NDG**

[1222] Dieter Jungnickel and Vladimir D. Tonchev. The number of designs with geometric parameters grows exponentially. *Designs, Codes, and Cryptography*, 55(2–3):131–140, May 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586

(electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=55&issue=2&spage=131.

**Chatterjee:2010:CTP**

[1223] Sanjit Chatterjee, Darrel Hankerson, Edward Knapp, and Alfred Menezes. Comparing two pairing-based aggregate signature schemes. *Designs, Codes, and Cryptography*, 55(2–3): 141–167, May 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=55&issue=2&spage=141.

**Mashatan:2010:PUS**

[1224] Atefeh Mashatan and Douglas R. Stinson. Practical unconditionally secure two-channel message authentication. *Designs, Codes, and Cryptography*, 55 (2–3):169–188, May 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=55&issue=2&spage=169.

**Vasco:2010:NSM**

[1225] María Isabel González Vasco, Angel L. Pérez del Pozo, and Pedro Taborda Duarte. A note on the security of $\mathrm{MST}_3$. *Designs, Codes, and Cryptography*, 55(2–3): 189–200, May 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=55&issue=2&spage=189.

**Colbourn:2010:CAC**

[1226] Charles J. Colbourn. Covering arrays from cyclotomy. *Designs, Codes, and Cryptography*, 55(2–3): 201–219, May 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=55&issue=2&spage=201.

**Abreu:2010:AMP**

[1227] M. Abreu, C. Balbuena, and D. Labbate. Adjacency matrices of polarity graphs and of other $C_4$-free graphs of large size. *Designs, Codes, and Cryptography*, 55(2–3): 221–233, May 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=55&issue=2&spage=221.

**Huber:2010:BTD**

[1228] Michael Huber. Block-transitive designs in affine spaces. *Designs, Codes, and Cryptography*, 55(2–3): 235–242, May 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=55&issue=2&spage=235.

**Singhi:2010:MLS**

[1229] Nidhi Singhi, Nikhil Singhi, and Spyros Magliveras. Minimal logarithmic signatures for finite groups of Lie type. *Designs, Codes, and Cryptography*, 55 (2–3):243–260, May 2010. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=55&issue=2&spage=243.

**Baker:2010:EOB**

[1230] R. D. Baker, G. L. Ebert, and K. L. Wantz. Enumeration of orthogonal Buekenhout unitals. *Designs, Codes, and Cryptography*, 55 (2–3):261–283, May 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=55&issue=2&spage=261.

**Korchmaros:2010:IFL**

[1231] Gábor Korchmáros and Nicola Pace. Infinite family of large complete arcs in $\mathrm{PG}(2, q^n)$, with $q$ odd and $n > 1$ odd. *Designs, Codes, and Cryptography*, 55 (2–3):285–296, May 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=55&issue=2&spage=285.

**Newman:2010:EFC**

[1232] N. A. Newman and C. A. Rodger. Enclosings of $\lambda$-fold 4-cycle systems. *Designs, Codes, and Cryptography*, 55 (2–3):297–310, May 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=55&issue=2&spage=297.

**Buratti:2010:FPD**

[1233] Marco Buratti and Anita Pasotti. Further progress on difference families with block size 4 or 5. *Designs, Codes, and Cryptography*, 56 (1):1–20, July 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=56&issue=1&spage=1.

**Hiramine:2010:MGH**

[1234] Yutaka Hiramine. Modified generalized Hadamard matrices and constructions for transversal designs. *Designs, Codes, and Cryptography*, 56 (1):21–33, July 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=56&issue=1&spage=21.

**Glebsky:2010:SCR**

[1235] Lev Glebsky and Igor E. Shparlinski. Short cycles in repeated exponentiation modulo a prime. *Designs, Codes, and Cryptography*, 56 (1):35–42, July 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=56&issue=1&spage=35.

**Fernandez-Cordoba:2010:LCR**

[1236] Cristina Fernández-Córdoba, Jaume Pujol, and Mercè Villanueva. $\mathbf{Z}_2\mathbf{Z}_4$-linear codes: rank and kernel. *Designs, Codes, and Cryptography*, 56 (1):43–59, July 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.

asp?genre=article&issn=0925-1022&volume=56&issue=1&spage=43.

**OReilly-Regueiro:2010:RPF**

[1237] Eugenia O'Reilly-Regueiro. Reduction for primitive flag-transitive $(v, k, 4)$-symmetric designs. *Designs, Codes, and Cryptography*, 56 (1):61–63, July 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=56&issue=1&spage=61.

**Nevins:2010:NRB**

[1238] Monica Nevins, Camelia KarimianPour, and Ali Miri. NTRU over rings beyond **Z**. *Designs, Codes, and Cryptography*, 56(1): 65–78, July 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=56&issue=1&spage=65.

**Leung:2010:LCD**

[1239] Ka Hin Leung, Siu Lun Ma, and Bernhard Schmidt. On Lander's conjecture for difference sets whose order is a power of 2 or 3. *Designs, Codes, and Cryptography*, 56 (1):79–84, July 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=56&issue=1&spage=79.

**DeBeule:2010:GGA**

[1240] Jan De Beule, Yves Edel, Emilia Käsper, Andreas Klein, Svetla Nikova, et al. Galois geometries and applications. *Designs, Codes, and Cryptography*, 56(2–3):85–86, August 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=56&issue=2&spage=85.

**Ball:2010:MAG**

[1241] Simeon Ball, Jan De Beule, Leo Storme, Peter Sziklai, and Tamás Sz'onyi. In memoriam, András Gács. *Designs, Codes, and Cryptography*, 56 (2–3):87–88, August 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=56&issue=2&spage=87.

**Lavrauw:2010:LSP**

[1242] M. Lavrauw and G. Van de Voorde. On linear sets on a projective line. *Designs, Codes, and Cryptography*, 56 (2–3):89–104, August 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=56&issue=2&spage=89.

**Cossidente:2010:STC**

[1243] Antonio Cossidente and Oliver H. King. Some two-character sets. *Designs, Codes, and Cryptography*, 56 (2–3):105–113, August 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=56&issue=2&spage=105.

**Marino:2010:OBS**

[1244] G. Marino and O. Polverino. Ovoidal blocking sets and maximal partial ovoids of Hermitian varieties. *Designs, Codes, and Cryptography*, 56 (2–3):115–130, August 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=56&issue=2&spage=115`.

**Fanali:2010:SOP**

[1245] Stefania Fanali and Massimo Giulietti. On some open problems on maximal curves. *Designs, Codes, and Cryptography*, 56(2–3): 131–139, August 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=56&issue=2&spage=131`.

**Barreto:2010:WNC**

[1246] Paulo Barreto, Ventzislav Nikov, Svetla Nikova, Vincent Rijmen, and Elmar Tischhauser. Whirlwind: a new cryptographic hash function. *Designs, Codes, and Cryptography*, 56 (2–3):141–162, August 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=56&issue=2&spage=141`.

**Edel:2010:MCF**

[1247] Yves Edel and Ivan Landjev. On multiple caps in finite projective spaces. *Designs, Codes, and Cryptography*, 56 (2–3):163–175, August 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=56&issue=2&spage=163`.

**Aguglia:2010:MBS**

[1248] Angela Aguglia and Gábor Korchmáros. Multiple blocking sets and multisets in Desarguesian planes. *Designs, Codes, and Cryptography*, 56(2–3):177–181, August 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=56&issue=2&spage=177`.

**DeBruyn:2010:HPS**

[1249] Bart De Bruyn. On hyperovals of polar spaces. *Designs, Codes, and Cryptography*, 56(2–3):183–195, August 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=56&issue=2&spage=183`.

**Yoshiara:2010:NAF**

[1250] Satoshi Yoshiara. Notes on APN functions, semibiplanes and dimensional dual hyperovals. *Designs, Codes, and Cryptography*, 56(2–3): 197–218, August 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=56&issue=2&spage=197`.

**Edoukou:2010:SWC**

[1251] F. A. B. Edoukou, A. Hallez, F. Rodier, and L. Storme. The small weight codewords of the functional codes associated to non-singular Hermitian varieties. *Designs, Codes, and Cryptography*, 56 (2–3):219–233, August 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=56&issue=2&spage=219`.

**Harrach:2010:SPS**

[1252] Nóra V. Harrach and Klaus Metsch. Small point sets of $PG(n, q^3)$ intersecting each $k$-subspace in 1 mod $q$ points. *Designs, Codes, and Cryptography*, 56 (2–3):235–248, August 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=56&issue=2&spage=235`.

**Shum:2010:TAB**

[1253] Kenneth W. Shum and Wing Shing Wong. A tight asymptotic bound on the size of constant-weight conflict-avoiding codes. *Designs, Codes, and Cryptography*, 57(1):1–14, October 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=57&issue=1&spage=1`.

**Fuelberth:2010:ISN**

[1254] John Fuelberth, Athula Gunawardena, and C. David Shaffer. On incidence structures of nonsingular points and hyperbolic lines of ovoids in finite orthogonal spaces. *Designs, Codes, and Cryptography*, 57 (1):15–33, October 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=57&issue=1&spage=15`.

**Edel:2010:QAF**

[1255] Yves Edel. On quadratic APN functions and dimensional dual hyperovals. *Designs, Codes, and Cryptography*, 57 (1):35–44, October 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=57&issue=1&spage=35`.

**Schuster:2010:URD**

[1256] Ernst Schuster and Gennian Ge. On uniformly resolvable designs with block sizes 3 and 4. *Designs, Codes, and Cryptography*, 57(1):45–69, October 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=57&issue=1&spage=45`.

**Sakzad:2010:CGT**

[1257] Amin Sakzad, Mohammad-Reza Sadeghi, and Daniel Panario. Codes with girth 8 Tanner graph representation. *Designs, Codes, and Cryptography*, 57 (1):71–81, October 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.`

asp?genre=article&issn=0925-1022&volume=57&issue=1&spage=71.

**Zhao:2010:NRB**

[1258] Zhengjun Zhao and Xiwang Cao. A note on the reducibility of binary affine polynomials. *Designs, Codes, and Cryptography*, 57(1):83–90, October 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=57&issue=1&spage=83.

**Walikar:2010:DAM**

[1259] H. B. Walikar, B. D. Acharya, and Shailaja S. Shirkol. Designs associated with maximum independent sets of a graph. *Designs, Codes, and Cryptography*, 57(1):91–105, October 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=57&issue=1&spage=91.

**Nakashima:2010:ACV**

[1260] Tohru Nakashima. AG codes from vector bundles. *Designs, Codes, and Cryptography*, 57(1):107–115, October 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=57&issue=1&spage=107.

**Zhou:2010:AGF**

[1261] Shenglin Zhou and Huili Dong. Alternating groups and flag-transitive triplanes. *Designs, Codes, and Cryptography*, 57(2):117–126, November 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=57&issue=2&spage=117.

**Blinovsky:2010:WDM**

[1262] Vladimir Blinovsky, Uri Erez, and Simon Litsyn. Weight distribution moments of random linear/coset codes. *Designs, Codes, and Cryptography*, 57 (2):127–138, November 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=57&issue=2&spage=127.

**Zaverucha:2010:ASS**

[1263] Gregory M. Zaverucha and Douglas R. Stinson. Anonymity in shared symmetric key primitives. *Designs, Codes, and Cryptography*, 57(2):139–160, November 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=57&issue=2&spage=139.

**Fernandez-Cordoba:2010:MDG**

[1264] C. Fernández-Córdoba and K. T. Phelps. On the minimum distance graph of an extended Preparata code. *Designs, Codes, and Cryptography*, 57 (2):161–168, November 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=57&issue=2&spage=161.

**Byrne:2010:NBC**

[1265] Eimear Byrne, Marcus Greferath, Axel Kohnert, and Vitaly Skachek. New bounds for codes over finite Frobenius rings. *Designs, Codes, and Cryptography*, 57(2):169–179, November 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=57&issue=2&spage=169`.

**Krotov:2010:BCP**

[1266] Denis S. Krotov. On the binary codes with parameters of doubly-shortened 1-perfect codes. *Designs, Codes, and Cryptography*, 57(2):181–194, November 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=57&issue=2&spage=181`.

**Park:2010:MDH**

[1267] Seungkook Park. Minimum distance of Hermitian two-point codes. *Designs, Codes, and Cryptography*, 57(2):195–213, November 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=57&issue=2&spage=195`.

**Zhou:2010:OPD**

[1268] Zhengchun Zhou and Xiaohu Tang. Optimal and perfect difference systems of sets from $q$-ary sequences with difference-balanced property. *Designs, Codes, and Cryptography*, 57(2):215–223, November 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=57&issue=2&spage=215`.

**Zhang:2010:DPR**

[1269] Xiande Zhang and Gennian Ge. $H$-designs with the properties of resolvability or $(1, 2)$-resolvability. *Designs, Codes, and Cryptography*, 57(3):225–256, December 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=57&issue=3&spage=225`.

**Pasalic:2010:SRC**

[1270] E. Pasalic and P. Charpin. Some results concerning cryptographically significant mappings over GF($2^n$). *Designs, Codes, and Cryptography*, 57(3):257–269, December 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=57&issue=3&spage=257`.

**Wang:2010:EAI**

[1271] Chun peng Wang and Xiao song Chen. On extended algebraic immunity. *Designs, Codes, and Cryptography*, 57(3):271–281, December 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=57&issue=3&spage=271`.

**Rizomiliotis:2010:SFL**

[1272] Panagiotis Rizomiliotis. On the security of the Feng–Liao–Yang Boolean functions with optimal algebraic immunity against fast algebraic attacks. *Designs, Codes, and Cryptography*, 57 (3):283–292, December 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=57&issue=3&spage=283`.

**Hong:2010:CFA**

[1273] Jin Hong. The cost of false alarms in Hellman and rainbow tradeoffs. *Designs, Codes, and Cryptography*, 57(3): 293–327, December 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=57&issue=3&spage=293`.

**Kim:2010:SDC**

[1274] Hyun Jin Kim. Self-dual codes with automorphism of order 3 having 8 cycles. *Designs, Codes, and Cryptography*, 57 (3):329–346, December 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=57&issue=3&spage=329`.

**Donati:2010:IHC**

[1275] Giorgio Donati and Nicola Durante. On the intersection of a Hermitian curve with a conic. *Designs, Codes, and Cryptography*, 57(3):347–360, December 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=57&issue=3&spage=347`.

**Shaheen:2010:PFF**

[1276] Rasha Shaheen and Arne Winterhof. Permutations of finite fields for check digit systems. *Designs, Codes, and Cryptography*, 57(3):361–371, December 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=57&issue=3&spage=361`.

**Dempwolff:2010:GDT**

[1277] Ulrich Dempwolff and Timo Neumann. Geometric and design-theoretic aspects of semibent functions I. *Designs, Codes, and Cryptography*, 57(3): 373–381, December 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=57&issue=3&spage=373`.

**Abel:2010:EDB**

[1278] R. J. R. Abel and F. E. Bennett. Existence of directed BIBDs with block size 7 and related perfect 5-deletion-correcting codes of length 7. *Designs, Codes, and Cryptography*, 57(3): 383–397, December 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=57&issue=3&spage=383`.

**Liu:2011:EWB**

[1279] Xiaoyu Liu. An equivalence of Ward's bound and its application. *Designs, Codes, and Cryptography*, 58 (1):1–9, January 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=58&issue=1&spage=1`.

**Tassa:2011:GOT**

[1280] Tamir Tassa. Generalized oblivious transfer by secret sharing. *Designs, Codes, and Cryptography*, 58 (1):11–21, January 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=58&issue=1&spage=11`.

**Cui:2011:QGQ**

[1281] Jie Cui and Junying Pei. Quaternary 1-generator quasi-cyclic codes. *Designs, Codes, and Cryptography*, 58 (1):23–33, January 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=58&issue=1&spage=23`.

**Zhao:2011:CBP**

[1282] Chang-An Zhao, Dongqing Xie, Fangguo Zhang, Jingwei Zhang, and Bing-Long Chen. Computing bilinear pairings on elliptic curves with automorphisms. *Designs, Codes, and Cryptography*, 58(1):35–44, January 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=58&issue=1&spage=35`.

**Yun:2011:LMQ**

[1283] Aaram Yun, Je Hong Park, and Jooyoung Lee. On Lai–Massey and quasi-Feistel ciphers. *Designs, Codes, and Cryptography*, 58(1):45–72, January 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=58&issue=1&spage=45`.

**OCathain:2011:CHM**

[1284] Padraig Ó Catháin and Marc Röder. The cocyclic Hadamard matrices of order less than 40. *Designs, Codes, and Cryptography*, 58(1):73–88, January 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=58&issue=1&spage=73`.

**Buratti:2011:NRO**

[1285] Marco Buratti, Koji Momihara, and Anita Pasotti. New results on optimal $(v, 4, 2, 1)$ optical orthogonal codes. *Designs, Codes, and Cryptography*, 58 (1):89–109, January 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=58&issue=1&spage=89`.

**Pawale:2011:QSD**

[1286] Rajendra M. Pawale. Quasi-symmetric designs with the difference of block intersection numbers two. *Designs, Codes, and Cryptography*, 58(2):111–121, February 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=58&issue=2&spage=111`.

**Ghorpade:2011:PPS**

[1287] Sudhir R. Ghorpade, Sartaj Ul Hasan, and Meena Kumari. Primitive polynomials, Singer cycles and word-oriented linear feedback shift registers. *Designs, Codes, and Cryptography*, 58 (2):123–134, February 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=58&issue=2&spage=123`.

**Lei:2011:ODS**

[1288] Jianguo Lei and Cuiling Fan. Optimal difference systems of sets and partition-type cyclic difference packings. *Designs, Codes, and Cryptography*, 58 (2):135–153, February 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=58&issue=2&spage=135`.

**Glynn:2011:IMS**

[1289] David G. Glynn. An invariant for matrices and sets of points in prime characteristic. *Designs, Codes, and Cryptography*, 58(2):155–172, February 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=58&issue=2&spage=155`.

**Avanzi:2011:RAE**

[1290] Roberto Avanzi, Clemens Heuberger, and Helmut Prodinger. Redundant $\tau$-adic expansions I: non-adjacent digit sets and their applications to scalar multiplication. *Designs, Codes, and Cryptography*, 58(2):173–202, February 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=58&issue=2&spage=173`.

**Betsumiya:2011:HMO**

[1291] Koichi Betsumiya, Masaaki Harada, and Hiroshi Kimura. Hadamard matrices of order 32 and extremal ternary self-dual codes. *Designs, Codes, and Cryptography*, 58(2):203–214, February 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=58&issue=2&spage=203`.

**Glynn:2011:CAM**

[1292] David G. Glynn. A condition for arcs and MDS codes. *Designs, Codes, and Cryptography*, 58(2):215–218, February 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.`

asp?genre=article&issn=0925-1022&volume=58&issue=2&spage=215.

**Poulakis:2011:EVD**

[1293] Dimitrios Poulakis. Erratum to: A Variant of Digital Signature Algorithm. *Designs, Codes, and Cryptography*, 58(2):219, February 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=58&issue=2&spage=219. See [1134].

**Yildiz:2011:CC**

[1294] Bahattin Yildiz and Suat Karadeniz. Cyclic codes over $F_2+uF_2+vF_2+uvF_2$. *Designs, Codes, and Cryptography*, 58 (3):221–234, March 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=58&issue=3&spage=221.

**Park:2011:IPE**

[1295] Jong Hwan Park. Inner-product encryption under standard assumptions. *Designs, Codes, and Cryptography*, 58 (3):235–257, March 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=58&issue=3&spage=235.

**Li:2011:EEC**

[1296] Yongqiang Li and Mingsheng Wang. On EA-equivalence of certain permutations to power mappings. *Designs, Codes, and Cryptography*, 58 (3):259–269, March 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=58&issue=3&spage=259.

**Sarkar:2011:TBC**

[1297] Palash Sarkar. A trade-off between collision probability and key size in universal hashing using polynomials. *Designs, Codes, and Cryptography*, 58 (3):271–278, March 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=58&issue=3&spage=271.

**Zhou:2011:ELC**

[1298] Jianqin Zhou. On the $k$-error linear complexity of sequences with period $2p^n$ over GF(q). *Designs, Codes, and Cryptography*, 58(3):279–296, March 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=58&issue=3&spage=279.

**Lee:2011:IHV**

[1299] Kwangsu Lee and Dong Hoon Lee. Improved hidden vector encryption with short ciphertexts and tokens. *Designs, Codes, and Cryptography*, 58 (3):297–319, March 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=58&issue=3&spage=297.

**Zhang:2011:CRS**

[1300] Hui Zhang and Gennian Ge. Completely reducible super-simple designs with block size four and related super-simple packings. *Designs, Codes, and Cryptography*, 58 (3):321–346, March 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=58&issue=3&spage=321`.

**Parker:2011:E**

[1301] Matthew Geoffrey Parker, Sasha Kholosha, Pascale Charpin, and Eirik Rosnes. Editorial. *Designs, Codes, and Cryptography*, 59 (1–3):1, April 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=59&issue=1&spage=1`.

**Blondeau:2011:AED**

[1302] Céline Blondeau, Benoît Gérard, and Jean-Pierre Tillich. Accurate estimates of the data complexity and success probability for various cryptanalyses. *Designs, Codes, and Cryptography*, 59(1–3):3–34, April 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=59&issue=1&spage=3`.

**Bogdanov:2011:UFN**

[1303] Andrey Bogdanov. On unbalanced Feistel networks with contracting MDS diffusion. *Designs, Codes, and Cryptography*, 59(1–3): 35–58, April 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=59&issue=1&spage=35`.

**Brandstatter:2011:CTP**

[1304] Nina Brandstätter, Gottlieb Pirsic, and Arne Winterhof. Correlation of the two-prime Sidel'nikov sequence. *Designs, Codes, and Cryptography*, 59 (1–3):59–68, April 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=59&issue=1&spage=59`.

**Budaghyan:2011:CEB**

[1305] Lilya Budaghyan and Claude Carlet. CCZ-equivalence of bent vectorial functions and related constructions. *Designs, Codes, and Cryptography*, 59 (1–3):69–87, April 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=59&issue=1&spage=69`.

**Carlet:2011:RTN**

[1306] Claude Carlet. Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions. *Designs, Codes, and Cryptography*, 59(1–3): 89–109, April 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.`

asp?genre=article&issn=0925-1022&volume=59&issue=1&spage=89.

**Danev:2011:FCT**

[1307] Danyo Danev, Stefan Dodunekov, and Diana Radkova. A family of constacyclic ternary quasi-perfect codes with covering radius 3. *Designs, Codes, and Cryptography*, 59(1–3): 111–118, April 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=59&issue=1&spage=111.

**Danielsen:2011:DGR**

[1308] Lars Eirik Danielsen and Matthew G. Parker. Directed graph representation of half-rate additive codes over GF(4). *Designs, Codes, and Cryptography*, 59 (1–3):119–130, April 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=59&issue=1&spage=119.

**Gibson:2011:QGSa**

[1309] Richard G. Gibson and Jonathan Jedwab. Quaternary Golay sequence pairs I: even length. *Designs, Codes, and Cryptography*, 59 (1–3):131–146, April 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=59&issue=1&spage=131.

**Gibson:2011:QGSb**

[1310] Richard G. Gibson and Jonathan Jedwab. Quaternary Golay sequence pairs II: odd length. *Designs, Codes, and Cryptography*, 59 (1–3):147–157, April 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=59&issue=1&spage=147.

**Harris:2011:CRK**

[1311] David G. Harris. Critique of the related-key attack concept. *Designs, Codes, and Cryptography*, 59(1–3): 159–168, April 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=59&issue=1&spage=159.

**Joye:2011:HDS**

[1312] Marc Joye. How (not) to design strong-RSA signatures. *Designs, Codes, and Cryptography*, 59 (1–3):169–182, April 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=59&issue=1&spage=169.

**Klove:2011:LBS**

[1313] Torleiv Kløve. Lower bounds on the size of spheres of permutations under the Chebychev distance. *Designs, Codes, and Cryptography*, 59 (1–3):183–191, April 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=59&issue=1&spage=183.

**Langevin:2011:CAB**

[1314] Philippe Langevin and Gregor Leander. Counting all bent functions in dimension eight 99270589265934370305785861242880 [$\approx 2^{106}$]. *Designs, Codes, and Cryptography*, 59(1–3):193–205, April 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=59&issue=1&spage=193`.

**Leander:2011:BDA**

[1315] Gregor Leander and François Rodier. Bounds on the degree of APN polynomials: the case of $x^{-1} + g(x)$. *Designs, Codes, and Cryptography*, 59 (1–3):207–222, April 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=59&issue=1&spage=207`.

**Lisonek:2011:ZKS**

[1316] Petr Lisonek and Marko Moisio. On zeros of Kloosterman sums. *Designs, Codes, and Cryptography*, 59 (1–3):223–230, April 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=59&issue=1&spage=223`.

**Maitra:2011:SOH**

[1317] Subhamoy Maitra, Goutam Paul, Shashwat Raizada, Subhabrata Sen, and Rudradev Sengupta. Some observations on HC-128. *Designs, Codes, and Cryptography*, 59(1–3): 231–245, April 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=59&issue=1&spage=231`.

**Manuel:2011:CGD**

[1318] Stéphane Manuel. Classification and generation of disturbance vectors for collision attacks against SHA-1. *Designs, Codes, and Cryptography*, 59 (1–3):247–263, April 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=59&issue=1&spage=247`.

**Mesnager:2011:NCB**

[1319] Sihem Mesnager. A new class of bent and hyper-bent Boolean functions in polynomial forms. *Designs, Codes, and Cryptography*, 59 (1–3):265–279, April 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=59&issue=1&spage=265`.

**Ostergaard:2011:TOO**

[1320] Patric R. J. Östergård and Olli Pottonen. Two optimal one-error-correcting codes of length 13 that are not doubly shortened perfect codes. *Designs, Codes, and Cryptography*, 59 (1–3):281–285, April 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=59&issue=1&spage=281`.

**Ozbudak:2011:CAC**

[1321] Elif Kurtaran Özbudak, Ferruh Özbudak, and Zülfükar Saygi. A class of authentication codes with secrecy. *Designs, Codes, and Cryptography*, 59 (1–3):287–318, April 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=59&issue=1&spage=287`.

**Pott:2011:ASA**

[1322] Alexander Pott, Yin Tan, Tao Feng, and San Ling. Association schemes arising from bent functions. *Designs, Codes, and Cryptography*, 59 (1–3):319–331, April 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=59&issue=1&spage=319`.

**Schmidt:2011:CDD**

[1323] Kai-Uwe Schmidt. On the correlation distribution of Delsarte–Goethals sequences. *Designs, Codes, and Cryptography*, 59(1–3):333–347, April 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=59&issue=1&spage=333`.

**Semaev:2011:SBE**

[1324] Igor Semaev. Sparse Boolean equations and circuit lattices. *Designs, Codes, and Cryptography*, 59(1–3): 349–364, April 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=59&issue=1&spage=349`.

**Tu:2011:CAB**

[1325] Ziran Tu and Yingpu Deng. A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity. *Designs, Codes, and Cryptography*, 60(1):1–14, July 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=60&issue=1&spage=1`.

**Kim:2011:NRR**

[1326] Jongsung Kim, Jaechul Sung, Ermaliza Razali, Raphael C.-W. Phan, and Marc Joye. Notions and relations for RKA-secure permutation and function families. *Designs, Codes, and Cryptography*, 60(1):15–35, July 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=60&issue=1&spage=15`.

**Chang:2011:PDG**

[1327] Yanxun Chang, Yeow Meng Chee, and Junling Zhou. A pair of disjoint 3-GDDs of type $g^t u^1$. *Designs, Codes, and Cryptography*, 60 (1):37–62, July 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=60&issue=1&spage=37`.

**Ghodosi:2011:CHL**

[1328] Hossein Ghodosi. Comments on Harn–Lin's cheating detection scheme. *Designs, Codes, and Cryptography*, 60 (1):63–66, July 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=60&issue=1&spage=63`.

**Cao:2011:SPE**

[1329] Yonglin Cao. Structural properties and enumeration of 1-generator generalized quasi-cyclic codes. *Designs, Codes, and Cryptography*, 60 (1):67–79, July 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=60&issue=1&spage=67`.

**Ranto:2011:BLI**

[1330] Sanna Ranto. On binary linear $r$-identifying codes. *Designs, Codes, and Cryptography*, 60(1): 81–89, July 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=60&issue=1&spage=81`.

**Hiramine:2011:FNC**

[1331] Yutaka Hiramine. A family of non class-regular symmetric transversal designs of spread type. *Designs, Codes, and Cryptography*, 60 (1):91–99, July 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=60&issue=1&spage=91`.

**Trinker:2011:CHD**

[1332] Horst Trinker. Cubic and higher degree bounds for codes and $(t, m, s)$-nets. *Designs, Codes, and Cryptography*, 60 (2):101–121, August 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=60&issue=2&spage=101`.

**Lu:2011:RKI**

[1333] Jiqiang Lu. The (related-key) impossible boomerang attack and its application to the AES block cipher. *Designs, Codes, and Cryptography*, 60 (2):123–143, August 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=60&issue=2&spage=123`.

**Ma:2011:NDF**

[1334] Wenping Ma and Shaohui Sun. New designs of frequency hopping sequences with low hit zone. *Designs, Codes, and Cryptography*, 60 (2):145–153, August 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=60&issue=2&spage=145`.

**Alhakim:2011:RCN**

[1335] Abbas Alhakim and Mufutau Akinwande. A recursive construction of

nonbinary de Bruijn sequences. *Designs, Codes, and Cryptography*, 60 (2):155–169, August 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=60&issue=2&spage=155`.

**Li:2011:ACI**

[1336] Yin Li, Gong liang Chen, and Jian hua Li. An alternative class of irreducible polynomials for optimal extension fields. *Designs, Codes, and Cryptography*, 60(2):171–182, August 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=60&issue=2&spage=171`.

**Singhi:2011:MLS**

[1337] Nikhil Singhi and Nidhi Singhi. Minimal logarithmic signatures for classical groups. *Designs, Codes, and Cryptography*, 60(2):183–195, August 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=60&issue=2&spage=183`.

**Grundhofer:2011:NEI**

[1338] Theo Grundhöfer, Boris Krinn, and Markus Stroppel. Non-existence of isomorphisms between certain unitals. *Designs, Codes, and Cryptography*, 60 (2):197–201, August 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=60&issue=2&spage=197`.

**Menegatto:2011:EPD**

[1339] V. A. Menegatto, C. P. Oliveira, and A. P. Peron. Exact point-distributions over the complex sphere. *Designs, Codes, and Cryptography*, 60(3):203–223, September 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=60&issue=3&spage=203`.

**Donovan:2011:DHP**

[1340] D. M. Donovan and M. J. Grannell. Designs having the parameters of projective and affine spaces. *Designs, Codes, and Cryptography*, 60(3): 225–240, September 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=60&issue=3&spage=225`.

**Zhou:2011:GMG**

[1341] Zhengchun Zhou and Xiaohu Tang. Generalized modified Gold sequences. *Designs, Codes, and Cryptography*, 60 (3):241–253, September 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=60&issue=3&spage=241`.

**Park:2011:FCR**

[1342] Jong Hwan Park and Dong Hoon Lee. Fully collusion-resistant traitor tracing scheme with shorter ciphertexts. *Designs, Codes, and Cryptography*, 60(3):

255–276, September 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=60&issue=3&spage=255.

**Metsch:2011:GRD**

[1343] Klaus Metsch. A generalization of a result of Dembowski and Wagner. *Designs, Codes, and Cryptography*, 60(3): 277–282, September 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=60&issue=3&spage=277.

**Liang:2011:NCS**

[1344] Miao Liang and Beiliang Du. A new class of splitting 3-designs. *Designs, Codes, and Cryptography*, 60(3): 283–290, September 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=60&issue=3&spage=283.

**Carrillo-Pacheco:2011:LGC**

[1345] Jesús Carrillo-Pacheco and Felipe Zaldivar. On Lagrangian–Grassmannian codes. *Designs, Codes, and Cryptography*, 60(3):291–298, September 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=60&issue=3&spage=291.

**Lee:2011:DPA**

[1346] Chia-Jung Lee, Te-Tsung Lin, Min-Zheng Shieh, Shi-Chun Tsai, and Hsin-Lung Wu. Decoding permutation arrays with ternary vectors. *Designs, Codes, and Cryptography*, 61(1):1–9, October 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=61&issue=1&spage=1.

**Marino:2011:TCR**

[1347] Giuseppe Marino, Olga Polverino, and Rocco Trombetti. Towards the classification of rank 2 semifields 6-dimensional over their center. *Designs, Codes, and Cryptography*, 61 (1):11–29, October 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=61&issue=1&spage=11.

**Bilal:2011:MDS**

[1348] M. Bilal, J. Borges, S. T. Dougherty, and C. Fernández-Córdoba. Maximum distance separable codes over $\mathbf{Z}_4$ and $\mathbf{Z}_2 \times \mathbf{Z}_4$. *Designs, Codes, and Cryptography*, 61(1):31–40, October 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=61&issue=1&spage=31.

**Batra:2011:SCC**

[1349] Sudhir Batra and S. K. Arora. Some cyclic codes of length $2p^n$. *Designs, Codes, and Cryptography*, 61

(1):41–69, October 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=61&issue=1&spage=41.

**Avanzi:2011:DCN**

[1350] Roberto Avanzi, Waldyr Dias Benits, Steven D. Galbraith, and James McKee. On the distribution of the coefficients of normal forms for Frobenius expansions. *Designs, Codes, and Cryptography*, 61(1):71–89, October 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=61&issue=1&spage=71.

**Prazmowska:2011:SPC**

[1351] Małgorzata Prazmowska and Krzysztof Prazmowski. Semi-Pappus configurations; combinatorial generalizations of the Pappus configuration. *Designs, Codes, and Cryptography*, 61(1):91–103, October 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=61&issue=1&spage=91.

**Plagne:2011:ACT**

[1352] Alain Plagne and Wolfgang A. Schmid. An application of coding theory to estimating Davenport constants. *Designs, Codes, and Cryptography*, 61(1):105–118, October 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=61&issue=1&spage=105.

**Liu:2011:FRS**

[1353] Zihui Liu, Wende Chen, Zhimin Sun, and Xiangyong Zeng. Further results on support weights of certain subcodes. *Designs, Codes, and Cryptography*, 61(2):119–129, November 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=61&issue=2&spage=119.

**Cheon:2011:NEG**

[1354] E. J. Cheon. The non-existence of Griesmer codes with parameters close to codes of Belov type. *Designs, Codes, and Cryptography*, 61(2):131–139, November 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=61&issue=2&spage=131.

**Han:2011:BFS**

[1355] Sunghyu Han, Heisook Lee, and Yoonjin Lee. Binary formally self-dual odd codes. *Designs, Codes, and Cryptography*, 61(2):141–150, November 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=61&issue=2&spage=141.

**Chee:2011:LDS**

[1356] Yeow Meng Chee, Gennian Ge, Lijun Ji, San Ling, and Jianxing Yin.

List decodability at small radii. *Designs, Codes, and Cryptography*, 61(2): 151–166, November 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=61&issue=2&spage=151.

**Marti-Farre:2011:OCS**

[1357] Jaume Martí-Farré, Carles Padró, and Leonor Vázquez. Optimal complexity of secret sharing schemes with four minimal qualified subsets. *Designs, Codes, and Cryptography*, 61(2): 167–186, November 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=61&issue=2&spage=167.

**Bierbrauer:2011:CSP**

[1358] Jürgen Bierbrauer. Commutative semifields from projection mappings. *Designs, Codes, and Cryptography*, 61(2): 187–196, November 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=61&issue=2&spage=187.

**Cordero:2011:FDS**

[1359] Minerva Cordero and Vikram Jha. Fractional dimensions in semifields of odd order. *Designs, Codes, and Cryptography*, 61(2):197–221, November 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=61&issue=2&spage=197.

**Koga:2011:GMC**

[1360] Hiroki Koga and Takeru Ishihara. A general method for construction of $(t, n)$-threshold visual secret sharing schemes for color images. *Designs, Codes, and Cryptography*, 61(2): 223–249, November 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=61&issue=2&spage=223.

**Edemskiy:2011:ACL**

[1361] Vladimir Edemskiy. About computation of the linear complexity of generalized cyclotomic sequences with period $p^{n+1}$. *Designs, Codes, and Cryptography*, 61(3):251–260, December 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=61&issue=3&spage=251.

**Bracken:2011:EQA**

[1362] Carl Bracken, Eimear Byrne, Gary McGuire, and Gabriele Nebe. On the equivalence of quadratic APN functions. *Designs, Codes, and Cryptography*, 61(3):261–272, December 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=61&issue=3&spage=261.

**Hanson:2011:SLR**

[1363] B. Hanson, D. Panario, and D. Thomson. Swan-like results for binomials and trinomials over finite fields of odd characteristic. *Designs, Codes, and Cryptography*, 61(3):273–283, December 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=61&issue=3&spage=273`.

**Abel:2011:EGB**

[1364] R. Julian R. Abel, Nigel H. N. Chan, Diana Combe, and William D. Palmer. Existence of GBRDs with block size 4 and BRDs with block size 5. *Designs, Codes, and Cryptography*, 61(3):285–300, December 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=61&issue=3&spage=285`.

**Kyuregyan:2011:ICP**

[1365] Melsik K. Kyuregyan and Gohar M. Kyureghyan. Irreducible compositions of polynomials over finite fields. *Designs, Codes, and Cryptography*, 61(3):301–314, December 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=61&issue=3&spage=301`.

**Krotov:2011:WDP**

[1366] Denis S. Krotov. On weight distributions of perfect colorings and completely regular codes. *Designs, Codes, and Cryptography*, 61(3):315–329, December 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=61&issue=3&spage=315`.

**Wang:2011:LSF**

[1367] Qi Wang. The linear span of the frequency hopping sequences in optimal sets. *Designs, Codes, and Cryptography*, 61(3):331–344, December 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=61&issue=3&spage=331`.

**Jesso:2011:HCR**

[1368] Andrew T. Jesso, David A. Pike, and Nabil Shalaby. Hamilton cycles in restricted block-intersection graphs. *Designs, Codes, and Cryptography*, 61(3):345–353, December 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=61&issue=3&spage=345`.

**Lamberger:2012:MNC**

[1369] Mario Lamberger, Florian Mendel, Vincent Rijmen, and Koen Simoens. Memoryless near-collisions via coding theory. *Designs, Codes, and Cryptography*, 62(1):1–18, January 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=62&issue=1&spage=1`.

**Fan:2012:ESD**

[1370] Yun Fan and Guanghui Zhang. On the existence of self-dual permutation codes of finite groups. *Designs, Codes, and Cryptography*, 62 (1):19–29, January 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=62&issue=1&spage=19`.

**Guenda:2012:NMS**

[1371] Kenza Guenda. New MDS self-dual codes over finite fields. *Designs, Codes, and Cryptography*, 62 (1):31–42, January 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=62&issue=1&spage=31`.

**Christopoulou:2012:GPC**

[1372] M. Christopoulou, T. Garefalakis, D. Panario, and D. Thomson. Gauss periods as constructions of low complexity normal bases. *Designs, Codes, and Cryptography*, 62(1):43–62, January 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=62&issue=1&spage=43`.

**Bonvicini:2012:SPE**

[1373] Simona Bonvicini, Marco Buratti, Gloria Rinaldi, and Tommaso Traetta. Some progress on the existence of 1-rotational Steiner triple systems. *Designs, Codes, and Cryptography*, 62 (1):63–78, January 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=62&issue=1&spage=63`.

**Lang:2012:TTW**

[1374] Wolfgang Lang and Ekkehard Schneider. Turyn type Williamson matrices up to order 99. *Designs, Codes, and Cryptography*, 62(1):79–84, January 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=62&issue=1&spage=79`.

**Bhaintwal:2012:SQC**

[1375] Maheshanand Bhaintwal. Skew quasi-cyclic codes over Galois rings. *Designs, Codes, and Cryptography*, 62 (1):85–101, January 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=62&issue=1&spage=85`.

**Szonyi:2012:STL**

[1376] Tamás Szőnyi and Zsuzsa Weiner. A stability theorem for lines in Galois planes of prime order. *Designs, Codes, and Cryptography*, 62 (1):103–108, January 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=62&issue=1&spage=103`.

**Liang:2012:NCF**

[1377] Miao Liang and Beiliang Du. A new class of 3-fold perfect splitting authentication codes. *Designs, Codes, and Cryptography*, 62(1):109–119, January 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=62&issue=1&spage=109`.

**Maruta:2012:GET**

[1378] Tatsuya Maruta and Yuri Yoshida. A generalized extension theorem for linear codes. *Designs, Codes, and Cryptography*, 62(1):121–130, January 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=62&issue=1&spage=121`.

**Shi:2012:EBO**

[1379] Ce Shi, Yu Tang, and Jianxing Yin. The equivalence between optimal detecting arrays and super-simple OAs. *Designs, Codes, and Cryptography*, 62(2):131–142, February 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=62&issue=2&spage=131`.

**Zhang:2012:OCW**

[1380] Xiande Zhang, Hui Zhang, and Gennian Ge. Optimal constant weight covering codes and nonuniform group divisible 3-designs with block size four. *Designs, Codes, and Cryptography*, 62(2):143–160, February 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=62&issue=2&spage=143`.

**Kai:2012:NSD**

[1381] Xiaoshan Kai and Shixin Zhu. Negacyclic self-dual codes over finite chain rings. *Designs, Codes, and Cryptography*, 62(2):161–174, February 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=62&issue=2&spage=161`.

**Glynn:2012:FPM**

[1382] David G. Glynn. The factorization of the permanent of a matrix with minimal rank in prime characteristic. *Designs, Codes, and Cryptography*, 62(2):175–177, February 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=62&issue=2&spage=175`.

**Roh:2012:SRD**

[1383] Dongyoung Roh and Sang Geun Hahn. The square root Diffie–Hellman problem. *Designs, Codes, and Cryptography*, 62(2):179–187, February 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=62&issue=2&spage=179`.

**Ozbudak:2012:NCQ**

[1384] Ferruh Özbudak, Elif Saygi, and Zülfükar Saygi. A new class of quaternary LCZ sequence sets. *Designs, Codes, and Cryptography*, 62 (2):189–198, February 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=62&issue=2&spage=189`.

**Ji:2012:CCA**

[1385] Lijun Ji, Yang Li, and Jianxing Yin. Constructions of covering arrays of strength five. *Designs, Codes, and Cryptography*, 62(2):199–208, February 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=62&issue=2&spage=199`.

**Rifa:2012:IHC**

[1386] J. Rifà, F. I. Solov'eva, and M. Villanueva. Intersection of Hamming codes avoiding Hamming subcodes. *Designs, Codes, and Cryptography*, 62 (2):209–223, February 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=62&issue=2&spage=209`.

**Shaw:2012:ASV**

[1387] Ron Shaw, Neil Gordon, and Hans Havlicek. Aspects of the Segre variety $S_{1,1,1}(2)\mathcal{S}_{\infty,\infty,\infty}(\in)$. *Designs, Codes, and Cryptography*, 62(2):225–239, February 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=62&issue=2&spage=225`.

**Dempwolff:2012:GDT**

[1388] Ulrich Dempwolff. Geometric and design-theoretic aspects of semibent functions II. *Designs, Codes, and Cryptography*, 62(2):241–252, February 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=62&issue=2&spage=241`.

**Feng:2012:CCL**

[1389] Tao Feng. On cyclic codes of length $2^{2^r} - 1$ with two zeros whose dual codes have three weights. *Designs, Codes, and Cryptography*, 62(3):253–258, March 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=62&issue=3&spage=253`.

**Ghodosi:2012:MPC**

[1390] Hossein Ghodosi, Josef Pieprzyk, and Ron Steinfeld. Multi-party computation with conversion of secret sharing. *Designs, Codes, and Cryptography*, 62(3):259–272, March 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=62&issue=3&spage=259`.

**Arasu:2012:NC**

[1391] K. T. Arasu and Siu Lun Ma. Nonexistence of CW(110, 100). *Designs, Codes, and Cryptography*, 62(3):273–278, March 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=62&issue=3&spage=273`.

**Hiramine:2012:CMG**

[1392] Yutaka Hiramine. A construction for modified generalized Hadamard matrices using QGH matrices. *Designs, Codes, and Cryptography*, 62 (3):279–288, March 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=62&issue=3&spage=279`.

**Hu:2012:FAT**

[1393] Yupu Hu, Juntao Gao, Qing Liu, and Yiwei Zhang. Fault analysis of Trivium. *Designs, Codes, and Cryptography*, 62 (3):289–311, March 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=62&issue=3&spage=289`.

**Tan:2012:AAN**

[1394] Lin Tan, Wen-Feng Qi, and Hong Xu. Asymptotic analysis on the normalized $k$-error linear complexity of binary sequences. *Designs, Codes, and Cryptography*, 62(3):313–321, March 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=62&issue=3&spage=313`.

**Kaski:2012:STS**

[1395] Petteri Kaski, Mahdad Khatirinejad, and Patric R. J. Östergård. Steiner triple systems satisfying the 4-vertex condition. *Designs, Codes, and Cryptography*, 62(3):323–330, March 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=62&issue=3&spage=323`.

**Britz:2012:WTD**

[1396] Thomas Britz, Trygve Johnsen, Dillon Mayhew, and Keisuke Shiromoto. Wei-type duality theorems for matroids. *Designs, Codes, and Cryptography*, 62 (3):331–341, March 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=62&issue=3&spage=331`.

**Havlicek:2012:INS**

[1397] Hans Havlicek, Boris Odehnal, and Metod Saniga. On invariant notions of Segre varieties in binary projective spaces. *Designs, Codes, and Cryptography*, 62(3):343–356, March 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=62&issue=3&spage=343`.

**Webster:2012:URI**

[1398] Jordan D. Webster. Using rational idempotents to show Turyn's bound is sharp. *Designs, Codes, and Cryptography*, 62(3):357–365, March 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=62&issue=3&spage=357`.

**Bisson:2012:LMA**

[1399] Gaetan Bisson and Andrew V. Sutherland. A low-memory algorithm for finding short product representations in finite groups. *Designs, Codes, and Cryptography*, 63(1):1–13, April 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=63&issue=1&spage=1`.

**Donovan:2012:NDA**

[1400] D. M. Donovan and M. J. Grannell. On the number of designs with affine parameters. *Designs, Codes, and Cryptography*, 63(1):15–27, April 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=63&issue=1&spage=15`.

**McLoughlin:2012:GRC**

[1401] Ian McLoughlin. A group ring construction of the $[48, 24, 12]$ type II linear block code. *Designs, Codes, and Cryptography*, 63(1):29–41, April 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=63&issue=1&spage=29`.

**Kim:2012:BES**

[1402] Hyun Jin Kim. The binary extremal self-dual codes of lengths 38 and 40. *Designs, Codes, and Cryptography*, 63(1):43–57, April 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=63&issue=1&spage=43`.

**Ostafe:2012:PVS**

[1403] Alina Ostafe. Pseudorandom vector sequences of maximal period generated by triangular polynomial dynamical systems. *Designs, Codes, and Cryptography*, 63(1):59–72, April 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=63&issue=1&spage=59`.

**Mavron:2012:QSD**

[1404] V. C. Mavron, T. P. McDonough, and M. S. Shrikhande. On quasi-symmetric designs with intersection difference three. *Designs, Codes, and Cryptography*, 63(1):73–86, April 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=63&issue=1&spage=73`.

**Wang:2012:EFC**

[1405] Liping Wang and Qiang Wang. On explicit factors of cyclotomic polynomials over finite fields. *Designs, Codes, and Cryptography*, 63(1):87–104, April 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=63&issue=1&spage=87.

**Kiah:2012:NCC**

[1406] Han Mao Kiah, Ka Hin Leung, and San Ling. A note on cyclic codes over $\mathrm{GR}(p^2, m)$ of length $p^k$. *Designs, Codes, and Cryptography*, 63(1):105–112, April 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=63&issue=1&spage=105.

**Dougherty:2012:CCR**

[1407] Steven T. Dougherty, Suat Karadeniz, and Bahattin Yildiz. Cyclic codes over $\mathrm{R}_k$. *Designs, Codes, and Cryptography*, 63(1):113–126, April 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=63&issue=1&spage=113.

**Csirmaz:2012:LSS**

[1408] László Csirmaz and Gábor Tardos. On-line secret sharing. *Designs, Codes, and Cryptography*, 63(1):127–147, April 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=63&issue=1&spage=127.

**Aggarwal:2012:CST**

[1409] Manohar L. Aggarwal, Andreas Klein, and Leo Storme. The characterisation of the smallest two fold blocking sets in $\mathrm{PG}(n, 2)$. *Designs, Codes, and Cryptography*, 63(2):149–157, May 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=63&issue=2&spage=149.

**DeBeule:2012:CRP**

[1410] J. De Beule, A. Hallez, and L. Storme. A characterisation result on a particular class of non-weighted minihypers. *Designs, Codes, and Cryptography*, 63(2):159–170, May 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=63&issue=2&spage=159.

**DeBoeck:2012:SWC**

[1411] M. De Boeck. Small weight codewords in the dual code of points and hyperplanes in $\mathrm{PG}(n, q)$, $q$ even. *Designs, Codes, and Cryptography*, 63(2):171–182, May 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=63&issue=2&spage=171.

**Hou:2012:CSD**

[1412] Xiang-Dong Hou. Classification of self dual quadratic bent functions. *Designs, Codes, and Cryptography*, 63 (2):183–198, May 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=63&issue=2&spage=183.

**Kurosawa:2012:REP**

[1413] Kaoru Kurosawa. Round-efficient perfectly secure message transmission scheme against general adversary. *Designs, Codes, and Cryptography*, 63 (2):199–207, May 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=63&issue=2&spage=199.

**Zhang:2012:CCC**

[1414] Aixian Zhang and Keqin Feng. Construction of cyclotomic codebooks nearly meeting the Welch bound. *Designs, Codes, and Cryptography*, 63 (2):209–224, May 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=63&issue=2&spage=209.

**Stankovski:2012:IDH**

[1415] Paul Stankovski, Sushmita Ruj, Martin Hell, and Thomas Johansson. Improved distinguishers for HC-128. *Designs, Codes, and Cryptography*, 63 (2):225–240, May 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=63&issue=2&spage=225.

**Smith:2012:NTP**

[1416] Derek H. Smith and Roberto Montemanni. A new table of permutation codes. *Designs, Codes, and Cryptography*, 63(2):241–253, May 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=63&issue=2&spage=241.

**Farras:2012:OBS**

[1417] Oriol Farràs, Jessica Ruth Metcalf-Burton, Carles Padró, and Leonor Vázquez. On the optimization of bipartite secret sharing schemes. *Designs, Codes, and Cryptography*, 63 (2):255–271, May 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=63&issue=2&spage=255.

**Cusick:2012:AER**

[1418] Thomas W. Cusick and Younhwan Cheon. Affine equivalence for rotation symmetric Boolean functions with $2^k$ variables. *Designs, Codes, and Cryptography*, 63(2):273–294, May 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=63&issue=2&spage=273.

**Hyun:2012:MDG**

[1419] Jong Yoon Hyun, Heisook Lee, and Yoonjin Lee. MacWilliams duality and a Gleason-type theorem on self-dual bent functions. *Designs, Codes, and Cryptography*, 63(3):295–304, June 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=63&issue=3&spage=295`.

**Wang:2012:SGR**

[1420] Kun Wang and Jianmin Wang. Semi-cyclic 4-GDDs and related two-dimensional optical orthogonal codes. *Designs, Codes, and Cryptography*, 63(3):305–319, June 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=63&issue=3&spage=305`.

**Jurrius:2012:WEC**

[1421] Relinde P. M. J. Jurrius. Weight enumeration of codes from finite spaces. *Designs, Codes, and Cryptography*, 63(3):321–330, June 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=63&issue=3&spage=321`.

**Hu:2012:IDG**

[1422] Zhi Hu, Patrick Longa, and Maozhi Xu. Implementing the 4-dimensional GLV method on GLS elliptic curves with $j$-invariant 0. *Designs, Codes, and Cryptography*, 63(3):331–343, June 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=63&issue=3&spage=331`.

**Silvesan:2012:CBD**

[1423] Daniela Silvesan and Nabil Shalaby. Cyclic block designs with block size 3 from Skolem-type sequences. *Designs, Codes, and Cryptography*, 63 (3):345–355, June 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=63&issue=3&spage=345`.

**Huang:2012:TCO**

[1424] Yuemei Huang and Yanxun Chang. Two classes of optimal two-dimensional OOCs. *Designs, Codes, and Cryptography*, 63(3):357–363, June 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=63&issue=3&spage=357`.

**Ballico:2012:SCC**

[1425] E. Ballico. Scroll codes over curves of higher genus: reducible and superstable vector bundles. *Designs, Codes, and Cryptography*, 63(3):365–377, June 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=63&issue=3&spage=365`.

**Simone:2012:APT**

[1426] Antonino Simone and Boris Skorić. Accusation probabilities in Tardos codes: beyond the Gaussian approximation. *Designs, Codes, and Cryptography*, 63(3):379–412, June 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=63&issue=3&spage=379`.

**Weng:2012:FRP**

[1427] Guobiao Weng and Xiangyong Zeng. Further results on planar DO functions and commutative semifields. *Designs, Codes, and Cryptography*, 63 (3):413–423, June 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=63&issue=3&spage=413`.

**Panario:2012:DPF**

[1428] Daniel Panario, Olga Sosnovski, Brett Stevens, and Qiang Wang. Divisibility of polynomials over finite fields and combinatorial applications. *Designs, Codes, and Cryptography*, 63 (3):425–445, June 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=63&issue=3&spage=425`.

**Bonisoli:2012:PGC**

[1429] Arrigo Bonisoli, James Hirschfeld, and Spyros Magliveras. Preface: geometry, combinatorial designs and cryptology. *Designs, Codes, and Cryptography*, 64(1–2):1–2, July 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=64&issue=1&spage=1`.

**Korchmaros:2012:PAL**

[1430] Gábor Korchmáros, Valentino Lanzone, and Angelo Sonnino. Projective $k$-arcs and 2-level secret-sharing schemes. *Designs, Codes, and Cryptography*, 64(1–2):3–15, July 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=64&issue=1&spage=3`.

**DeClerck:2012:SAM**

[1431] Frank De Clerck, Stefaan De Winter, and Thomas Maes. Singer 8-arcs of Mathon type in $\mathrm{PG}(2, 2^7)$. *Designs, Codes, and Cryptography*, 64(1–2):17–31, July 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=64&issue=1&spage=17`.

**Indaco:2012:APL**

[1432] Lucia Indaco and Gábor Korchmáros. 42-arcs in $\mathrm{PG}(2, q)$ left invariant by $\mathrm{PSL}(2, 7)$. *Designs, Codes, and Cryptography*, 64(1–2):33–46, July 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=64&issue=1&spage=33`.

**Cardinali:2012:TFR**

[1433] Ilaria Cardinali and Antonio Pasini. Two forms related to the symplectic dual polar space in odd characteristic. *Designs, Codes, and Cryptography*, 64(1–2):47–60, July 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=64&issue=1&spage=47`.

**Temmermans:2012:CPS**

[1434] B. Temmermans, J. A. Thas, and H. Van Maldeghem. Collineations of polar spaces with restricted displacements. *Designs, Codes, and Cryptography*, 64(1–2):61–80, July 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=64&issue=1&spage=61`.

**DeBruyn:2012:DUE**

[1435] Bart De Bruyn. A decomposition of the universal embedding space for the near polygon $\mathbf{H}_n$. *Designs, Codes, and Cryptography*, 64 (1–2):81–91, July 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=64&issue=1&spage=81`.

**Payne:2012:ESD**

[1436] S. E. Payne and J. A. Thas. An essay on self-dual generalized quadrangles. *Designs, Codes, and Cryptography*, 64 (1–2):93–103, July 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=64&issue=1&spage=93`.

**Cara:2012:QIG**

[1437] Philippe Cara, Alice Devillers, Michael Giudici, and Cheryl E. Praeger. Quotients of incidence geometries. *Designs, Codes, and Cryptography*, 64 (1–2):105–128, July 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=64&issue=1&spage=105`.

**Georgiou:2012:SDC**

[1438] S. D. Georgiou and E. Lappas. Self-dual codes from circulant matrices. *Designs, Codes, and Cryptography*, 64 (1–2):129–141, July 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=64&issue=1&spage=129`.

**Leung:2012:NRP**

[1439] Ka Hin Leung and Bernhard Schmidt. New restrictions on possible orders of circulant Hadamard matrices. *Designs, Codes, and Cryptography*, 64 (1–2):143–151, July 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=64&issue=1&spage=143`.

**Abreu:2012:IPF**

[1440] Marién Abreu, Domenico Labbate, and John Sheehan. Irreducible

pseudo 2-factor isomorphic cubic bipartite graphs. *Designs, Codes, and Cryptography*, 64(1–2):153–160, July 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=64&issue=1&spage=153.

**Muniz:2012:SMA**

[1441] Madeline González Muñiz and Rainer Steinwandt. Security of message authentication codes in the presence of key-dependent messages. *Designs, Codes, and Cryptography*, 64 (1–2):161–169, July 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=64&issue=1&spage=161.

**Blackburn:2012:CHA**

[1442] Simon R. Blackburn, Douglas R. Stinson, and Jalaj Upadhyay. On the complexity of the herding attack and some related attacks on hash functions. *Designs, Codes, and Cryptography*, 64 (1–2):171–193, July 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=64&issue=1&spage=171.

**Steinwandt:2012:IBN**

[1443] Rainer Steinwandt and Adriana Suárez Corona. Identity-based non-interactive key distribution with forward security. *Designs, Codes, and Cryptography*, 64 (1–2):195–208, July 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=64&issue=1&spage=195. See comment [1787].

**Marquardt:2012:PNG**

[1444] Pascal Marquardt, Pavol Svaba, and Tran van Trung. Pseudorandom number generators based on random covers for finite groups. *Designs, Codes, and Cryptography*, 64 (1–2):209–220, July 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=64&issue=1&spage=209.

**Grosek:2012:QFA**

[1445] Otokar Grosek and Peter Horák. On quasigroups with few associative triples. *Designs, Codes, and Cryptography*, 64(1–2):221–227, July 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=64&issue=1&spage=221.

**Cao:2012:RSC**

[1446] Xiwang Cao and Lei Hu. On the reducibility of some composite polynomials over finite fields. *Designs, Codes, and Cryptography*, 64(3):229–239, September 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=64&issue=3&spage=229.

**Fu:2012:CHN**

[1447] Shaojing Fu, Kanta Matsuura, Chao Li, and Longjiang Qu. Construction of highly nonlinear resilient S-boxes with given degree. *Designs, Codes, and Cryptography*, 64(3):241–253, September 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=64&issue=3&spage=241`.

**Pun:2012:GPT**

[1448] Anna Y. Pun and Philip P. W. Wong. A geometric proof of a theorem on antiregularity of generalized quadrangles. *Designs, Codes, and Cryptography*, 64 (3):255–263, September 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=64&issue=3&spage=255`.

**Heden:2012:ESS**

[1449] Olof Heden, Juliane Lehmann, Esmeralda Nastase, and Papa Sissokho. Extremal sizes of subspace partitions. *Designs, Codes, and Cryptography*, 64(3): 265–274, September 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=64&issue=3&spage=265`.

**Krotov:2012:BCP**

[1450] Denis S. Krotov. On the binary codes with parameters of triply-shortened 1-perfect codes. *Designs, Codes, and Cryptography*, 64(3):275–283, September 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=64&issue=3&spage=275`.

**Zhou:2012:CCE**

[1451] Jianqin Zhou. A counterexample concerning the 3-error linear complexity of $2^n$-periodic binary sequences. *Designs, Codes, and Cryptography*, 64(3): 285–286, September 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=64&issue=3&spage=285`.

**Sajadieh:2012:CIM**

[1452] Mahdi Sajadieh, Mohammad Dakhilalian, Hamid Mala, and Behnaz Omoomi. On construction of involutory MDS matrices from Vandermonde Matrices in GF($2^q$). *Designs, Codes, and Cryptography*, 64(3): 287–308, September 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=64&issue=3&spage=287`.

**Cossidente:2012:HHP**

[1453] Antonio Cossidente and Giuseppe Marino. Hyperovals of Hermitian polar spaces. *Designs, Codes, and Cryptography*, 64(3):309–314, September 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.`

asp?genre=article&issn=0925-1022&volume=64&issue=3&spage=309.

**vanDam:2012:PGA**

[1454] Edwin R. van Dam and Willem H. Haemers. Preface: Geometric and algebraic combinatorics. *Designs, Codes, and Cryptography*, 65(1–2): 1–3, October 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=65&issue=1&spage=1.

**Ball:2012:SVF**

[1455] Simeon Ball and Jan De Beule. On sets of vectors of a finite vector space in which every subset of basis size is a basis II. *Designs, Codes, and Cryptography*, 65(1–2):5–14, October 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=65&issue=1&spage=5.

**Jungnickel:2012:HTC**

[1456] Dieter Jungnickel and Vladimir D. Tonchev. A Hamada type characterization of the classical geometric designs. *Designs, Codes, and Cryptography*, 65 (1–2):15–28, October 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=65&issue=1&spage=15.

**Jurisic:2012:ECD**

[1457] Aleksandar Jurisić and Janos Vidali. Extremal 1-codes in distance-regular graphs of diameter 3. *Designs, Codes, and Cryptography*, 65 (1–2):29–47, October 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=65&issue=1&spage=29.

**Gavrilyuk:2012:DRG**

[1458] Alexander L. Gavrilyuk and Alexander A. Makhnev. Distance-regular graphs with intersection arrays $\{52, 35, 16; 1, 4, 28\}$ and $\{69, 48, 24; 1, 4, 46\}$ do not exist. *Designs, Codes, and Cryptography*, 65 (1–2):49–54, October 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=65&issue=1&spage=49.

**Koolen:2012:RBD**

[1459] Jack H. Koolen and Jongyook Park. A relationship between the diameter and the intersection number $c_2$ for a distance-regular graph. *Designs, Codes, and Cryptography*, 65 (1–2):55–63, October 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=65&issue=1&spage=55.

**Blokhuis:2012:SCG**

[1460] A. Blokhuis and A. E. Brouwer. Spectral characterization of a graph on the flags of the eleven point biplane. *Designs, Codes, and Cryptography*, 65 (1–2):65–69, October 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http:

//www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=65&issue=1&spage=65.

**Blokhuis:2012:GS**

[1461] Aart Blokhuis, Andries E. Brouwer, and Willem H. Haemers. The graph with spectrum $14^1 2^{40} (-4)^{10} (-6)^9$. *Designs, Codes, and Cryptography*, 65 (1–2):71–75, October 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=65&issue=1&spage=71.

**Yu:2012:LPS**

[1462] Hyonju Yu. On the limit points of the smallest eigenvalues of regular graphs. *Designs, Codes, and Cryptography*, 65 (1–2):77–88, October 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=65&issue=1&spage=77.

**Kurihara:2012:ETS**

[1463] Hirotake Kurihara. An excess theorem for spherical 2-designs. *Designs, Codes, and Cryptography*, 65 (1–2):89–98, October 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=65&issue=1&spage=89.

**Ikuta:2012:NAN**

[1464] Takuya Ikuta and Akihiro Munemasa. Nomura algebras of non-symmetric Hadamard models. *Designs, Codes, and Cryptography*, 65 (1–2):99–106, October 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=65&issue=1&spage=99.

**Brouwer:2012:GRS**

[1465] Andries Brouwer and Çiçek Güven. The generating rank of the space of short vectors in the Leech lattice mod 2. *Designs, Codes, and Cryptography*, 65(1–2):107–113, October 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=65&issue=1&spage=107.

**VanMaldeghem:2012:SPB**

[1466] Hendrik Van Maldeghem. Symplectic polarities of buildings of type $E_6$. *Designs, Codes, and Cryptography*, 65 (1–2):115–125, October 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=65&issue=1&spage=115.

**DeBruyn:2012:PHH**

[1467] Bart De Bruyn. The pseudo-hyperplanes and homogeneous pseudo-embeddings of $\mathrm{AG}(n, 4)$ and $\mathrm{PG}(n, 4)$. *Designs, Codes, and Cryptography*, 65 (1–2):127–156, October 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=65&issue=1&spage=127.

**Kantor:2012:PWE**

[1468] William M. Kantor and Tim Penttila. Planes in which every quadrangle lies on a unique Baer subplane. *Designs, Codes, and Cryptography*, 65(1–2):157–161, October 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=65&issue=1&spage=157`.

**Arasu:2012:PRM**

[1469] K. T. Arasu, Xiaoyu Liu, and Gary McGuire. Preface: Richard M. Wilson, Special issue honoring his 65th birthday. *Designs, Codes, and Cryptography*, 65(3):163–164, December 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=65&issue=3&spage=163`.

**Butler:2012:NML**

[1470] Steve Butler and Ron Graham. A note on marking lines in $[k]^n$ in honor of Rick Wilson's 65th birthday. *Designs, Codes, and Cryptography*, 65(3):165–175, December 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=65&issue=3&spage=165`.

**Yildiz:2012:LBC**

[1471] Bahattin Yildiz. A lemma on binomial coefficients and applications to Lee weights modulo $2^e$ of codes over $\mathbf{Z}_4$. *Designs, Codes, and Cryptography*, 65(3):177–185, December 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=65&issue=3&spage=177`.

**Blokhuis:2012:CNK**

[1472] A. Blokhuis, A. E. Brouwer, and T. Szőnyi. On the chromatic number of $q$-Kneser graphs. *Designs, Codes, and Cryptography*, 65(3):187–197, December 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=65&issue=3&spage=187`.

**Colbourn:2012:TTP**

[1473] Charles J. Colbourn, Daniel Horsley, and Chengmin Wang. Trails of triples in partial triple systems. *Designs, Codes, and Cryptography*, 65(3):199–212, December 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=65&issue=3&spage=199`.

**Dukes:2012:CI**

[1474] Peter J. Dukes. Coding with injections. *Designs, Codes, and Cryptography*, 65(3):213–222, December 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=65&issue=3&spage=213`.

**Haemers:2012:MOA**

[1475] W. H. Haemers and M. J. P. Peeters. The maximum order of adjacency matrices of graphs with a given rank. *Designs, Codes, and Cryptography*, 65 (3):223–232, December 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=65&issue=3&spage=223`.

**Alon:2012:BET**

[1476] Noga Alon, Keith E. Mellinger, Dhruv Mubayi, and Jacques Verstraëte. The de Bruijn–Erdős theorem for hypergraphs. *Designs, Codes, and Cryptography*, 65(3):233–245, December 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=65&issue=3&spage=233`.

**Feng:2012:PNA**

[1477] Tao Feng, Fan Wu, and Qing Xiang. Pseudocyclic and non-amorphic fusion schemes of the cyclotomic association schemes. *Designs, Codes, and Cryptography*, 65(3): 247–257, December 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=65&issue=3&spage=247`.

**Hoholdt:2012:EEB**

[1478] Tom Høholdt and Heeralal Janwa. Eigenvalues and expansion of bipartite graphs. *Designs, Codes, and Cryptography*, 65(3):259–273, December 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=65&issue=3&spage=259`.

**Hernando:2012:PCS**

[1479] Fernando Hernando and Gary McGuire. Proof of a conjecture of Segre and Bartocci on monomial hyperovals in projective planes. *Designs, Codes, and Cryptography*, 65(3):275–289, December 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=65&issue=3&spage=275`.

**Katz:2012:TDM**

[1480] Daniel J. Katz. On theorems of Delsarte–McEliece and Chevalley–Warning–Ax–Katz. *Designs, Codes, and Cryptography*, 65(3):291–324, December 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=65&issue=3&spage=291`.

**Dinitz:2012:CRP**

[1481] Jeffrey H. Dinitz, Maura B. Paterson, Douglas R. Stinson, and Ruizhong Wei. Constructions for retransmission permutation arrays. *Designs, Codes, and Cryptography*, 65(3):325–351, December 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.`

asp?genre=article&issn=0925-1022&volume=65&issue=3&spage=325.

**Balachandran:2012:FCS**

[1482] Niranjan Balachandran. Forbidden configurations and Steiner designs. *Designs, Codes, and Cryptography*, 65(3): 353–364, December 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=65&issue=3&spage=353.

**Singhi:2012:SDM**

[1483] Navin Singhi and D. K. Ray-Chaudhuri. Studying designs via multisets. *Designs, Codes, and Cryptography*, 65(3):365–381, December 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=65&issue=3&spage=365.

**Baldi:2012:BAH**

[1484] P. Baldi. Boolean autoencoders and hypercube clustering complexity. *Designs, Codes, and Cryptography*, 65(3): 383–403, December 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=65&issue=3&spage=383.

**Augot:2013:E**

[1485] Daniel Augot, Anne Canteaut, and Gohar Kyureghyan. Editorial. *Designs, Codes, and Cryptography*, 66 (1–3):1–2, January 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9731-1; http://link.springer.com/content/pdf/10.1007/s10623-012-9731-1; http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=66&issue=1&spage=1-2.

**Byrne:2013:ADN**

[1486] Eimear Byrne, Marcus Greferath, and Jaume Pernas. Algebraic decoding of negacyclic codes over $\mathbf{Z}_4$. *Designs, Codes, and Cryptography*, 66 (1–3):3–16, January 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9632-3; http://link.springer.com/article/10.1007/s10623-012-9632-3/; http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=66&issue=1&spage=3-16.

**Sole:2013:CSC**

[1487] Patrick Solé and Jean-Claude Belfiore. Constructive spherical codes near the Shannon bound. *Designs, Codes, and Cryptography*, 66(1–3): 17–26, January 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9633-2; http://link.springer.com/article/10.1007/s10623-012-9633-2/; http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=66&issue=1&spage=17-26.

**Honold:2013:NFE**

[1488] Thomas Honold and Ivan Land-

jev. Non-free extensions of the simplex codes over a chain ring with four elements. *Designs, Codes, and Cryptography*, 66(1–3):27–38, January 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9649-7; http://link.springer.com/article/10.1007/s10623-012-9649-7/; http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=66&issue=1&spage=27-38.

**Kiermaier:2013:NRL**

[1489] Michael Kiermaier and Johannes Zwanzger. New ring-linear codes from dualization in projective Hjelmslev geometries. *Designs, Codes, and Cryptography*, 66(1–3):39–55, January 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9650-1; http://link.springer.com/article/10.1007/s10623-012-9650-1/; http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=66&issue=1&spage=39-55.

**Wachter-Zeh:2013:FDG**

[1490] Antonia Wachter-Zeh and Valentin Afanassiev. Fast decoding of Gabidulin codes. *Designs, Codes, and Cryptography*, 66(1–3):57–73, January 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9659-5; http://link.springer.com/article/10.1007/s10623-012-9659-5/; http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=66&issue=1&spage=57-73.

**Bogdanov:2013:GFN**

[1491] Andrey Bogdanov and Kyoji Shibutani. Generalized Feistel networks revisited. *Designs, Codes, and Cryptography*, 66(1–3):75–97, January 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9660-z; http://link.springer.com/article/10.1007/s10623-012-9660-z/; http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=66&issue=1&spage=75-97.

**Pott:2013:CEE**

[1492] Alexander Pott and Yue Zhou. CCZ and EA equivalence between mappings over finite Abelian groups. *Designs, Codes, and Cryptography*, 66 (1–3):99–109, January 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9661-y; http://link.springer.com/article/10.1007/s10623-012-9661-y/; http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=66&issue=1&spage=99-109.

**Schulte-Geers:2013:CEA**

[1493] Ernst Schulte-Geers. On CCZ-equivalence of addition mod$2^n$. *Designs, Codes, and Cryptography*, 66(1–3):111–127, January 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.

1007/s10623-012-9668-4; http://link.springer.com/article/10.1007/s10623-012-9668-4/; http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=66&issue=1&spage=111-127.

**Bassalygo:2013:DES**

[1494] L. A. Bassalygo and V. A. Zinoviev. On divisibility of exponential sums of polynomials of special type over fields of characteristic 2. *Designs, Codes, and Cryptography*, 66(1–3): 129–143, January 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9669-3; http://link.springer.com/article/10.1007/s10623-012-9669-3/; http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=66&issue=1&spage=129-143.

**Greferath:2013:CIW**

[1495] Marcus Greferath, Cathy Mc Fadden, and Jens Zumbrägel. Characteristics of invariant weights related to code equivalence over rings. *Designs, Codes, and Cryptography*, 66(1–3):145–156, January 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9671-9; http://link.springer.com/article/10.1007/s10623-012-9671-9/; http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=66&issue=1&spage=145-156.

**Sarkar:2013:CRD**

[1496] Santanu Sarkar and Subhamoy Maitra. Cryptanalytic results on 'Dual CRT' and 'Common Prime' RSA. *Designs, Codes, and Cryptography*, 66(1–3):157–174, January 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9675-5; http://link.springer.com/article/10.1007/s10623-012-9675-5/; http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=66&issue=1&spage=157-174.

**Rock:2013:GMA**

[1497] Andrea Röck and Kaisa Nyberg. Generalization of Matsui's Algorithm 1 to linear hull for key-alternating block ciphers. *Designs, Codes, and Cryptography*, 66(1–3): 175–193, January 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9679-1; http://link.springer.com/article/10.1007/s10623-012-9679-1/; http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=66&issue=1&spage=175-193.

**Geil:2013:WRM**

[1498] Olav Geil and Casper Thomsen. Weighted Reed–Muller codes revisited. *Designs, Codes, and Cryptography*, 66 (1–3):195–220, January 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9680-8; http://link.springer.com/article/10.1007/s10623-012-9680-8/; http://www.springerlink.com/openurl.

asp?genre=article&issn=0925-1022&volume=66&issue=1&spage=195-220.

**Beelen:2013:BNP**

[1499] Peter Beelen and Diego Ruano. Bounding the number of points on a curve using a generalization of Weierstrass semigroups. *Designs, Codes, and Cryptography*, 66(1–3): 221–230, January 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9685-3; http://link.springer.com/article/10.1007/s10623-012-9685-3/; http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=66&issue=1&spage=221-230.

**Cesmelioglu:2013:CBF**

[1500] Ayça Çesmelioglu and Wilfried Meidl. A construction of bent functions from plateaued functions. *Designs, Codes, and Cryptography*, 66(1–3): 231–242, January 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9686-2; http://link.springer.com/article/10.1007/s10623-012-9686-2/; http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=66&issue=1&spage=231-242.

**Gangopadhyay:2013:NCB**

[1501] Sugata Gangopadhyay, Anand Joshi, and Gregor Leander. A new construction of bent functions based on **Z**-bent functions. *Designs, Codes, and Cryptography*, 66(1–3): 243–256, January 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9687-1; http://link.springer.com/article/10.1007/s10623-012-9687-1/; http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=66&issue=1&spage=243-256.

**Meidl:2013:QFP**

[1502] Wilfried Meidl and Alev Topuzoglu. Quadratic functions with prescribed spectra. *Designs, Codes, and Cryptography*, 66(1–3):257–273, January 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9690-6; http://link.springer.com/article/10.1007/s10623-012-9690-6/; http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=66&issue=1&spage=257-273.

**Rosenthal:2013:CCI**

[1503] Joachim Rosenthal and Anna-Lena Trautmann. A complete characterization of irreducible cyclic orbit codes and their Plücker embedding. *Designs, Codes, and Cryptography*, 66(1–3):275–289, January 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9691-5; http://link.springer.com/article/10.1007/s10623-012-9691-5/; http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=66&issue=1&spage=275-289.

**Couvreur:2013:ECS**

[1504] Alain Couvreur and Iwan Duursma. Evaluation codes from smooth quadric surfaces and twisted Segrè varieties. *Designs, Codes, and Cryptography*, 66 (1–3):291–303, January 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9692-4; http://link.springer.com/article/10.1007/s10623-012-9692-4/; http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=66&issue=1&spage=291-303`.

**Gao:2013:MPK**

[1505] Shuhong Gao and Raymond Heindl. Multivariate public key cryptosystems from Diophantine equations. *Designs, Codes, and Cryptography*, 67 (1):1–18, April 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-011-9582-1; http://link.springer.com/article/10.1007/s10623-011-9582-1/; http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=67&issue=1&spage=1-18`.

**Li:2013:FQS**

[1506] Jie Li, Xiangyong Zeng, Xiaohu Tang, and Chunlei Li. A family of quadriphase sequences of period $4(2^n - 1)$ with low correlation and large linear span. *Designs, Codes, and Cryptography*, 67(1):19–35, April 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-011-9583-0; http://link.springer.com/article/10.1007/s10623-011-9583-0/; http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=67&issue=1&spage=19-35`.

**Yamada:2013:DSG**

[1507] Mieko Yamada. Difference sets over Galois rings with odd extension degrees and characteristic an even power of 2. *Designs, Codes, and Cryptography*, 67(1):37–57, April 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-011-9584-z; http://link.springer.com/article/10.1007/s10623-011-9584-z/; http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=67&issue=1&spage=37-57`.

**Cao:2013:CQC**

[1508] Yonglin Cao and Jian Gao. Constructing quasi-cyclic codes from linear algebra theory. *Designs, Codes, and Cryptography*, 67(1):59–75, April 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-011-9586-x; http://link.springer.com/article/10.1007/s10623-011-9586-x/; http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=67&issue=1&spage=59-75`.

**Tang:2013:CBB**

[1509] Deng Tang, Weiguo Zhang, and Xiaohu Tang. Construction of balanced Boolean functions with high nonlinearity and good autocorrelation proper-

ties. *Designs, Codes, and Cryptography*, 67(1):77–91, April 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-011-9587-9; http://link.springer.com/article/10.1007/s10623-011-9587-9/; http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=67&issue=1&spage=77-91.

**Leemans:2013:BCS**

[1510] Dimitri Leemans and B. G. Rodrigues. Binary codes of some strongly regular subgraphs of the McLaughlin graph. *Designs, Codes, and Cryptography*, 67(1):93–109, April 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-011-9589-7; http://link.springer.com/article/10.1007/s10623-011-9589-7/; http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=67&issue=1&spage=93-109.

**Bose:2013:KPS**

[1511] Mausumi Bose, Aloke Dey, and Rahul Mukerjee. Key predistribution schemes for distributed sensor networks via block designs. *Designs, Codes, and Cryptography*, 67(1):111–136, April 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-011-9590-1; http://link.springer.com/article/10.1007/s10623-011-9590-1/; http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=67&issue=1&spage=111-136.

**Bamberg:2013:HSF**

[1512] John Bamberg, Michael Giudici, and Gordon F. Royle. Hemisystems of small flock generalized quadrangles. *Designs, Codes, and Cryptography*, 67(1):137–157, April 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-011-9591-0; http://link.springer.com/article/10.1007/s10623-011-9591-0/; http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=67&issue=1&spage=137-157.

**Ghinelli:2013:ODR**

[1513] Dina Ghinelli, J. W. P. Hirschfeld, and Dieter Jungnickel. Obituary: Daniel R. Hughes (1927–2012). *Designs, Codes, and Cryptography*, 67(2):159–162, May 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9798-3.

**Ghinelli:2013:OMJ**

[1514] Dina Ghinelli and Dieter Jungnickel. Obituary: Marialuisa J. de Resmini (1939–2012). *Designs, Codes, and Cryptography*, 67(2):163–167, May 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9799-2.

**Gharahi:2013:CGA**

[1515] Motahhareh Gharahi and Massoud Hadian Dehkordi. The complexity of

the graph access structures on six participants. *Designs, Codes, and Cryptography*, 67(2):169–173, May 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-011-9592-z`.

**Chen:2013:AER**

[1516] Huajin Chen, Tian Tian, and Wenfeng Qi. On the affine equivalence relation between two classes of Boolean functions with optimal algebraic immunity. *Designs, Codes, and Cryptography*, 67(2):175–185, May 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-011-9596-8`.

**Ozen:2013:MSW**

[1517] Ibrahim Özen and Eda Tekin. Moments of the support weight distribution of linear codes. *Designs, Codes, and Cryptography*, 67(2):187–196, May 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-011-9597-7`.

**Zhang:2013:SEC**

[1518] Fangguo Zhang and Ping Wang. Speeding up elliptic curve discrete logarithm computations with point halving. *Designs, Codes, and Cryptography*, 67(2):197–208, May 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-011-9599-5`.

**Armknecht:2013:GHE**

[1519] Frederik Armknecht, Stefan Katzenbeisser, and Andreas Peter. Group homomorphic encryption: characterizations, impossibility results, and applications. *Designs, Codes, and Cryptography*, 67(2):209–232, May 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-011-9601-2`.

**Wang:2013:FRE**

[1520] Kun Wang and Jianxing Yin. Further results on the existence of nested orthogonal arrays. *Designs, Codes, and Cryptography*, 67(2):233–243, May 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-011-9603-0`.

**Goldberg:2013:AOW**

[1521] Ian Goldberg, Douglas Stebila, and Berkant Ustaoglu. Anonymity and one-way authentication in key exchange protocols. *Designs, Codes, and Cryptography*, 67(2):245–269, May 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-011-9604-z`.

**Hong:2013:SEF**

[1522] Hoon Hong, Eunjeong Lee, Hyang-Sook Lee, and Cheol-Min Park. Simple and exact formula for minimum loop length in ate$_i$ pairing based on Brezing–Weng curves. *Designs, Codes, and Cryptography*, 67(2):271–292, May

2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-011-9605-y.

**Nagata:2013:MFS**

[1523] Kiyoshi Nagata, Fidel Nemenzo, and Hideo Wada. Mass formula and structure of self-dual codes over Z2s $\mathbf{Z}_{2^s}$. *Designs, Codes, and Cryptography*, 67(3):293–316, June 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-011-9606-x.

**Chen:2013:LCB**

[1524] Zhixiong Chen and Xiaoni Du. On the linear complexity of binary threshold sequences derived from Fermat quotients. *Designs, Codes, and Cryptography*, 67(3):317–323, June 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9608-3.

**Ke:2013:LCA**

[1525] Pinhui Ke, Jie Zhang, and Shengyuan Zhang. On the linear complexity and the autocorrelation of generalized cyclotomic binary sequences of length $2p^m$. *Designs, Codes, and Cryptography*, 67(3):325–339, June 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9610-9.

**Lauter:2013:GPF**

[1526] Kristin Lauter and Ning Shang. Generating pairing-friendly parameters for the CM construction of genus 2 curves over prime fields. *Designs, Codes, and Cryptography*, 67(3):341–355, June 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9611-8.

**Dunkelman:2013:CSC**

[1527] Orr Dunkelman and Nathan Keller. Cryptanalysis of the stream cipher LEX. *Designs, Codes, and Cryptography*, 67(3):357–373, June 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9612-7.

**Giuzzi:2013:FTT**

[1528] Luca Giuzzi and Valentina Pepe. Families of twisted tensor product codes. *Designs, Codes, and Cryptography*, 67(3):375–384, June 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9613-6.

**Gillespie:2013:NTC**

[1529] Neil I. Gillespie and Cheryl E. Praeger. Neighbour transitivity on codes in Hamming graphs. *Designs, Codes, and Cryptography*, 67(3):385–393, June 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9614-5.

**Gutierrez:2013:PML**

[1530] Jaime Gutierrez, Álvar Ibeas, Domingo Gómez-Pérez, and Igor E. Shparlinski. Predicting masked linear pseudorandom number generators over finite fields. *Designs, Codes, and Cryptography*, 67(3):395–402, June 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9615-4.

**Ghinelli:2013:EFG**

[1531] D. Ghinelli, J. W. P. Hirschfeld, D. Jungnickel, and J. A. Thas. Editorial: Finite geometries. *Designs, Codes, and Cryptography*, 68 (1–3):1–2, July 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-012-9781-4?coverImageUrl=/static-content%2Fcovers%2Fjournals_single_issue%2F612%2F10623_068_001.jpg; http://link.springer.com/article/10.1007/s10623-012-9781-4.

**DeBeule:2013:LMP**

[1532] Jan De Beule. On large maximal partial ovoids of the parabolic quadric $Q(4, q)$. *Designs, Codes, and Cryptography*, 68(1–3):3–10, July 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9629-y.

**Beukemann:2013:STS**

[1533] L. Beukemann and K. Metsch. Small tight sets of hyperbolic quadrics. *Designs, Codes, and Cryptography*, 68 (1–3):11–24, July 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9676-4.

**Sziklai:2013:SMB**

[1534] Peter Sziklai and Geertrui Van de Voorde. A small minimal blocking set in $\mathrm{PG}(n, p^t)$, spanning a $(t-1)$-space, is linear. *Designs, Codes, and Cryptography*, 68(1–3):25–32, July 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9751-x.

**Rodgers:2013:CLL**

[1535] Morgan Rodgers. Cameron–Liebler line classes. *Designs, Codes, and Cryptography*, 68(1–3):33–37, July 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-011-9581-2.

**Glynn:2013:PFV**

[1536] David G. Glynn. Permanent formulae from the Veronesean. *Designs, Codes, and Cryptography*, 68(1–3):39–47, July 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9618-1.

**Betten:2013:TFM**

[1537] Anton Betten, Eun Ju Cheon, Seon Jeong Kim, and Tatsuya Maruta. Three families of multiple blocking sets in Desarguesian projective planes of even order. *Designs, Codes, and Cryptography*, 68(1–3):49–59, July

2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9634-1.

**Giulietti:2013:AAD**

[1538] Massimo Giulietti and Gábor Korchmáros. Arcs in AG$(2, q)$ determining few directions. *Designs, Codes, and Cryptography*, 68(1–3):61–72, July 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9630-5.

**Giulietti:2013:TIA**

[1539] Massimo Giulietti, Gábor Korchmáros, Stefano Marcugini, and Fernanda Pambianco. Transitive $A_6$-invariant $k$-arcs in PG$(2, q)$. *Designs, Codes, and Cryptography*, 68(1–3):73–79, July 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9619-0.

**Dempwolff:2013:MTP**

[1540] Ulrich Dempwolff. More translation planes and semifields from Dembowski–Ostrom polynomials. *Designs, Codes, and Cryptography*, 68(1–3):81–103, July 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9709-z.

**Honold:2013:EMA**

[1541] Thomas Honold and Michael Kiermaier. The existence of maximal $(q^2, 2)$-arcs in projective Hjelmslev planes over chain rings of length 2 and odd prime characteristic. *Designs, Codes, and Cryptography*, 68 (1–3):105–126, July 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9653-y.

**Amarra:2013:SDT**

[1542] Carmen Amarra, Michael Giudici, and Cheryl E. Praeger. Symmetric diameter two graphs with affine-type vertex-quasiprimitive automorphism group. *Designs, Codes, and Cryptography*, 68 (1–3):127–139, July 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9644-z.

**Chen:2013:ANA**

[1543] Yu Qing Chen and Tao Feng. Abelian and non-abelian Paley type group schemes. *Designs, Codes, and Cryptography*, 68(1–3):141–154, July 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9640-3.

**Polhill:2013:NPC**

[1544] John Polhill, James A. Davis, and Ken Smith. A new product construction for partial difference sets. *Designs, Codes, and Cryptography*, 68 (1–3):155–161, July 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9616-3.

**Jungnickel:2013:NII**

[1545] Dieter Jungnickel and Vladimir D. Tonchev. New invariants for incidence structures. *Designs, Codes, and Cryptography*, 68(1–3):163–177, July 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9636-z.

**Coolsaet:2013:CNH**

[1546] Kris Coolsaet. On the classification of nonsingular $2 \times 2 \times 2 \times 2$ hypercubes. *Designs, Codes, and Cryptography*, 68 (1–3):179–194, July 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9737-8.

**Glynn:2013:NNH**

[1547] David G. Glynn. Nonfactorizable nonsingular hypercubes. *Designs, Codes, and Cryptography*, 68(1–3):195–203, July 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-011-9585-y.

**Lavrauw:2013:FSN**

[1548] Michel Lavrauw. Finite semifields and nonsingular tensors. *Designs, Codes, and Cryptography*, 68(1–3):205–227, July 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9710-6.

**Cardinali:2013:CFQ**

[1549] Ilaria Cardinali and Antonio Pasini. On certain forms and quadrics related to symplectic dual polar spaces in characteristic 2. *Designs, Codes, and Cryptography*, 68(1–3):229–258, July 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-011-9602-1.

**Bruyn:2013:PHH**

[1550] Bart De Bruyn. The pseudo-hyperplanes and homogeneous pseudo-embeddings of the generalized quadrangles of order $(3, t)$. *Designs, Codes, and Cryptography*, 68(1–3):259–284, July 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9705-3.

**Bettale:2013:CHM**

[1551] Luk Bettale, Jean-Charles Faugère, and Ludovic Perret. Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic. *Designs, Codes, and Cryptography*, 69 (1):1–52, October 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9617-2.

**Chen:2013:TSO**

[1552] Gang Chen and Ruihu Li. Ternary self-orthogonal codes of dual distance three and ternary quantum codes of distance three. *Designs, Codes, and Cryptography*, 69(1):53–63, October 2013. CODEN DCCREC. ISSN

0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9620-7.

**Zhang:2013:NEP**

[1553] Xiande Zhang and Gennian Ge. A new existence proof for Steiner quadruple systems. *Designs, Codes, and Cryptography*, 69(1):65–76, October 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9621-6.

**Stanica:2013:BGB**

[1554] Pantelimon Stănică, Thor Martinsen, Sugata Gangopadhyay, and Brajesh Kumar Singh. Bent and generalized bent Boolean functions. *Designs, Codes, and Cryptography*, 69(1):77–94, October 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9622-5.

**Smith:2013:PCS**

[1555] Derek H. Smith and Roberto Montemanni. Permutation codes with specified packing radius. *Designs, Codes, and Cryptography*, 69(1):95–106, October 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9623-4.

**Mateer:2013:SAD**

[1556] Todd D. Mateer. Simple algorithms for decoding systematic Reed–Solomon codes. *Designs, Codes, and Cryptography*, 69(1):107–121, October 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9626-1.

**Munuera:2013:GHC**

[1557] C. Munuera, A. Sepúlveda, and F. Torres. Generalized Hermitian codes. *Designs, Codes, and Cryptography*, 69(1):123–130, October 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9627-0.

**Hernando:2013:DSS**

[1558] Fernando Hernando, Kyle Marshall, and Michael E. O'Sullivan. The dimension of subcode-subfields of shortened generalized Reed–Solomon codes. *Designs, Codes, and Cryptography*, 69(1):131–142, October 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9628-z.

**Lunardon:2013:RSS**

[1559] G. Lunardon, G. Marino, O. Polverino, and R. Trombetti. A remark on symplectic semifield planes and $Z_4$-linear codes. *Designs, Codes, and Cryptography*, 69(2):143–149, November 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9631-4.

**Yankov:2013:NOS**

[1560] Nikolay Yankov. New optimal $[52, 26, 10]$ self-dual codes. *Designs,*

*Codes, and Cryptography*, 69(2):151–159, November 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9639-9`.

**Martinez-Moro:2013:ASM**

[1561] E. Martínez-Moro, A. Piñera-Nicolás, and I. F. Rúa. Additive semisimple multivariable codes over $\mathbf{f}_4$. *Designs, Codes, and Cryptography*, 69(2):161–180, November 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9641-2`.

**Gravier:2013:NRV**

[1562] Sylvain Gravier, Matjaz Kovse, Michel Mollard, Julien Moncel, and Aline Parreau. New results on variants of covering codes in Sierpiński graphs. *Designs, Codes, and Cryptography*, 69(2):181–188, November 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9642-1`.

**Abel:2013:GSG**

[1563] R. Julian R. Abel, Diana Combe, Adrian M. Nelson, and William D. Palmer. GBRDs over supersolvable groups and solvable groups of order prime to 3. *Designs, Codes, and Cryptography*, 69(2):189–201, November 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9646-x`.

**Tuxanidy:2013:CPF**

[1564] Aleksandr Tuxanidy and Qiang Wang. Composed products and factors of cyclotomic polynomials over finite fields. *Designs, Codes, and Cryptography*, 69(2):203–231, November 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9647-9`.

**Hu:2013:GPC**

[1565] Liqin Hu and Qin Yue. Gauss periods and codebooks from generalized cyclotomic sets of order four. *Designs, Codes, and Cryptography*, 69(2):233–246, November 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9648-8`.

**Liu:2013:NFH**

[1566] Fang Liu, Daiyuan Peng, Zhengchun Zhou, and Xiaohu Tang. A new frequency-hopping sequence set based upon generalized cyclotomy. *Designs, Codes, and Cryptography*, 69(2):247–259, November 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9652-z`.

**Jungnickel:2013:OHL**

[1567] Dieter Jungnickel. Obituary: Hanfried Lenz (1916–2013). *Designs, Codes, and Cryptography*, 69(3):261–263, December 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9869-5`.

**Ma:2013:CBG**

[1568] Tengyu Ma, Xiaoming Sun, and Huacheng Yu. On a conjecture of Butler and Graham. *Designs, Codes, and Cryptography*, 69(3):265–274, December 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9656-8`.

**Zhuang:2013:CCE**

[1569] Zhuojun Zhuang, Yuan Luo, and Bin Dai. Code constructions and existence bounds for relative generalized Hamming weight. *Designs, Codes, and Cryptography*, 69(3):275–297, December 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9657-7`.

**Shimada:2013:NRN**

[1570] Ichiro Shimada. A note on rational normal curves totally tangent to a Hermitian variety. *Designs, Codes, and Cryptography*, 69(3):299–303, December 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9662-x`.

**Heden:2013:SSP**

[1571] O. Heden, J. Lehmann, E. Nastase, and P. Sissokho. The supertail of a subspace partition. *Designs, Codes, and Cryptography*, 69(3):305–316, December 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9664-8`.

**Pillai:2013:AAC**

[1572] N. Rajesh Pillai and S. S. Bedi. Algebraic attacks on a class of stream ciphers with unknown output function. *Designs, Codes, and Cryptography*, 69(3):317–330, December 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9665-7`.

**Bonnecaze:2013:ASC**

[1573] Alexis Bonnecaze, Pierre Liardet, and Alexandre Venelli. AES side-channel countermeasure using random tower field constructions. *Designs, Codes, and Cryptography*, 69(3):331–349, December 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9670-x`.

**Sarkar:2013:NML**

[1574] Palash Sarkar. A new multi-linear universal hash family. *Designs, Codes, and Cryptography*, 69(3):351–367, December 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9672-8`.

**Bazrafshan:2013:IBS**

[1575] Marjan Bazrafshan and Tran van Trung. Improved bounds for separating hash families. *Designs, Codes, and Cryptography*, 69(3):369–382, December 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.`

com/article/10.1007/s10623-012-9673-7.

**Borges:2014:EIC**

[1576] Joaquim Borges, Mercè Villanueva, and Victor Zinoviev. Editorial: 3rd International Castle Meeting on Coding Theory and Applications. *Designs, Codes, and Cryptography*, 70 (1–2):1–2, January 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9775-2; http://link.springer.com/content/pdf/10.1007/s10623-012-9775-2.pdf.

**Auger:2014:SCI**

[1577] David Auger, Gérard Cohen, and Sihem Mesnager. Sphere coverings and identifying codes. *Designs, Codes, and Cryptography*, 70(1–2):3–7, January 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9638-x.

**Kampf:2014:BCD**

[1578] Sabine Kampf. Bounds on collaborative decoding of interleaved Hermitian codes and virtual extension. *Designs, Codes, and Cryptography*, 70 (1–2):9–25, January 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9625-2.

**Seneviratne:2014:CAC**

[1579] Padmapani Seneviratne. Codes associated with circulant graphs and permutation decoding. *Designs, Codes, and Cryptography*, 70(1–2):27–33, January 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9637-y.

**Ghinelli:2014:HCI**

[1580] D. Ghinelli, J. D. Key, and T. P. McDonough. Hulls of codes from incidence matrices of connected regular graphs. *Designs, Codes, and Cryptography*, 70 (1–2):35–54, January 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9635-0.

**Sidorenko:2014:FSF**

[1581] Vladimir Sidorenko and Martin Bossert. Fast skew-feedback shift-register synthesis. *Designs, Codes, and Cryptography*, 70(1–2):55–67, January 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9663-9.

**Malevich:2014:CES**

[1582] Anton Malevich and Wolfgang Willems. On the classification of the extremal self-dual codes over small fields with 2-transitive automorphism groups. *Designs, Codes, and Cryptography*, 70 (1–2):69–76, January 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9655-9.

**Araujo:2014:GLC**

[1583] C. Araujo, I. Dejter, and P. Horak. A generalization of Lee codes. *De-*

*signs, Codes, and Cryptography*, 70 (1–2):77–90, January 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9666-6`.

**Haymaker:2014:GWC**

[1584] Kathryn Haymaker and Christine A. Kelley. Geometric WOM codes and coding strategies for multilevel flash memories. *Designs, Codes, and Cryptography*, 70(1–2):91–104, January 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9681-7`.

**Pernas:2014:CAG**

[1585] Jaume Pernas, Jaume Pujol, and Mercè Villanueva. Characterization of the automorphism group of quaternary linear Hadamard codes. *Designs, Codes, and Cryptography*, 70(1–2):105–115, January 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9678-2`.

**Bras-Amoros:2014:GMB**

[1586] Maria Bras-Amorós and Albert Vico-Oton. On the Geil–Matsumoto bound and the length of AG codes. *Designs, Codes, and Cryptography*, 70(1–2):117–125, January 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9703-5`.

**Feulner:2014:CNR**

[1587] Thomas Feulner. Classification and nonexistence results for linear codes with prescribed minimum distances. *Designs, Codes, and Cryptography*, 70 (1–2):127–138, January 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9700-8`.

**Borges:2014:NFC**

[1588] Joaquim Borges, Josep Rifà, and Victor Zinoviev. New families of completely regular codes and their corresponding distance regular coset graphs. *Designs, Codes, and Cryptography*, 70 (1–2):139–148, January 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9713-3`.

**Tomlinson:2014:NBC**

[1589] M. Tomlinson, M. Jibril, C. Tjhai, M. Grassl, and M. Z. Ahmed. New binary codes from extended Goppa codes. *Designs, Codes, and Cryptography*, 70 (1–2):149–156, January 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9707-1`.

**Pinero:2014:SSH**

[1590] Fernando Piñero and Heeralal Janwa. On the subfield subcodes of Hermitian codes. *Designs, Codes, and Cryptography*, 70(1–2):157–173, January 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.`

com/article/10.1007/s10623-012-9736-9.

**Bernal:2014:ISA**

[1591] José Joaquín Bernal and Juan Jacobo Simón. Information sets in abelian codes: defining sets and Groebner basis. *Designs, Codes, and Cryptography*, 70(1–2):175–188, January 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9735-x.

**Galindo:2014:ECD**

[1592] C. Galindo and F. Monserrat. Evaluation codes defined by finite families of plane valuations at infinity. *Designs, Codes, and Cryptography*, 70(1–2):189–213, January 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9738-7.

**Marquez-Corbella:2014:URV**

[1593] Irene Márquez-Corbella, Edgar Martínez-Moro, and Ruud Pellikaan. On the unique representation of very strong algebraic geometry codes. *Designs, Codes, and Cryptography*, 70(1–2):215–230, January 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9758-3.

**Khan:2014:MNT**

[1594] Eraj Khan, Ernst Gabidulin, Bahram Honary, and Hassan Ahmed. Modified Niederreiter type of GPT cryptosystem based on reducible rank codes. *Designs, Codes, and Cryptography*, 70(1–2):231–239, January 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9757-4.

**Pinho:2014:RCC**

[1595] Telma Pinho, Raquel Pinto, and Paula Rocha. Realization of 2D convolutional codes of rate $\frac{1}{n}$ by separable Roesser models. *Designs, Codes, and Cryptography*, 70(1–2):241–250, January 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9768-1.

**Ideguchi:2014:IDC**

[1596] Kota Ideguchi, Elmar Tischhauser, and Bart Preneel. Internal differential collision attacks on the reduced-round Grøstl-0 hash function. *Designs, Codes, and Cryptography*, 70(3):251–271, March 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9674-6.

**Wu:2014:PTC**

[1597] Junhua Wu. Proofs of two conjectures on the dimensions of binary codes. *Designs, Codes, and Cryptography*, 70(3):273–304, March 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9682-6.

**Choi:2014:LDT**

[1598] Soohak Choi, Jong Yoon Hyun, and Hyun Kwang Kim. Local duality theorem for $q$-ary 1-perfect codes. *De-*

*signs, Codes, and Cryptography*, 70 (3):305–311, March 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9683-5`.

**Lee:2014:EPM**

[1599] Myung-Kyu Lee and Kyeongcheol Yang. The exponent of a polarizing matrix constructed from the Kronecker product. *Designs, Codes, and Cryptography*, 70(3):313–322, March 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9689-z`.

**Herranz:2014:SST**

[1600] Javier Herranz, Alexandre Ruiz, and Germán Sáez. Signcryption schemes with threshold unsigncryption, and applications. *Designs, Codes, and Cryptography*, 70(3):323–345, March 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9688-0`.

**Batoul:2014:SDC**

[1601] Aicha Batoul, Kenza Guenda, and T. Aaron Gulliver. On self-dual cyclic codes over finite chain rings. *Designs, Codes, and Cryptography*, 70 (3):347–358, March 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9696-0`.

**Zheng:2014:DMR**

[1602] Qun-Xiong Zheng, Wen-Feng Qi, and Tian Tian. On the distinctness of modular reductions of primitive sequences over $Z/(2^{32}-1)$. *Designs, Codes, and Cryptography*, 70(3):359–368, March 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9698-y`.

**Bogdanov:2014:LHC**

[1603] Andrey Bogdanov and Vincent Rijmen. Linear hulls with correlation zero and linear cryptanalysis of block ciphers. *Designs, Codes, and Cryptography*, 70 (3):369–383, March 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9697-z`.

**Ozbudak:2014:FNF**

[1604] Ferruh Özbudak and Burcu Gülmez Temür. Finite number of fibre products of Kummer covers and curves with many points over finite fields. *Designs, Codes, and Cryptography*, 70 (3):385–404, March 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9706-2`.

**Boucher:2014:LCU**

[1605] D. Boucher and F. Ulmer. Linear codes using skew polynomials with automorphisms and derivations. *Designs, Codes, and Cryptography*, 70 (3):405–431, March 2014. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9704-4.

**Blokhuis:2014:NSB**

[1606] Aart Blokhuis, Andries E. Brouwer, and Attila Sali. Note on the size of binary Armstrong codes. *Designs, Codes, and Cryptography*, 71(1):1–4, April 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9711-5.

**Lopez:2014:ACC**

[1607] Hiram H. López, Carlos Rentería-Márquez, and Rafael H. Villarreal. Affine cartesian codes. *Designs, Codes, and Cryptography*, 71(1):5–19, April 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9714-2.

**Bartoli:2014:FCD**

[1608] D. Bartoli, M. De Boeck, S. Fanali, and L. Storme. On the functional codes defined by quadrics and Hermitian varieties. *Designs, Codes, and Cryptography*, 71(1):21–46, April 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9712-4.

**Wu:2014:CRS**

[1609] Guangfu Wu, Hsin-Chiu Chang, Lin Wang, and T. K. Truong. Constructing rate $1/p$ systematic binary quasi-cyclic codes based on the matroid theory. *Designs, Codes, and Cryptography*, 71(1):47–56, April 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9715-1.

**Smart:2014:FHS**

[1610] N. P. Smart and F. Vercauteren. Fully homomorphic SIMD operations. *Designs, Codes, and Cryptography*, 71(1):57–81, April 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9720-4.

**Laarhoven:2014:OST**

[1611] Thijs Laarhoven and Benne de Weger. Optimal symmetric Tardos traitor tracing schemes. *Designs, Codes, and Cryptography*, 71(1):83–103, April 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9718-y; http://link.springer.com/content/pdf/10.1007/s10623-012-9718-y.pdf.

**Loidreau:2014:ABC**

[1612] P. Loidreau. Asymptotic behaviour of codes in rank metric over finite fields. *Designs, Codes, and Cryptography*, 71 (1):105–118, April 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9716-0.

**Sharma:2014:SNM**

[1613] Anuradha Sharma and Amit K. Sharma. On some new $m$-spotty Lee weight enumerators. *Designs, Codes, and Cryptography*, 71(1):119–

152, April 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9725-z.

**Arumugam:2014:VCS**

[1614] S. Arumugam, R. Lakshmanan, and Atulya K. Nagar. On ( $k$, n )*-visual cryptography scheme. *Designs, Codes, and Cryptography*, 71 (1):153–162, April 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9722-2.

**Tian:2014:LAS**

[1615] Tian Tian and Wen-Feng Qi. On the largest affine sub-families of a family of NFSR sequences. *Designs, Codes, and Cryptography*, 71(1):163–181, April 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9723-1.

**Su:2014:CRS**

[1616] Sihong Su and Xiaohu Tang. Construction of rotation symmetric Boolean functions with optimal algebraic immunity and high nonlinearity. *Designs, Codes, and Cryptography*, 71 (2):183–199, May 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9727-x.

**Fan:2014:MPC**

[1617] Yun Fan, San Ling, and Hongwei Liu. Matrix product codes over finite commutative Frobenius rings. *Designs, Codes, and Cryptography*, 71 (2):201–227, May 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9726-y.

**Zeh:2014:NBM**

[1618] Alexander Zeh and Sergey Bezzateev. A new bound on the minimum distance of cyclic codes using small-minimum-distance cyclic codes. *Designs, Codes, and Cryptography*, 71(2):229–246, May 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9721-3.

**Nilson:2014:IBS**

[1619] Tomas Nilson and Pia Heidtmann. Inner balance of symmetric designs. *Designs, Codes, and Cryptography*, 71(2):247–260, May 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9730-2.

**Wachter-Zeh:2014:DIR**

[1620] Antonia Wachter-Zeh, Alexander Zeh, and Martin Bossert. Decoding interleaved Reed–Solomon codes beyond their joint error-correcting capability. *Designs, Codes, and Cryptography*, 71(2):261–281, May 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9728-9.

**Dukes:2014:GDD**

[1621] Peter Dukes and Leah Howard. Group divisible designs in MOLS of order

ten. *Designs, Codes, and Cryptography*, 71(2):283–291, May 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9729-8`.

**Sepahi:2014:LBC**

[1622] Reza Sepahi, Ron Steinfeld, and Josef Pieprzyk. Lattice-based completely non-malleable public-key encryption in the standard model. *Designs, Codes, and Cryptography*, 71(2):293–313, May 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9732-0`.

**Dai:2014:CCO**

[1623] Peipei Dai, Jianmin Wang, and Jianxing Yin. Combinatorial constructions for optimal 2-D optical orthogonal codes with AM–OPPTS property. *Designs, Codes, and Cryptography*, 71(2):315–330, May 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9733-z`.

**Zhou:2014:PCG**

[1624] Caixue Zhou, Wan Zhou, and Xiwei Dong. Provable certificateless generalized signcryption scheme. *Designs, Codes, and Cryptography*, 71 (2):331–346, May 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9734-y`.

**Chen:2014:RTB**

[1625] Jie Chen, Hoon Wei Lim, San Ling, and Huaxiong Wang. The relation and transformation between hierarchical inner product encryption and spatial encryption. *Designs, Codes, and Cryptography*, 71(2):347–364, May 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9742-y`.

**Zhu:2014:RSS**

[1626] Mingzhi Zhu and Gennian Ge. Room squares with super-simple property. *Designs, Codes, and Cryptography*, 71(3):365–381, June 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9746-7`.

**Anashin:2014:FRN**

[1627] Vladimir Anashin, Andrei Khrennikov, and Ekaterina Yurova. $T$-functions revisited: new criteria for bijectivity/transitivity. *Designs, Codes, and Cryptography*, 71(3):383–407, June 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9741-z`.

**Petit:2014:TF**

[1628] Christophe Petit. Towards factoring in $\mathrm{SL}(2, \mathbf{F}_{2^n})$. *Designs, Codes, and Cryptography*, 71(3):409–431, June 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.`

com/article/10.1007/s10623-012-9743-x.

**Paterson:2014:UAC**

[1629] Maura B. Paterson and Douglas R. Stinson. A unified approach to combinatorial key predistribution schemes for sensor networks. *Designs, Codes, and Cryptography*, 71(3):433–457, June 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9749-4.

**Braun:2014:LTC**

[1630] Johannes Braun, Johannes Buchmann, Ciaran Mullan, and Alex Wiesmaier. Long term confidentiality: a survey. *Designs, Codes, and Cryptography*, 71(3):459–478, June 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9747-6.

**Evans:2014:MOL**

[1631] Anthony B. Evans. Mutually orthogonal Latin squares based on general linear groups. *Designs, Codes, and Cryptography*, 71(3):479–492, June 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9752-9.

**Yu:2014:NCN**

[1632] Nam Yul Yu, Keqin Feng, and Aixian Zhang. A new class of near-optimal partial Fourier codebooks from an almost difference set. *Designs, Codes, and Cryptography*, 71(3):493–501, June 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9753-8.

**Stokes:2014:LST**

[1633] Klara Stokes and Oriol Farràs. Linear spaces and transversal designs: $k$-anonymous combinatorial configurations for anonymous database search notes. *Designs, Codes, and Cryptography*, 71(3):503–524, June 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9745-8. See erratum [1634].

**Stokes:2014:ELS**

[1634] Klara Stokes and Oriol Farràs. Erratum to: Linear spaces and transversal designs: ($k$)-anonymous combinatorial configurations for anonymous database search. *Designs, Codes, and Cryptography*, 71(3):525, June 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9776-1; http://link.springer.com/content/pdf/10.1007/s10623-012-9776-1.pdf. See [1633].

**Ogata:2014:CDT**

[1635] Wakaha Ogata and Hiroshi Eguchi. Cheating detectable threshold scheme against most powerful cheaters for long secrets. *Designs, Codes, and Cryptography*, 71(3):527–539, June 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9756-5.

**Barwick:2014:CTS**

[1636] S. G. Barwick and Wen-Ai Jackson. A characterisation of tangent subplanes of $\mathrm{PG}(2, q^3)$. *Designs, Codes, and Cryptography*, 71(3):541–545, June 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9754-7`.

**Bamberg:2014:ESI**

[1637] John Bamberg, Jan De Beule, Nicola Durante, and Michel Lavrauw. Editorial: Special issue on finite geometries in honor of Frank De Clerck. *Designs, Codes, and Cryptography*, 72(1):1–5, July 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-9931-y`.

**Ghinelli:2014:RPD**

[1638] Dina Ghinelli, Dieter Jungnickel, and Klaus Metsch. Remarks on polarity designs. *Designs, Codes, and Cryptography*, 72(1):7–19, July 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9748-5`.

**Blokhuis:2014:KPG**

[1639] A. Blokhuis, M. De Boeck, F. Mazzocca, and L. Storme. The Kakeya problem: a gap in the spectrum and classification of the smallest examples. *Designs, Codes, and Cryptography*, 72(1):21–31, July 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9790-3`.

**Rottey:2014:MPL**

[1640] S. Rottey and L. Storme. Maximal partial line spreads of non-singular quadrics. *Designs, Codes, and Cryptography*, 72(1):33–51, July 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9788-x`.

**Korchmaros:2014:CII**

[1641] Gábor Korchmáros and Nicola Pace. Coset intersection of irreducible plane cubics. *Designs, Codes, and Cryptography*, 72(1):53–75, July 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9806-7`.

**DeBoeck:2014:LEK**

[1642] Maarten De Boeck. The largest Erdős–Ko–Rado sets of planes in finite projective and finite classical polar spaces. *Designs, Codes, and Cryptography*, 72(1):77–117, July 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9812-9`.

**Coolsaet:2014:SLP**

[1643] Kris Coolsaet. Some large partial ovoids of $(Q^{-(5,q)})$ for odd $q$. *Designs, Codes, and Cryptography*, 72 (1):119–128, July 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9828-1`.

**Bartoli:2014:NES**

[1644] Daniele Bartoli, Stefano Marcugini, and Fernanda Pambianco. The non-existence of some NMDS codes and the extremal sizes of complete $(n, 3)$-arcs in PG$(2, 16)$. *Designs, Codes, and Cryptography*, 72(1):129–134, July 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9837-0.

**Donati:2014:USH**

[1645] Giorgio Donati, Nicola Durante, and Alessandro Siciliano. On unitals in PG$(2, q^2)$ stabilized by a homology group. *Designs, Codes, and Cryptography*, 72(1):135–139, July 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9836-1.

**Neunhoffer:2014:SNT**

[1646] Max Neunhöffer and Cheryl E. Praeger. Sporadic neighbour-transitive codes in Johnson graphs. *Designs, Codes, and Cryptography*, 72 (1):141–152, July 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9853-0.

**Nagy:2014:LGR**

[1647] Gábor P. Nagy. Linear groups as right multiplication groups of quasifields. *Designs, Codes, and Cryptography*, 72(1):153–164, July 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9860-1.

**Crnkovic:2014:WRD**

[1648] Dean Crnković and Willem H. Haemers. Walk-regular divisible design graphs. *Designs, Codes, and Cryptography*, 72(1):165–175, July 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9861-0.

**Ball:2014:ACW**

[1649] Simeon Ball. A $p$-adic condition on the weight of a codeword of a linear code. *Designs, Codes, and Cryptography*, 72(1):177–183, July 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9863-y.

**Durante:2014:SBS**

[1650] Nicola Durante and Alessandro Siciliano. Some blocking semiovals of homology type in planes of square order. *Designs, Codes, and Cryptography*, 72(1):185–193, July 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9844-1.

**Aw:2014:MRP**

[1651] Alan J. Aw. The multicovering radius problem for some types of discrete structures. *Designs, Codes, and Cryptography*, 72(2):195–209, August 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.

com/article/10.1007/s10623-012-9755-6.

**Cossidente:2014:RSS**

[1652] Antonio Cossidente, Giuseppe Marino, and Tim Penttila. Relative symplectic subquadrangle hemisystems of the Hermitian surface. *Designs, Codes, and Cryptography*, 72(2):211–217, August 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9759-2.

**Zhuang:2014:RPL**

[1653] Zhuojun Zhuang, Bin Dai, Yuan Luo, and A. J. Han Vinck. On the relative profiles of a linear code and a subcode. *Designs, Codes, and Cryptography*, 72 (2):219–247, August 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9750-y.

**Li:2014:CDU**

[1654] Yongqiang Li and Mingsheng Wang. Constructing differentially 4-uniform permutations over GF($2^{2m}$) from quadratic APN permutations over GF($2^{2m+1}$). *Designs, Codes, and Cryptography*, 72(2):249–264, August 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9760-9.

**Payne:2014:DSS**

[1655] Stanley Payne and Morgan Rodgers. Double $k$-sets in symplectic generalized quadrangles. *Designs, Codes, and Cryptography*, 72(2):265–271, August 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9761-8.

**Hyun:2014:BFM**

[1656] Jong Yoon Hyun, Heisook Lee, and Yoonjin Lee. Boolean functions with MacWilliams duality. *Designs, Codes, and Cryptography*, 72(2):273–287, August 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9762-7.

**Fu:2014:OCA**

[1657] Hung-Lin Fu, Yuan-Hsun Lo, and Kenneth W. Shum. Optimal conflict-avoiding codes of odd length and weight three. *Designs, Codes, and Cryptography*, 72(2):289–309, August 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9764-5.

**Ihringer:2014:MSE**

[1658] Ferdinand Ihringer and Klaus Metsch. On the maximum size of Erdős–Ko–Rado sets in $H(2d + 1, q^2)$. *Designs, Codes, and Cryptography*, 72 (2):311–316, August 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9765-4.

**Bracken:2014:NCT**

[1659] Carl Bracken and Faruk Göloglu. A non-cyclic triple-error-correcting BCH-

like code and some minimum distance results. *Designs, Codes, and Cryptography*, 72(2):317–330, August 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9763-6`.

**Wood:2014:ROW**

[1660] Jay A. Wood. Relative one-weight linear codes. *Designs, Codes, and Cryptography*, 72(2):331–344, August 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9769-0`.

**Swanson:2014:CSP**

[1661] C. M. Swanson and D. R. Stinson. Combinatorial solutions providing improved security for the generalized Russian cards problem. *Designs, Codes, and Cryptography*, 72(2):345–367, August 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9770-7`.

**Shi:2014:ESS**

[1662] Ce Shi and Jianxing Yin. Existence of super-simple $\mathrm{OA}_\lambda(3,5,v)'s$. *Designs, Codes, and Cryptography*, 72(2):369–380, August 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9771-6`.

**Adams:2014:RIM**

[1663] Megan Adams and Junhua Wu. 2-ranks of incidence matrices associated with conics in finite projective planes. *Designs, Codes, and Cryptography*, 72(2):381–404, August 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9772-5`.

**Etzion:2014:CSS**

[1664] Tuvi Etzion. Covering of subspaces by subspaces. *Designs, Codes, and Cryptography*, 72(2):405–421, August 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9766-3`.

**Ren:2014:NSF**

[1665] Wenli Ren, Fang-Wei Fu, and Zhengchun Zhou. New sets of frequency-hopping sequences with optimal Hamming correlation. *Designs, Codes, and Cryptography*, 72(2):423–434, August 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9774-3`.

**Dougherty:2014:AFS**

[1666] S. T. Dougherty and C. Fernández-Córdoba. $\mathbf{Z}_2\mathbf{Z}_4$-additive formally self-dual codes. *Designs, Codes, and Cryptography*, 72(2):435–453, August 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9773-4`.

**Sonnino:2014:TIA**

[1667] Angelo Sonnino. Transitive $\mathrm{PSL}(2,7)$-invariant 42-arcs in 3-dimensional pro-

jective spaces. *Designs, Codes, and Cryptography*, 72(2):455–463, August 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9778-z`.

**Krcadinac:2014:ECT**

[1668] Vedran Krcadinac, Anamari Nakić, and Mario Osvin Pavcević. Equations for coefficients of tactical decomposition matrices for $t$-designs. *Designs, Codes, and Cryptography*, 72 (2):465–469, August 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9779-y`.

**Johnsen:2014:SRR**

[1669] Trygve Johnsen and Hugues Verdure. Stanley–Reisner resolution of constant weight linear codes. *Designs, Codes, and Cryptography*, 72(2):471–481, August 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9767-2`.

**Cao:2014:CGR**

[1670] Yonglin Cao. A class of 1-generator repeated root quasi-cyclic codes. *Designs, Codes, and Cryptography*, 72(3): 483–496, September 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9777-0`.

**Wei:2014:KFH**

[1671] Hengjia Wei and Gennian Ge. Kirkman frames having hole type $h^u m^1$ for $h \equiv 0 \bmod 12$. *Designs, Codes, and Cryptography*, 72(3):497–510, September 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9780-5`.

**Xiong:2014:WDC**

[1672] Maosheng Xiong. The weight distributions of a class of cyclic codes II. *Designs, Codes, and Cryptography*, 72 (3):511–528, September 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9785-0`.

**Horiguchi:2014:SDE**

[1673] Naoyuki Horiguchi, Tsuyoshi Miezaki, and Hiroyuki Nakasora. On the support designs of extremal binary doubly even self-dual codes. *Designs, Codes, and Cryptography*, 72(3):529–537, September 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9782-3`.

**Leung:2014:PCW**

[1674] Ka Hin Leung and Siu Lun Ma. Proper circulant weighing matrices of weight $p^2$. *Designs, Codes, and Cryptography*, 72(3):539–550, September 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9786-z`.

**Landjev:2014:SBB**

[1675] Ivan Landjev and Assia Rousseva. On the sharpness of Bruen's bound

for intersection sets in Desarguesian affine spaces. *Designs, Codes, and Cryptography*, 72(3):551–558, September 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9783-2`.

**Cengellenmis:2014:CIF**

[1676] Yasemin Cengellenmis, Abdullah Dertli, and S. T. Dougherty. Codes over an infinite family of rings with a Gray map. *Designs, Codes, and Cryptography*, 72(3):559–580, September 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9787-y`.

**Ding:2014:CAD**

[1677] Cunsheng Ding, Alexander Pott, and Qi Wang. Constructions of almost difference sets from finite fields. *Designs, Codes, and Cryptography*, 72(3):581–592, September 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9789-9`.

**Liu:2014:KIS**

[1678] Siyu Liu, Felice Manganiello, and Frank R. Kschischang. Kötter interpolation in skew polynomial rings. *Designs, Codes, and Cryptography*, 72(3):593–608, September 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9784-1`.

**Berg:2014:SSE**

[1679] James Berg and Max Wakefield. Skeleton simplicial evaluation codes. *Designs, Codes, and Cryptography*, 72(3):609–625, September 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9793-0`.

**Hiramine:2014:NEM**

[1680] Yutaka Hiramine. On the non-existence of maximal difference matrices of deficiency 1. *Designs, Codes, and Cryptography*, 72(3):627–635, September 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9794-7`.

**Horan:2014:OCS**

[1681] Victoria Horan and Glenn Hurlbert. 1-overlap cycles for Steiner triple systems. *Designs, Codes, and Cryptography*, 72(3):637–651, September 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9802-y`.

**Su:2014:SMC**

[1682] Sihong Su, Xiaohu Tang, and Xiangyong Zeng. A systematic method of constructing Boolean functions with optimal algebraic immunity based on the generator matrix of the Reed–Muller code. *Designs, Codes, and Cryptography*, 72(3):653–673, September 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.`

com/article/10.1007/s10623-013-9801-z.

**Jha:2014:UOF**

[1683] Vikram Jha. The ubiquity of the orders of fractional semifields of even characteristic. *Designs, Codes, and Cryptography*, 72(3):675–686, September 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9795-6.

**Coxon:2014:LDN**

[1684] Nicholas Coxon. List decoding of number field codes. *Designs, Codes, and Cryptography*, 72(3):687–711, September 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9803-x.

**vanTrung:2014:TBF**

[1685] Tran van Trung. A tight bound for frameproof codes viewed in terms of separating hash families. *Designs, Codes, and Cryptography*, 72(3):713–718, September 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9800-0.

**Hering:2014:NC**

[1686] Christoph Hering, Andreas Krebs, and Thomas Edgar. Naive configurations. *Designs, Codes, and Cryptography*, 72(3):719–731, September 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9797-4.

**Bierbrauer:2014:SQQ**

[1687] Jürgen Bierbrauer, Daniele Bartoli, Giorgio Faina, Stefano Marcugini, Fernanda Pambianco, and Yves Edel. The structure of quaternary quantum caps. *Designs, Codes, and Cryptography*, 72(3):733–747, September 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9796-5.

**Guenda:2014:LR**

[1688] Kenza Guenda, T. Aaron Gulliver, and S. Arash Sheikholeslam. Lexicodes over rings. *Designs, Codes, and Cryptography*, 72(3):749–763, September 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9791-2.

**Liebler:2014:NTC**

[1689] Robert A. Liebler and Cheryl E. Praeger. Neighbour-transitive codes in Johnson graphs. *Designs, Codes, and Cryptography*, 73(1):1–25, October 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9982-0.

**Stichtenoth:2014:NCP**

[1690] Henning Stichtenoth. A note on composed products of polynomials over finite fields. *Designs, Codes, and Cryptography*, 73(1):27–32, October 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.

com/article/10.1007/s10623-013-9808-5.

**Chigira:2014:CED**

[1691] Naoki Chigira, Masaaki Harada, and Masaaki Kitazume. On the classification of extremal doubly even self-dual codes with 2-transitive automorphism groups. *Designs, Codes, and Cryptography*, 73(1):33–35, October 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9807-6.

**Lu:2014:EVO**

[1692] Hui-Chuan Lu and Hung-Lin Fu. The exact values of the optimal average information ratio of perfect secret-sharing schemes for tree-based access structures. *Designs, Codes, and Cryptography*, 73(1):37–46, October 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-012-9792-1.

**Nakashima:2014:CCA**

[1693] Tohru Nakashima. Construction of codes from Arakelov geometry. *Designs, Codes, and Cryptography*, 73 (1):47–54, October 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9809-4.

**Zhou:2014:ELC**

[1694] Jianqin Zhou and Wanquan Liu. The $k$-error linear complexity distribution for $2^n$-periodic binary sequences. *Designs, Codes, and Cryptography*, 73 (1):55–75, October 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9805-8.

**Broughton:2014:APS**

[1695] Wayne Broughton. Admissible parameters of symmetric designs satisfying $v = 4(k - \lambda) + 2$ and symmetric designs with inner balance. *Designs, Codes, and Cryptography*, 73 (1):77–83, October 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9810-y.

**Huang:2014:RKS**

[1696] Jialin Huang and Xuejia Lai. Revisiting key schedule's diffusion in relation with round function's diffusion. *Designs, Codes, and Cryptography*, 73 (1):85–103, October 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9804-9.

**Schmidt:2014:CRD**

[1697] Bernhard Schmidt and Ming Ming Tan. Construction of relative difference sets and Hadamard groups. *Designs, Codes, and Cryptography*, 73 (1):105–119, October 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9811-x.

**Mennink:2014:CPS**

[1698] Bart Mennink. On the collision and preimage security of MDC-4 in the

ideal cipher model. *Designs, Codes, and Cryptography*, 73(1):121–150, October 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9813-8`.

**Dougherty:2014:CCR**

[1699] Steven T. Dougherty and Esengül Saltürk. Counting codes over rings. *Designs, Codes, and Cryptography*, 73 (1):151–165, October 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9815-6`.

**Liu:2014:LHZ**

[1700] Xing Liu, Daiyuan Peng, and Hongyu Han. Low-hit-zone frequency hopping sequence sets with optimal partial Hamming correlation properties. *Designs, Codes, and Cryptography*, 73 (1):167–176, October 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9817-4`.

**Groza:2014:CPR**

[1701] Bogdan Groza and Bogdan Warinschi. Cryptographic puzzles and DoS resilience, revisited. *Designs, Codes, and Cryptography*, 73(1):177–207, October 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9816-5`.

**Lisonek:2014:BFP**

[1702] Petr Lisonek and Hui Yi Lu. Bent functions on partial spreads. *Designs, Codes, and Cryptography*, 73 (1):209–216, October 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9820-9`.

**Cossidente:2014:NIF**

[1703] Antonio Cossidente and Francesco Pavese. New infinite families of hyperovals on $\mathcal{H}(\ni, \amalg^{\in}), \amalg$ odd. *Designs, Codes, and Cryptography*, 73 (1):217–222, October 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9818-3`.

**Fang:2014:NSQ**

[1704] Jianying Fang, Junling Zhou, and Yanxun Chang. Nonexistence of some quantum jump codes with specified parameters. *Designs, Codes, and Cryptography*, 73(1):223–235, October 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9814-7`.

**Li:2014:NAS**

[1705] Nian Li, Xiaohu Tang, and Tor Helleseth. New $M$-ary sequences with low autocorrelation from interleaved technique. *Designs, Codes, and Cryptography*, 73(1):237–249, October 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9821-8`.

**Liu:2014:FEC**

[1706] Huaning Liu. A family of elliptic curve pseudorandom binary sequences. *Designs, Codes, and Cryptography*, 73 (1):251–265, October 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9822-7`.

**Geil:2014:ESW**

[1707] Olav Geil. Erratum to: On the second weight of generalized Reed–Muller codes. *Designs, Codes, and Cryptography*, 73(1):267, October 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-9966-0; http://link.springer.com/content/pdf/10.1007/s10623-014-9966-0.pdf`. See [1072].

**Budaghyan:2014:ESI**

[1708] Lilya Budaghyan, Tor Helleseth, and Matthew Parker. Editorial: special issue on coding and cryptography. *Designs, Codes, and Cryptography*, 73 (2):269, November 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-9995-8; http://link.springer.com/content/pdf/10.1007/s10623-014-9995-8.pdf`.

**Ballet:2014:LWC**

[1709] Stéphane Ballet and Robert Rolland. On low weight codewords of generalized affine and projective Reed–Muller codes. *Designs, Codes, and Cryptography*, 73(2):271–297, November 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9911-7`.

**Carlet:2014:AWC**

[1710] Claude Carlet and Andrew Klapper. On the arithmetic Walsh coefficients of Boolean functions. *Designs, Codes, and Cryptography*, 73(2):299–318, November 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9915-3`.

**Pirsic:2014:DFT**

[1711] Gottlieb Isabel Pirsic and Arne Winterhof. On discrete Fourier transform, ambiguity, and Hamming-autocorrelation of pseudorandom sequences. *Designs, Codes, and Cryptography*, 73(2): 319–328, November 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9916-2`.

**Klove:2014:LCC**

[1712] Torleiv Kløve and Moshe Schwartz. Linear covering codes and error-correcting codes for limited-magnitude errors. *Designs, Codes, and Cryptography*, 73(2):329–354, November 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9917-1`.

**Fontein:2014:PPT**

[1713] Felix Fontein, Michael Schneider, and Urs Wagner. PotLLL: a polynomial

time version of LLL with deep insertions. *Designs, Codes, and Cryptography*, 73(2):355–368, November 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-9918-8`.

**Kim:2014:NIA**

[1714] Hyun Kwang Kim and Phan Thanh Toan. New inequalities for $q$-ary constant-weight codes. *Designs, Codes, and Cryptography*, 73(2):369–381, November 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-9924-x`.

**Sarkar:2014:SSE**

[1715] Santanu Sarkar. Small secret exponent attack on RSA variant with modulus $N = p^r q$. *Designs, Codes, and Cryptography*, 73(2):383–392, November 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-9928-6`.

**Rosenthal:2014:GBG**

[1716] Joachim Rosenthal, Natalia Silberstein, and Anna-Lena Trautmann. On the geometry of balls in the Grassmannian and list decoding of lifted Gabidulin codes. *Designs, Codes, and Cryptography*, 73(2):393–416, November 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-9932-x`.

**Lisonek:2014:QCN**

[1717] Petr Lisonek and Vijaykumar Singh. Quantum codes from nearly self-orthogonal quaternary linear codes. *Designs, Codes, and Cryptography*, 73(2):417–424, November 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-9934-8`.

**Ong:2014:WLC**

[1718] Soon Sheng Ong and Frédérique Oggier. Wiretap lattice codes from number fields with no small norm elements. *Designs, Codes, and Cryptography*, 73(2):425–440, November 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-9935-7`.

**Kositwattanarerk:2014:CBC**

[1719] Wittawat Kositwattanarerk and Frédérique Oggier. Connections between Construction $D$ and related constructions of lattices. *Designs, Codes, and Cryptography*, 73(2):441–455, November 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-9939-3`.

**Ozbudak:2014:ENS**

[1720] Ferruh Özbudak and Zülfükar Saygi. On the exact number of solutions of certain linearized equations. *Designs, Codes, and Cryptography*, 73(2):457–468, November 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http:`

//link.springer.com/article/10.1007/s10623-014-9942-8.

**Dubrova:2014:GFC**

[1721] Elena Dubrova. Generation of full cycles by a composition of NLFSRs. *Designs, Codes, and Cryptography*, 73(2):469–486, November 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9947-3.

**Blondeau:2014:MDU**

[1722] Céline Blondeau and Léo Perrin. More differentially 6-uniform power functions. *Designs, Codes, and Cryptography*, 73(2):487–505, November 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9948-2.

**Nielsen:2014:MTG**

[1723] Johan S. R. Nielsen and Alexander Zeh. Multi-trial Guruswami–Sudan decoding for generalised Reed–Solomon codes. *Designs, Codes, and Cryptography*, 73(2):507–527, November 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9951-7.

**Jhanwar:2014:PBP**

[1724] Mahabir Prasad Jhanwar, Ayineedi Venkateswarlu, and Reihaneh Safavi-Naini. Paillier-based publicly verifiable (non-interactive) secret sharing. *Designs, Codes, and Cryptography*, 73(2):529–546, November 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9952-6.

**Wachter-Zeh:2014:LUE**

[1725] Antonia Wachter-Zeh and Alexander Zeh. List and unique error-erasure decoding of interleaved Gabidulin codes with interpolation techniques. *Designs, Codes, and Cryptography*, 73(2):547–570, November 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9953-5.

**Li:2014:TDE**

[1726] Wenhui Li, Vladimir Sidorenko, and Danilo Silva. On transform-domain error and erasure correction by Gabidulin codes. *Designs, Codes, and Cryptography*, 73(2):571–586, November 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9954-4.

**Yu:2014:MAC**

[1727] Yuyin Yu, Mingsheng Wang, and Yongqiang Li. A matrix approach for constructing quadratic APN functions. *Designs, Codes, and Cryptography*, 73(2):587–600, November 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9955-3.

**Cao:2014:PIP**

[1728] Weiwei Cao and Lei Hu. Projective interpolation of polynomial vectors and improved key recovery attack on SFLASH. *Designs, Codes, and*

*Cryptography*, 73(3):719–730, December 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9819-2`.

**Chen:2014:SES**

[1729] Jie Chen, Hoon Wei Lim, San Ling, Le Su, and Huaxiong Wang. Spatial encryption supporting non-monotone access structure. *Designs, Codes, and Cryptography*, 73(3):731–746, December 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9823-6`.

**Liu:2014:WDS**

[1730] Xiaogang Liu and Yuan Luo. The weight distributions of some cyclic codes with three or four nonzeros over $\mathbf{F}_3$. *Designs, Codes, and Cryptography*, 73(3):747–768, December 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9824-5`.

**Fang:2014:MDD**

[1731] Jianying Fang and Yanxun Chang. Mutually disjoint $t$-designs and $t$-SEEDs from extremal doubly-even self-dual codes. *Designs, Codes, and Cryptography*, 73(3):769–780, December 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9825-4`.

**Liang:2014:CFP**

[1732] Miao Liang, Mingchao Li, and Beiliang Du. A construction for $t$-fold perfect authentication codes with arbitration. *Designs, Codes, and Cryptography*, 73(3):781–790, December 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9826-3`.

**Ma:2014:NOC**

[1733] Wenping Ma, Chun e Zhao, and Dongsu Shen. New optimal constructions of conflict-avoiding codes of odd length and weight 3. *Designs, Codes, and Cryptography*, 73(3):791–804, December 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9827-2`.

**Lin:2014:EPS**

[1734] Yiling Lin and Masakazu Jimbo. Extremal properties of $t$-SEEDs and recursive constructions. *Designs, Codes, and Cryptography*, 73(3):805–823, December 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9829-0`.

**Feng:2014:DSF**

[1735] Tao Feng, Sihuang Hu, Shuxing Li, and Gennian Ge. Difference sets with few character values. *Designs, Codes, and Cryptography*, 73(3):825–839, December 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.`

com/article/10.1007/s10623-013-9830-7.

**Herranz:2014:NRA**

[1736] Javier Herranz, Alexandre Ruiz, and Germán Sáez. New results and applications for multi-secret sharing schemes. *Designs, Codes, and Cryptography*, 73 (3):841–864, December 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9831-6.

**Adhikari:2014:LAT**

[1737] Avishek Adhikari. Linear algebraic techniques to construct monochrome visual cryptographic schemes for general access structure and its applications to color images. *Designs, Codes, and Cryptography*, 73(3):865–895, December 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9832-5.

**Momihara:2014:DDF**

[1738] Koji Momihara and Mieko Yamada. Divisible difference families from Galois rings $\mathrm{GR}(4, n)$ and Hadamard matrices. *Designs, Codes, and Cryptography*, 73(3):897–909, December 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9833-4.

**Chen:2014:SIB**

[1739] Jie Chen, Hoon Wei Lim, San Ling, Huaxiong Wang, and Hoeteck Wee. Shorter identity-based encryption via asymmetric pairings. *Designs, Codes, and Cryptography*, 73(3):911–947, December 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9834-3.

**Raaphorst:2014:CSC**

[1740] Sebastian Raaphorst, Lucia Moura, and Brett Stevens. A construction for strength-3 covering arrays from linear feedback shift register sequences. *Designs, Codes, and Cryptography*, 73 (3):949–968, December 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9835-2.

**Gavrilyuk:2014:CLL**

[1741] Alexander L. Gavrilyuk and Ivan Yu. Mogilnykh. Cameron-liebler line classes in $PG(n, 4)$. *Designs, Codes, and Cryptography*, 73(3):969–982, December 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9838-z.

**Yankov:2014:NBS**

[1742] Nikolay Yankov and Moon Ho Lee. New binary self-dual codes of lengths 50–60. *Designs, Codes, and Cryptography*, 73(3):983–996, December 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9839-y.

**Bulygin:2014:FAP**

[1743] Stanislav Bulygin, Michael Walter, and Johannes Buchmann. Full analysis

of PRINTcipher with respect to invariant subspace attack: efficient key recovery and countermeasures. *Designs, Codes, and Cryptography*, 73(3): 997–1022, December 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9840-5`.

**Ballico:2014:NCC**

[1744] Edoardo Ballico. Any network code comes from an algebraic curve taking osculating spaces. *Designs, Codes, and Cryptography*, 73(3):1023–1026, December 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9841-4`.

**Horiguchi:2014:ESD**

[1745] Naoyuki Horiguchi, Tsuyoshi Miezaki, and Hiroyuki Nakasora. Erratum to: On the support designs of extremal binary doubly even self-dual codes. *Designs, Codes, and Cryptography*, 73(3): 1027–1028, December 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-9990-0; http://link.springer.com/content/pdf/10.1007/s10623-014-9990-0.pdf`.

**Klove:2014:ELC**

[1746] Torleiv Kløve and Moshe Schwartz. Erratum to: Linear covering codes and error-correcting codes for limited-magnitude errors. *Designs, Codes, and Cryptography*, 73(3):1029, December 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-9991-z; http://link.springer.com/content/pdf/10.1007/s10623-014-9991-z.pdf`.

**Singh:2015:CCR**

[1747] Abhay Kumar Singh and Pramod Kumar Kewat. On cyclic codes over the ring $\mathbf{Z}_p[u]/\langle u^k \rangle$. *Designs, Codes, and Cryptography*, 74(1):1–13, January 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9843-2`.

**Dai:2015:TSE**

[1748] Peipei Dai, Jianmin Wang, and Jianxing Yin. Two series of equitable symbol weight codes meeting the Plotkin bound. *Designs, Codes, and Cryptography*, 74(1):15–29, January 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9846-z`.

**Cheng:2015:NBS**

[1749] Minquan Cheng, Hung-Lin Fu, Jing Jiang, Yuan-Hsun Lo, and Ying Miao. New bounds on $\bar{2}$-separable codes of length 2. *Designs, Codes, and Cryptography*, 74(1):31–40, January 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9849-9; http://link.springer.com/content/pdf/10.1007/s10623-013-9849-9.pdf`.

**Wang:2015:GBA**

[1750] Hui Wang, Paul Stankovski, and Thomas Johansson. A generalized birthday approach for efficiently finding linear relations in $\ell$-sequences. *Designs, Codes, and Cryptography*, 74 (1):41–57, January 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9845-0`.

**Cheon:2015:MNP**

[1751] Eun Ju Cheon and Seon Jeong Kim. On the minimum number of points covered by a set of lines in PG$(2, q)$. *Designs, Codes, and Cryptography*, 74 (1):59–74, January 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9851-2`.

**Skoric:2015:BAT**

[1752] Boris Skorić and Jan-Jaap Oosterwijk. Binary and $q$-ary Tardos codes, revisited. *Designs, Codes, and Cryptography*, 74(1):75–111, January 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9842-3`.

**Cordon-Franco:2015:GPC**

[1753] Andrés Cordón-Franco, Hans van Ditmarsch, David Fernández-Duque, and Fernando Soler-Toscano. A geometric protocol for cryptography with cards. *Designs, Codes, and Cryptography*, 74 (1):113–125, January 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9855-y`.

**Wei:2015:SSP**

[1754] Hengjia Wei and Gennian Ge. Spectrum of sizes for perfect 2-deletion-correcting codes of length 4. *Designs, Codes, and Cryptography*, 74 (1):127–151, January 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9848-x`.

**Dempwolff:2015:SDD**

[1755] Ulrich Dempwolff. Symmetric doubly dual hyperovals have an odd rank. *Designs, Codes, and Cryptography*, 74 (1):153–157, January 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9847-y`.

**Simone:2015:FNP**

[1756] Antonino Simone and Boris Skorić. False Negative probabilities in Tardos codes. *Designs, Codes, and Cryptography*, 74(1):159–182, January 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9856-x`.

**Cremers:2015:BEP**

[1757] Cas Cremers and Michèle Feltz. Beyond eCK: perfect forward secrecy under actor compromise and ephemeral-key reveal. *Designs, Codes, and Cryptography*, 74(1):183–218, January 2015. CODEN DCCREC. ISSN

0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9852-1.

**Jarvis:2015:ENE**

[1758] Katherine Jarvis and Monica Nevins. ETRU: NTRU over the Eisenstein integers. *Designs, Codes, and Cryptography*, 74(1):219–242, January 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9850-3.

**Wei:2015:GDD**

[1759] Hengjia Wei and Gennian Ge. Group divisible designs with block size four and group type $g^u m^1$. *Designs, Codes, and Cryptography*, 74(1):243–282, January 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9854-z.

**Rifa:2015:EIH**

[1760] J. Rifà, F. I. Solov'eva, and M. Villanueva. Erratum to: Intersection of Hamming codes avoiding Hamming subcodes. *Designs, Codes, and Cryptography*, 74(1):283, January 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-0011-0; http://link.springer.com/content/pdf/10.1007/s10623-014-0011-0.pdf.

**Chen:2015:CMC**

[1761] Bocong Chen, Hongwei Liu, and Guanghui Zhang. A class of minimal cyclic codes over finite fields. *Designs, Codes, and Cryptography*, 74(2):285–300, February 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9857-9.

**Feng:2015:SCH**

[1762] Tao Feng, Xiaomiao Wang, and Yanxun Chang. Semi-cyclic holey group divisible designs with block size three. *Designs, Codes, and Cryptography*, 74(2):301–324, February 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9859-7.

**Albrecht:2015:CBA**

[1763] Martin R. Albrecht, Carlos Cid, Jean-Charles Faugère, Robert Fitzpatrick, and Ludovic Perret. On the complexity of the BKW algorithm on LWE. *Designs, Codes, and Cryptography*, 74(2):325–354, February 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9864-x.

**Yang:2015:SDC**

[1764] Yiansheng Yang and Wenchao Cai. On self-dual constacyclic codes over finite fields. *Designs, Codes, and Cryptography*, 74(2):355–364, February 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9865-9.

**Dokovic:2015:CPC**

[1765] Dragomir Z. Đoković and Ilias S. Kotsireas. Compression of periodic complementary sequences and applications. *Designs, Codes, and Cryptography*, 74 (2):365–377, February 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9862-z`.

**Torezzan:2015:OCG**

[1766] Cristiano Torezzan, João E. Strapasson, Sueli I. R. Costa, and Rogerio M. Siqueira. Optimum commutative group codes. *Designs, Codes, and Cryptography*, 74(2):379–394, February 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9867-7`.

**Lee:2015:AHS**

[1767] Kwangsu Lee, Jong Hwan Park, and Dong Hoon Lee. Anonymous HIBE with short ciphertexts: full security in prime order groups. *Designs, Codes, and Cryptography*, 74 (2):395–425, February 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9868-6`.

**Lavrauw:2015:EMD**

[1768] Michel Lavrauw, John Sheekey, and Corrado Zanella. On embeddings of minimum dimension of $\mathrm{PG}(n,q) \times \mathrm{PG}(n,q)$. *Designs, Codes, and Cryptography*, 74(2):427–440, February 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9866-8`.

**Randriam:2015:LBM**

[1769] Hugues Randriam, Lin Sok, and Patrick Solé. Lower bounds on the minimum distance of long codes in the Lee metric. *Designs, Codes, and Cryptography*, 74(2):441–452, February 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9870-z`.

**Alfaro:2015:CSD**

[1770] R. Alfaro and K. Dhul-Qarnayn. Constructing self-dual codes over $\mathbf{F}_q[u]/(u^t)$. *Designs, Codes, and Cryptography*, 74(2):453–465, February 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9873-9`.

**Yang:2015:FRD**

[1771] Dong Yang, Wen-Feng Qi, and Qun-Xiong Zheng. Further results on the distinctness of modulo 2 reductions of primitive sequences over $\mathbf{Z}(\mathbf{2^{32}} - \mathbf{1})$. *Designs, Codes, and Cryptography*, 74 (2):467–480, February 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9871-y`.

**Hunt:2015:DME**

[1772] Francis H. Hunt, Stephanie Perkins, and Derek H. Smith. Decoding

mixed errors and erasures in permutation codes. *Designs, Codes, and Cryptography*, 74(2):481–493, February 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9872-x`.

**Farras:2015:EBD**

[1773] Oriol Farràs and Carles Padró. Extending Brickell–Davenport theorem to non-perfect secret sharing schemes. *Designs, Codes, and Cryptography*, 74 (2):495–510, February 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9858-8`.

**Jitman:2015:QAC**

[1774] Somphong Jitman and San Ling. Quasi-abelian codes. *Designs, Codes, and Cryptography*, 74(3):511–531, March 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9878-4`.

**Liu:2015:BAA**

[1775] Xiaogang Liu and Yuan Luo. On the bounds and achievability about the ODPC of $\mathcal{GRM}(\in, \Updownarrow)^*$ over prime fields for increasing message length. *Designs, Codes, and Cryptography*, 74 (3):533–557, March 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9877-5`.

**Doliskani:2015:CDT**

[1776] Javad Doliskani and Éric Schost. Computing in degree $2^k$-extensions of finite fields of odd characteristic. *Designs, Codes, and Cryptography*, 74 (3):559–569, March 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9875-7`.

**Yankov:2015:CSD**

[1777] Nikolay Yankov and Moon Ho Lee. Classification of self-dual codes of length 50 with an automorphism of odd prime order. *Designs, Codes, and Cryptography*, 74(3):571–579, March 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9874-8`.

**Chen:2015:PTS**

[1778] Yu Qing Chen and Tao Feng. Paley type sets from cyclotomic classes and Arasu–Dillon-player difference sets. *Designs, Codes, and Cryptography*, 74 (3):581–600, March 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9881-9`.

**Danielsen:2015:GCP**

[1779] Lars Eirik Danielsen, Matthew G. Parker, and Constanza Riera. On graphs and codes preserved by edge local complementation. *Designs, Codes, and Cryptography*, 74(3):601–621, March 2015. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9876-6.

**Li:2015:OAS**

[1780] Qiang Li, Xiang Xue Li, Xue Jia Lai, and Ke Fei Chen. Optimal assignment schemes for general access structures based on linear programming. *Designs, Codes, and Cryptography*, 74 (3):623–644, March 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9879-3.

**Minematsu:2015:BBS**

[1781] Kazuhiko Minematsu. Building blockcipher from small-block tweakable blockcipher. *Designs, Codes, and Cryptography*, 74(3):645–663, March 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9882-8.

**Schmidt:2015:HNF**

[1782] Kai-Uwe Schmidt. Highly nonlinear functions. *Designs, Codes, and Cryptography*, 74(3):665–672, March 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9880-x.

**Karadeniz:2015:NEB**

[1783] Suat Karadeniz and Bahattin Yildiz. New extremal binary self-dual codes of length 64 from $R_3$-lifts of the extended binary Hamming code. *Designs, Codes, and Cryptography*, 74 (3):673–680, March 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9884-6.

**Matsui:2015:GMP**

[1784] Hajime Matsui. On generator matrices and parity check matrices of generalized integer codes. *Designs, Codes, and Cryptography*, 74(3):681–701, March 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9883-7.

**Su:2015:LCL**

[1785] Ming Su. On the linear complexity of Legendre–Sidelnikov sequences. *Designs, Codes, and Cryptography*, 74 (3):703–717, March 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9889-1.

**Csirmaz:2015:SSD**

[1786] László Csirmaz. Secret sharing on the $d$-dimensional cube. *Designs, Codes, and Cryptography*, 74(3):719–729, March 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9888-2.

**Lin:2015:CIB**

[1787] Xi Jun Lin, Ran Ren, Zhengang Wei, and Lin Sun. Comment on "Identity-based non-interactive key distribution with forward security". *Designs, Codes, and Cryptography*, 75(1):1–7, April 2015. CODEN DCCREC. ISSN

0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9886-4. See [1443].

**Topalova:2015:PTT**

[1788] Svetlana Topalova and Stela Zhelezova. On point-transitive and transitive deficiency one parallelisms of PG $(3, 4)$. *Designs, Codes, and Cryptography*, 75(1):9–19, April 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9887-3.

**Ezerman:2015:XLC**

[1789] Martianus Frederic Ezerman, Somphong Jitman, and Patrick Solé. Xing-Ling codes, duals of their subcodes, and good asymmetric quantum codes. *Designs, Codes, and Cryptography*, 75(1):21–42, April 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9885-5.

**Li:2015:TFN**

[1790] Chengju Li, Qin Yue, and Yiwei Huang. Two families of nearly optimal codebooks. *Designs, Codes, and Cryptography*, 75(1):43–57, April 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9891-7.

**Fazio:2015:HLP**

[1791] Nelly Fazio, Kevin Iga, Antonio R. Nicolosi, Ludovic Perret, and William E. Skeith III. Hardness of learning problems over Burnside groups of exponent 3. *Designs, Codes, and Cryptography*, 75(1):59–70, April 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9892-6.

**Zieve:2015:PFP**

[1792] Michael E. Zieve. Planar functions and perfect nonlinear monomials over finite fields. *Designs, Codes, and Cryptography*, 75(1):71–80, April 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9890-8.

**Kovacevic:2015:PCD**

[1793] Mladen Kovacević and Dejan Vukobratović. Perfect codes in the discrete simplex. *Designs, Codes, and Cryptography*, 75(1):81–95, April 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9893-5.

**Britz:2015:DMC**

[1794] Thomas Britz, Keisuke Shiromoto, and Thomas Westerbäck. Demi-matroids from codes over finite Frobenius rings. *Designs, Codes, and Cryptography*, 75(1):97–107, April 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9895-3.

**Shum:2015:OTD**

[1795] Kenneth W. Shum. Optimal three-dimensional optical orthogonal codes of weight three. *Designs, Codes, and*

*Cryptography*, 75(1):109–126, April 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9894-4`.

**Liu:2015:RCW**

[1796] Zihui Liu and Xin-Wen Wu. On relative constant-weight codes. *Designs, Codes, and Cryptography*, 75 (1):127–144, April 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9896-2`.

**Ugolini:2015:SIP**

[1797] S. Ugolini. Sequences of irreducible polynomials without prescribed coefficients over odd prime fields. *Designs, Codes, and Cryptography*, 75 (1):145–155, April 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9897-1`.

**Han:2015:NLB**

[1798] Hongyu Han, Daiyuan Peng, and Xing Liu. New lower bounds on the aperiodic Hamming correlations of frequency hopping sequences with low hit zone. *Designs, Codes, and Cryptography*, 75 (1):157–174, April 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9900-x`.

**Horak:2015:SDH**

[1799] Peter Horak and Zsolt Tuza. Speeding up deciphering by hypergraph ordering. *Designs, Codes, and Cryptography*, 75(1):175–185, April 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9899-z`.

**Yang:2015:OPK**

[1800] Chih-Yen Yang and Chung-Chin Lu. One-point Klein codes and their serial-in-serial-out systematic encoding. *Designs, Codes, and Cryptography*, 75 (2):187–197, May 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9898-0`.

**Ma:2015:ASF**

[1801] Zhen Ma, Wen-Feng Qi, and Tian Tian. On affine sub-families of the NFSR in grain. *Designs, Codes, and Cryptography*, 75(2):199–212, May 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9901-9`.

**Cossidente:2015:NFR**

[1802] Antonio Cossidente. A new family of relative hemisystems on the Hermitian surface. *Designs, Codes, and Cryptography*, 75(2):213–221, May 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9906-4`.

**Newman:2015:CD**

[1803] N. A. Newman. 4-cycle decompositions of $(\lambda + m)K_{v+u} \backslash \lambda K_v$. *Designs, Codes, and Cryptography*, 75(2):223–235, May 2015. CODEN DCCREC. ISSN

0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9904-6.

**Swartz:2015:CPD**

[1804] Eric Swartz. A construction of a partial difference set in the extraspecial groups of order $p^3$ with exponent $p^2$. *Designs, Codes, and Cryptography*, 75(2):237–242, May 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9903-7.

**delaCruz:2015:ESD**

[1805] Javier de la Cruz. On extremal self-dual codes of length 120. *Designs, Codes, and Cryptography*, 75 (2):243–252, May 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9902-8.

**Han:2015:MCS**

[1806] Sunghyu Han. A method for constructing self-dual codes over $\mathbf{Z}_{2^m}$. *Designs, Codes, and Cryptography*, 75(2):253–262, May 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9907-3.

**Zheng:2015:WDF**

[1807] Dabin Zheng, Xiaoqiang Wang, Xiangyong Zeng, and Lei Hu. The weight distribution of a family of $p$-ary cyclic codes. *Designs, Codes, and Cryptography*, 75(2):263–275, May 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9908-2.

**Kageyama:2015:CGC**

[1808] Yuuki Kageyama and Tatsuya Maruta. On the construction of Griesmer codes of dimension 5. *Designs, Codes, and Cryptography*, 75(2):277–280, May 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9914-4.

**Leducq:2015:FWP**

[1809] Elodie Leducq. Functions which are PN on infinitely many extensions of $\mathbf{F}_p, p$ odd. *Designs, Codes, and Cryptography*, 75(2):281–299, May 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9912-6.

**Ram:2015:ELT**

[1810] Samrith Ram. Enumeration of linear transformation shift registers. *Designs, Codes, and Cryptography*, 75 (2):301–314, May 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9913-5.

**vanZanten:2015:GRR**

[1811] A. J. van Zanten, A. Bojilov, and S. M. Dodunekov. Generalized residue and $t$-residue codes and their idempotent generators. *Designs, Codes, and Cryptography*, 75(2):315–334, May 2015. CODEN DCCREC. ISSN

0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9905-5.

**Gorla:2015:PCT**

[1812] Elisa Gorla and Maike Massierer. Point compression for the trace zero subgroup over a small degree extension field. *Designs, Codes, and Cryptography*, 75(2):335–357, May 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9921-0.

**Olteanu:2015:CMN**

[1813] Gabriela Olteanu and Inneke Van Gelder. Construction of minimal non-abelian left group codes. *Designs, Codes, and Cryptography*, 75(3):359–373, June 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9922-z.

**Jiang:2015:NRN**

[1814] Yupeng Jiang and Yingpu Deng. New results on nonexistence of generalized bent functions. *Designs, Codes, and Cryptography*, 75(3):375–385, June 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9923-y.

**Chee:2015:HTP**

[1815] Yeow Meng Chee, Gennian Ge, Hui Zhang, and Xiande Zhang. Hanani triple packings and optimal $q$-ary codes of constant weight three. *Designs, Codes, and Cryptography*, 75(3):387–403, June 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9919-7.

**Rifa:2015:SEH**

[1816] Josep Rifà, Faina I. Solov'eva, and Mercè Villanueva. Self-embeddings of Hamming Steiner triple systems of small order and APN permutations. *Designs, Codes, and Cryptography*, 75(3):405–427, June 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9909-1.

**Nilson:2015:TAY**

[1817] Tomas Nilson and Lars-Daniel Öhman. Triple arrays and Youden squares. *Designs, Codes, and Cryptography*, 75(3):429–451, June 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9926-8.

**Vandendriessche:2015:SLS**

[1818] Peter Vandendriessche. On small line sets with few odd-points. *Designs, Codes, and Cryptography*, 75(3):453–463, June 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9920-1.

**DeBoeck:2015:LEK**

[1819] Maarten De Boeck. The largest Erdős–Ko–Rado sets in $2-(v,k,1)$ designs.

*Designs, Codes, and Cryptography*, 75(3):465–481, June 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-9929-5`.

**Cho:2015:NCR**

[1820] Gook Hwa Cho, Namhun Koo, Eunhye Ha, and Soonhak Kwon. New cube root algorithm based on the third order linear recurrence relations in finite fields. *Designs, Codes, and Cryptography*, 75(3):483–495, June 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9910-8`.

**Janiszczak:2015:PCI**

[1821] Ingo Janiszczak, Wolfgang Lempken, Patric R. J. Östergård, and Reiner Staszewski. Permutation codes invariant under isometries. *Designs, Codes, and Cryptography*, 75(3):497–507, June 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-9930-z`.

**Hiramine:2015:DMR**

[1822] Yutaka Hiramine and Chihiro Suetake. Difference matrices related to Sophie Germain primes $p$ using functions on the fields $F_{2p+1}$. *Designs, Codes, and Cryptography*, 75(3):509–518, June 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-9933-9`.

**Simone:2015:FPP**

[1823] Antonino Simone and Boris Skorić. False positive probabilities in $q$-ary Tardos codes: comparison of attacks. *Designs, Codes, and Cryptography*, 75(3):519–542, June 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-9937-5`.

**Gluesing-Luerssen:2015:FRP**

[1824] Heide Gluesing-Luerssen. Fourier-reflexive partitions and MacWilliams identities for additive codes. *Designs, Codes, and Cryptography*, 75 (3):543–563, June 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-9940-x`.

**Langlois:2015:WCA**

[1825] Adeline Langlois and Damien Stehlé. Worst-case to average-case reductions for module lattices. *Designs, Codes, and Cryptography*, 75(3):565–599, June 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-9938-4`.

**Kotsireas:2015:FCA**

[1826] I. Kotsireas and Edgar Martínez-Moro. Foreword: Computer algebra in coding theory and cryptography. *Designs, Codes, and Cryptography*, 76(1):1–2, July 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0041-2; http://link.springer.`

com/content/pdf/10.1007/s10623-015-0041-2.pdf.

**Villanueva:2015:ERB**

[1827] Mercè Villanueva, Fanxuan Zeng, and Jaume Pujol. Efficient representation of binary nonlinear codes: constructions and minimum distance computation. *Designs, Codes, and Cryptography*, 76(1):3–21, July 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-0028-4.

**Duck:2015:HDL**

[1828] Natalia Dück and Karl-Heinz Zimmermann. Heuristic decoding of linear codes using commutative algebra. *Designs, Codes, and Cryptography*, 76(1):23–35, July 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-0008-8.

**Hoholdt:2015:OCT**

[1829] Tom Høholdt, Fernando Piñero, and Peng Zeng. Optimal codes as Tanner codes with cyclic component codes. *Designs, Codes, and Cryptography*, 76(1):37–47, July 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9962-4.

**Geil:2015:IFR**

[1830] Olav Geil and Stefano Martin. An improvement of the Feng–Rao bound for primary codes. *Designs, Codes, and Cryptography*, 76(1):49–79, July 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9983-z.

**Olaya-Leon:2015:SGH**

[1831] Wilson Olaya-León and Claudia Granados-Pinzón. The second generalized Hamming weight of certain Castle codes. *Designs, Codes, and Cryptography*, 76(1):81–87, July 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9981-1.

**Galindo:2015:QCA**

[1832] Carlos Galindo and Fernando Hernando. Quantum codes from affine variety codes and their subfield-subcodes. *Designs, Codes, and Cryptography*, 76(1):89–100, July 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-0016-8.

**Munuera:2015:HCW**

[1833] Carlos Munuera. Hamming codes for wet paper steganography. *Designs, Codes, and Cryptography*, 76(1):101–111, July 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9998-5.

**Cusick:2015:TRS**

[1834] Thomas W. Cusick and Bryan Johns. Theory of 2-rotation symmetric cubic Boolean functions. *Designs, Codes, and Cryptography*, 76(1):113–133, July 2015. CODEN DCCREC. ISSN

0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9964-2.

**Biliotti:2015:DPP**

[1835] Mauro Biliotti, Alessandro Montinaro, and Eliana Francot. 2- $(v, k, 1)$ designs with a point-primitive rank 3 automorphism group of affine type. *Designs, Codes, and Cryptography*, 76 (2):135–171, August 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9925-9.

**Ozbudak:2015:SBM**

[1836] Ferruh Özbudak, Seher Tutdere, and Oguz Yayla. On some bounds on the minimum distance of cyclic codes over finite fields. *Designs, Codes, and Cryptography*, 76(2):173–178, August 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9927-7.

**Lee:2015:MFA**

[1837] Jooyoung Lee and Martijn Stam. MJH: a faster alternative to MDC-2. *Designs, Codes, and Cryptography*, 76 (2):179–205, August 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9936-6.

**Heger:2015:SPV**

[1838] Tamás Héger, Balázs Patkós, and Marcella Takáts. Search problems in vector spaces. *Designs, Codes, and Cryptography*, 76(2):207–216, August 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9941-9.

**Shaska:2015:TFS**

[1839] T. Shaska and C. Shor. Theta functions and symmetric weight enumerators for codes over imaginary quadratic fields. *Designs, Codes, and Cryptography*, 76 (2):217–235, August 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9943-7.

**Best:2015:MUW**

[1840] D. Best, H. Kharaghani, and H. Ramp. Mutually unbiased weighing matrices. *Designs, Codes, and Cryptography*, 76 (2):237–256, August 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9944-6.

**Dobson:2015:MIC**

[1841] Edward Dobson. Monomial isomorphisms of cyclic codes. *Designs, Codes, and Cryptography*, 76(2):257–267, August 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9945-5.

**Bernal:2015:PDL**

[1842] José Joaquín Bernal, Joaquim Borges, Cristina Fernández-Córdoba, and Mercè Villanueva. Permutation decoding of $\mathbf{Z}_2\mathbf{Z}_4$-linear codes. *Designs, Codes, and Cryptography*, 76 (2):269–277, August 2015. CODEN

DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9946-4.

**Li:2015:TCB**

[1843] Jiao Li, Claude Carlet, Xiangyong Zeng, Chunlei Li, Lei Hu, and Jinyong Shan. Two constructions of balanced Boolean functions with optimal algebraic immunity, high nonlinearity and good behavior against fast algebraic attacks. *Designs, Codes, and Cryptography*, 76(2):279–305, August 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9949-1.

**Chen:2015:NIC**

[1844] Eric Zhi Chen. A new iterative computer search algorithm for good quasi-twisted codes. *Designs, Codes, and Cryptography*, 76(2):307–323, August 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9950-8.

**Plantard:2015:LIL**

[1845] Thomas Plantard, Willy Susilo, and Zhenfei Zhang. LLL for ideal lattices: re-evaluation of the security of Gentry–Halevi's FHE scheme. *Designs, Codes, and Cryptography*, 76(2):325–344, August 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9957-1.

**Hu:2015:NPP**

[1846] Sihuang Hu, Shuxing Li, Tao Zhang, Tao Feng, and Gennian Ge. New pseudo-planar binomials in characteristic two and related schemes. *Designs, Codes, and Cryptography*, 76(2):345–360, August 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9958-0.

**Lo:2015:WMM**

[1847] Yuan-Hsun Lo, Hung-Lin Fu, and Yi-Hean Lin. Weighted maximum matchings and optimal equi-difference conflict-avoiding codes. *Designs, Codes, and Cryptography*, 76(2):361–372, August 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9961-5.

**Harada:2015:DRP**

[1848] Masaaki Harada. On a 5-design related to a putative extremal doubly even self-dual code of length a multiple of 24. *Designs, Codes, and Cryptography*, 76(3):373–384, September 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9963-3.

**Liu:2015:DCP**

[1849] Guo-Qiang Liu and Chen-Hui Jin. Differential cryptanalysis of PRESENT-like cipher. *Designs, Codes, and Cryptography*, 76(3):385–408, September 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.

com/article/10.1007/s10623-014-9965-1.

**Xu:2015:BNF**

[1850] Bangteng Xu. Bentness and nonlinearity of functions on finite groups. *Designs, Codes, and Cryptography*, 76(3): 409–430, September 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9968-y.

**Dunkelman:2015:AUF**

[1851] Orr Dunkelman, Nathan Keller, and Adi Shamir. Almost universal forgery attacks on AES-based MAC's. *Designs, Codes, and Cryptography*, 76(3): 431–449, September 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9969-x.

**Barwick:2015:ITS**

[1852] S. G. Barwick and Wen-Ai Jackson. An investigation of the tangent splash of a subplane of $\mathrm{PG}(2, \mathrm{q}^3)$. *Designs, Codes, and Cryptography*, 76(3): 451–468, September 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9971-3.

**Fujioka:2015:SSA**

[1853] Atsushi Fujioka, Koutarou Suzuki, Keita Xagawa, and Kazuki Yoneyama. Strongly secure authenticated key exchange from factoring, codes, and lattices. *Designs, Codes, and Cryptography*, 76(3):469–504, September 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9972-2.

**Le:2015:ADC**

[1854] Tung Le and Jamshid Moori. On the automorphisms of designs constructed from finite simple groups. *Designs, Codes, and Cryptography*, 76(3): 505–517, September 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9973-1.

**Dougherty:2015:CRH**

[1855] Steven Dougherty, Jon-Lark Kim, and Yoonjin Lee. Codes over rings and Hermitian lattices. *Designs, Codes, and Cryptography*, 76(3):519–535, September 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9974-0.

**Olmez:2015:PFO**

[1856] Oktay Olmez. Plateaued functions and one-and-half difference sets. *Designs, Codes, and Cryptography*, 76(3): 537–549, September 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9975-z.

**Evans:2015:DCE**

[1857] Anthony B. Evans, David Fear, and Rebecca J. Stones. Diagonally cyclic equitable rectangles. *Designs, Codes, and Cryptography*, 76(3):551–569, September 2015. CODEN DCCREC. ISSN

0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9977-x.

**Carlet:2015:EBF**

[1858] Claude Carlet and Deng Tang. Enhanced Boolean functions suitable for the filter model of pseudo-random generator. *Designs, Codes, and Cryptography*, 76(3):571–587, September 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9978-9.

**Wei:2015:CRS**

[1859] Hengjia Wei, Hui Zhang, and Gennian Ge. Completely reducible super-simple designs with block size five and index two. *Designs, Codes, and Cryptography*, 76(3):589–600, September 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9979-8.

**Dunkelman:2015:PTA**

[1860] Orr Dunkelman and Nathan Keller. Practical-time attacks against reduced variants of MISTY1. *Designs, Codes, and Cryptography*, 76(3):601–627, September 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9980-2.

**Liu:2015:CSW**

[1861] Yan Liu, Haode Yan, and Chunlei Liu. A class of six-weight cyclic codes and their weight distribution. *Designs, Codes, and Cryptography*, 77(1):1–9, October 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9984-y.

**Lu:2015:MDL**

[1862] Jiqiang Lu. A methodology for differential-linear cryptanalysis and its applications. *Designs, Codes, and Cryptography*, 77(1):11–48, October 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9985-x.

**Nakic:2015:TDD**

[1863] Anamari Nakić and Mario Osvin Pavcević. Tactical decompositions of designs over finite fields. *Designs, Codes, and Cryptography*, 77(1):49–60, October 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9988-7.

**Nishimaki:2015:VES**

[1864] Ryo Nishimaki and Keita Xagawa. Verifiably encrypted signatures with short keys based on the decisional linear problem and obfuscation for encrypted VES. *Designs, Codes, and Cryptography*, 77(1):61–98, October 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9986-9.

**Mesnager:2015:BVF**

[1865] Sihem Mesnager. Bent vectorial functions and linear codes from $o$-polynomials. *Designs, Codes, and Cryptography*, 77(1):99–116, October 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-9989-6`.

**Tang:2015:DUB**

[1866] Deng Tang, Claude Carlet, and Xiaohu Tang. Differentially 4-uniform bijections by permuting the inverse function. *Designs, Codes, and Cryptography*, 77(1):117–141, October 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-9992-y`.

**Kim:2015:FAP**

[1867] Sungwook Kim and Jung Hee Cheon. Fixed argument pairing inversion on elliptic curves. *Designs, Codes, and Cryptography*, 77(1):143–152, October 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-9993-x`.

**Cao:2015:SML**

[1868] Yonglin Cao, Jian Gao, and Fang-Wei Fu. Semisimple multivariable $\mathbf{F}_q$-linear codes over $\mathbf{F}_{q^l}$. *Designs, Codes, and Cryptography*, 77(1):153–177, October 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-9994-9`.

**Hong:2015:MLS**

[1869] Haibo Hong, Licheng Wang, and Yixian Yang. Minimal logarithmic signatures for the unitary group $U_n(q)$. *Designs, Codes, and Cryptography*, 77(1):179–191, October 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-9996-7`.

**Qian:2015:EAQ**

[1870] Jianfa Qian and Lina Zhang. Entanglement-assisted quantum codes from arbitrary binary linear codes. *Designs, Codes, and Cryptography*, 77(1):193–202, October 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-9997-6`.

**Winter:2015:LRS**

[1871] Stefaan De Winter, Sara Rottey, and Geertrui Van de Voorde. Linear representations of subgeometries. *Designs, Codes, and Cryptography*, 77(1):203–215, October 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-9999-4`.

**Bao:2015:CDO**

[1872] Jingjun Bao and Lijun Ji. The completion determination of optimal $(3, 4)$-packings. *Designs, Codes, and Cryptography*, 77(1):217–229, October 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.`

com/article/10.1007/s10623-014-0001-2.

**Sarkar:2015:PTA**

[1873] Santanu Sarkar, Sourav Sen Gupta, and Goutam Paul. Proving TLS-attack related open biases of RC4. *Designs, Codes, and Cryptography*, 77 (1):231–253, October 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-0003-0.

**Zeng:2015:SGC**

[1874] Min Zeng, Yuan Luo, and Guang Gong. Sequences with good correlation property based on depth and interleaving techniques. *Designs, Codes, and Cryptography*, 77(1):255–275, October 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-0004-z.

**Martinez:2015:EF**

[1875] Fabio Enrique Brochero Martínez. Explicit factorization of $x^{n-1} \in \mathbf{F}_q[x]$. *Designs, Codes, and Cryptography*, 77 (1):277–286, October 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-0005-y.

**Blake:2015:GES**

[1876] Ian Blake, Alfred Menezes, and Doug Stinson. Guest editorial: Special issue in honor of Scott A. Vanstone. *Designs, Codes, and Cryptography*, 77(2–3):287–299, December 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-015-0106-2; http://link.springer.com/content/pdf/10.1007/s10623-015-0106-2.pdf.

**Guo:2015:TBB**

[1877] Chuan Guo, Douglas R. Stinson, and Tran van Trung. On tight bounds for binary frameproof codes. *Designs, Codes, and Cryptography*, 77(2–3):301–319, December 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-015-0037-y.

**Lindner:2015:APC**

[1878] Charles C. Lindner, Mariusz Meszka, and Alexander Rosa. Almost 2-perfect 6-cycle systems. *Designs, Codes, and Cryptography*, 77(2–3):321–333, December 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-015-0049-7.

**Hachenberger:2015:PNB**

[1879] Dirk Hachenberger. Primitive normal bases for quartic and cubic extensions: a geometric approach. *Designs, Codes, and Cryptography*, 77(2–3):335–350, December 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-015-0051-0.

**Fuji-Hara:2015:PHF**

[1880] Ryoh Fuji-Hara. Perfect hash families of strength three with three rows from varieties on finite projective ge-

ometries. *Designs, Codes, and Cryptography*, 77(2–3):351–356, December 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0052-z`.

**Phelps:2015:EKC**

[1881] Kevin Phelps. Enumeration of Kerdock codes of length 64. *Designs, Codes, and Cryptography*, 77(2–3):357–363, December 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0053-y`.

**Jungnickel:2015:MAQ**

[1882] Dieter Jungnickel and Vladimir D. Tonchev. Maximal arcs and quasi-symmetric designs. *Designs, Codes, and Cryptography*, 77(2–3):365–374, December 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0065-7`.

**Laarhoven:2015:FSL**

[1883] Thijs Laarhoven, Michele Mosca, and Joop van de Pol. Finding shortest lattice vectors faster using quantum search. *Designs, Codes, and Cryptography*, 77(2–3):375–400, December 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0067-5; http://link.springer.com/content/pdf/10.1007/s10623-015-0067-5.pdf`.

**Chiasson:2015:QSA**

[1884] Sonia Chiasson and P. C. van Oorschot. Quantifying the security advantage of password expiration policies. *Designs, Codes, and Cryptography*, 77(2–3):401–408, December 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0071-9`.

**Archdeacon:2015:SIH**

[1885] D. S. Archdeacon, J. H. Dinitz, and D. M. Donovan. Square integer Heffter arrays with empty cells. *Designs, Codes, and Cryptography*, 77(2–3):409–426, December 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0076-4`.

**Silverberg:2015:IAV**

[1886] Alice Silverberg and Yuri G. Zarhin. Isogenies of abelian varieties over finite fields. *Designs, Codes, and Cryptography*, 77(2–3):427–439, December 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0078-2`.

**Libert:2015:LHS**

[1887] Benoît Libert, Thomas Peters, Marc Joye, and Moti Yung. Linearly homomorphic structure-preserving signatures and their applications. *Designs, Codes, and Cryptography*, 77(2–3):441–477, December 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http:`

//link.springer.com/article/10.1007/s10623-015-0079-1.

**Chee:2015:OLP**

[1888] Yeow Meng Chee, Charles J. Colbourn, and Alan Chi Hung Ling. Optimal low-power coding for error correction and crosstalk avoidance in on-chip data buses. *Designs, Codes, and Cryptography*, 77(2–3):479–491, December 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-015-0084-4.

**Dull:2015:HSC**

[1889] Michael Düll, Björn Haase, and Gesine Hinterwälder. High-speed Curve25519 on 8-bit, 16-bit, and 32-bit microcontrollers. *Designs, Codes, and Cryptography*, 77(2–3):493–514, December 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-015-0087-1; http://link.springer.com/content/pdf/10.1007/s10623-015-0087-1.pdf.

**Roettger:2015:SPT**

[1890] E. L. Roettger, H. C. Williams, and R. K. Guy. Some primality tests that eluded Lucas. *Designs, Codes, and Cryptography*, 77(2–3):515–539, December 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-015-0088-0.

**Hoffstein:2015:PEP**

[1891] Jeffrey Hoffstein and Joseph H. Silverman. PASS-Encrypt: a public key cryptosystem based on partial evaluation of polynomials. *Designs, Codes, and Cryptography*, 77(2–3):541–552, December 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-015-0089-z.

**Lamken:2015:AED**

[1892] E. R. Lamken. The asymptotic existence of DR$(v, k, k-1)$ $(v, k, k-1)$-BIBDs. *Designs, Codes, and Cryptography*, 77(2–3):553–562, December 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-015-0090-6.

**Zhang:2015:BVC**

[1893] Liang Feng Zhang and Reihaneh Safavi-Naini. Batch verifiable computation of outsourced functions. *Designs, Codes, and Cryptography*, 77(2–3):563–585, December 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-015-0092-4.

**Koblitz:2015:ROM**

[1894] Neal Koblitz and Alfred J. Menezes. The random oracle model: a twenty-year retrospective. *Designs, Codes, and Cryptography*, 77(2–3):587–610, December 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-015-0094-2.

**Andreeva:2015:OPH**

[1895] Elena Andreeva, Bart Mennink, and Bart Preneel. Open problems in hash function security. *Designs, Codes, and Cryptography*, 77(2–3):611–631, December 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0096-0`.

**Dinur:2015:RST**

[1896] Itai Dinur, Orr Dunkelman, Nathan Keller, and Adi Shamir. Reflections on slide with a twist attacks. *Designs, Codes, and Cryptography*, 77(2–3):633–651, December 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0098-y`.

**McGuire:2015:FRN**

[1897] Gary McGuire and Emrah Sercan Yilmaz. Further results on the number of rational points of hyperelliptic supersingular curves in characteristic 2. *Designs, Codes, and Cryptography*, 77(2–3):653–662, December 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0102-6`.

**Maurer:2015:ZKP**

[1898] Ueli Maurer. Zero-knowledge proofs of knowledge for group homomorphisms. *Designs, Codes, and Cryptography*, 77(2–3):663–676, December 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0103-5`.

**Frey:2015:NFH**

[1899] Gerhard Frey and Ernst Kani. Normal forms of hyperelliptic curves of genus 3. *Designs, Codes, and Cryptography*, 77(2–3):677–712, December 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0122-2`.

**Landrock:2015:PMP**

[1900] Peter Landrock. Power map permutations and the discrete log problem. *Designs, Codes, and Cryptography*, 77(2–3):713–724, December 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0128-9`.

**Okamoto:2015:ASC**

[1901] Tatsuaki Okamoto and Katsuyuki Takashima. Achieving short ciphertexts or short secret-keys for adaptively secure general inner-product encryption. *Designs, Codes, and Cryptography*, 77(2–3):725–771, December 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0131-1; http://link.springer.com/content/pdf/10.1007/s10623-015-0131-1.pdf`.

**Jungnickel:2016:EAI**

[1902] Dieter Jungnickel, Jennifer Key, and Chris Mitchell. Editorial for the 25th anniversary issue. *Designs, Codes, and Cryptography*, 78(1):1–3, January

2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-015-0158-3; http://link.springer.com/content/pdf/10.1007/s10623-015-0158-3.pdf.

**Carlet:2016:FDR**

[1903] Claude Carlet and Sihem Mesnager. Four decades of research on bent functions. *Designs, Codes, and Cryptography*, 78(1):5–50, January 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-015-0145-8.

**Galbraith:2016:RPE**

[1904] Steven D. Galbraith and Pierrick Gaudry. Recent progress on the elliptic curve discrete logarithm problem. *Designs, Codes, and Cryptography*, 78 (1):51–72, January 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-015-0146-7.

**Joux:2016:THD**

[1905] Antoine Joux and Cécile Pierrot. Technical history of discrete logarithms in small characteristic finite fields. *Designs, Codes, and Cryptography*, 78 (1):73–85, January 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-015-0147-6.

**Koblitz:2016:CCC**

[1906] Neal Koblitz and Alfred J. Menezes. Cryptocash, cryptocurrencies, and cryptocontracts. *Designs, Codes, and Cryptography*, 78(1):87–102, January 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-015-0148-5.

**Ng:2016:DDF**

[1907] Siaw-Lynn Ng and Maura Beth Paterson. Disjoint difference families and their applications. *Designs, Codes, and Cryptography*, 78(1):103–127, January 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-015-0149-4; http://link.springer.com/content/pdf/10.1007/s10623-015-0149-4.pdf.

**Niederreiter:2016:SSA**

[1908] Harald Niederreiter. A survey of some applications of finite fields. *Designs, Codes, and Cryptography*, 78 (1):129–139, January 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-015-0150-y.

**Pott:2016:APP**

[1909] Alexander Pott. Almost perfect and planar functions. *Designs, Codes, and Cryptography*, 78(1):141–195, January 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-015-0151-x.

**Moura:2016:FFC**

[1910] Lucia Moura, Gary L. Mullen, and Daniel Panario. Finite field construc-

tions of combinatorial arrays. *Designs, Codes, and Cryptography*, 78 (1):197–219, January 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0152-9`.

**Gordon:2016:SMC**

[1911] Daniel M. Gordon and Bernhard Schmidt. A survey of the multiplier conjecture. *Designs, Codes, and Cryptography*, 78(1):221–236, January 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0153-8`.

**Schmidt:2016:SSC**

[1912] Kai-Uwe Schmidt. Sequences with small correlation. *Designs, Codes, and Cryptography*, 78(1):237–267, January 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0154-7`.

**Fragouli:2016:SLN**

[1913] Christina Fragouli and Emina Soljanin. (secure) linear network coding multicast. *Designs, Codes, and Cryptography*, 78(1):269–310, January 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0155-6`.

**Etzion:2016:GGC**

[1914] T. Etzion and L. Storme. Galois geometries and coding theory. *Designs, Codes, and Cryptography*, 78 (1):311–350, January 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0156-5`.

**Broadbent:2016:QCB**

[1915] Anne Broadbent and Christian Schaffner. Quantum cryptography beyond quantum key distribution. *Designs, Codes, and Cryptography*, 78(1):351–382, January 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0157-4; http://link.springer.com/content/pdf/10.1007/s10623-015-0157-4.pdf`.

**Braun:2016:AWB**

[1916] Michael Braun. $q$-analogs of $t$-wise balanced designs from Borel subgroups. *Designs, Codes, and Cryptography*, 78 (2):383–390, February 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-0002-1`.

**Qu:2016:MCD**

[1917] Longjiang Qu, Yin Tan, Chao Li, and Guang Gong. More constructions of differentially 4-uniform permutations on $\mathbf{F}_{2^{2k}}$. *Designs, Codes, and Cryptography*, 78(2):391–408, February 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-0006-x`.

**Silberstein:2016:OCB**

[1918] Natalia Silberstein and Anna Gál. Optimal combinatorial batch codes based

on block designs. *Designs, Codes, and Cryptography*, 78(2):409–424, February 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-0007-9`.

**Delfs:2016:CIB**

[1919] Christina Delfs and Steven D. Galbraith. Computing isogenies between supersingular elliptic curves over $\mathbf{F}_p$. *Designs, Codes, and Cryptography*, 78 (2):425–440, February 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-0010-1`.

**Dagdelen:2016:ESA**

[1920] Özgür Dagdelen, David Galindo, and Pascal Véron. Extended security arguments for signature schemes. *Designs, Codes, and Cryptography*, 78 (2):441–461, February 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-0009-7`.

**Suda:2016:TFC**

[1921] Sho Suda. A two-fold cover of strongly regular graphs with spreads and association schemes of class five. *Designs, Codes, and Cryptography*, 78 (2):463–471, February 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-0012-z`.

**Madison:2016:CAE**

[1922] Adonus L. Madison and Junhua Wu. Conics arising from external points and their binary codes. *Designs, Codes, and Cryptography*, 78(2):473–491, February 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-0013-y`.

**Chen:2016:GCI**

[1923] Yu Chen, Jiang Zhang, Dongdai Lin, and Zhenfeng Zhang. Generic constructions of integrated PKE and PEKS. *Designs, Codes, and Cryptography*, 78 (2):493–526, February 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-0014-x`.

**Cossidente:2016:SC**

[1924] Antonio Cossidente and Francesco Pavese. On subspace codes. *Designs, Codes, and Cryptography*, 78 (2):527–531, February 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-0018-6`.

**Wu:2016:SIP**

[1925] Di Wu, Wenfeng Qi, and Huajin Chen. On the spectral immunity of periodic sequences restricted to binary annihilators. *Designs, Codes, and Cryptography*, 78(2):533–545, February 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-0019-5`.

**Gauravaram:2016:BIC**

[1926] Praveen Gauravaram, Nasour Bagheri, and Lars R. Knudsen. Building indif-

ferentiable compression functions from the PGV compression functions. *Designs, Codes, and Cryptography*, 78 (2):547–581, February 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-0020-z`.

**Lavrauw:2016:BCF**

[1927] Michel Lavrauw and John Sheekey. On BEL-configurations and finite semifields. *Designs, Codes, and Cryptography*, 78(3):583–603, March 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-0015-9`.

**Caullery:2016:EPP**

[1928] Florian Caullery, Kai-Uwe Schmidt, and Yue Zhou. Exceptional planar polynomials. *Designs, Codes, and Cryptography*, 78(3):605–613, March 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-0017-7`.

**Steinbach:2016:CQL**

[1929] Martin Steinbach and Dirk Hachenberger. A class of quaternary linear codes improving known minimum distances. *Designs, Codes, and Cryptography*, 78(3):615–627, March 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-0021-y`.

**Carlet:2016:QZD**

[1930] Claude Carlet, Guang Gong, and Yin Tan. Quadratic zero-difference balanced functions, APN functions and strongly regular graphs. *Designs, Codes, and Cryptography*, 78 (3):629–654, March 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-0022-x`.

**DeBeule:2016:NFT**

[1931] Jan De Beule, Jeroen Demeyer, Klaus Metsch, and Morgan Rodgers. A new family of tight sets in $\mathcal{Q}^+(\bigtriangledown, \mathrm{II})$. *Designs, Codes, and Cryptography*, 78 (3):655–678, March 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-0023-9`.

**Lo:2016:PUI**

[1932] Yuan-Hsun Lo, Wing Shing Wong, and Hung-Lin Fu. Partially user-irrepressible sequence sets and conflict-avoiding codes. *Designs, Codes, and Cryptography*, 78(3):679–691, March 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-0024-8`.

**delaCruz:2016:AGE**

[1933] Javier de la Cruz, Michael Kiermaier, and Alfred Wassermann. The automorphism group of an extremal $[120, 60, 24]$ code does not contain elements of order 29. *Designs, Codes, and Cryptography*, 78(3):693–702, March 2016. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-0025-7.

**Anonymous:2016:WES**

[1934] Anonymous. Weight enumerator of some irreducible cyclic codes. *Designs, Codes, and Cryptography*, 78(3):??, March 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-0026-6.

**Montanari:2016:ECM**

[1935] Andrea Montanari. Effective compression maps for torus-based cryptography. *Designs, Codes, and Cryptography*, 79(1):1–17, April 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-0031-9.

**Ji:2016:EOS**

[1936] Lijun Ji and Zhengwu Dong. Existence of optimal strong partially balanced 3-designs with block size four. *Designs, Codes, and Cryptography*, 79(1):19–36, April 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-0032-8.

**Miezaki:2016:UBV**

[1937] Tsuyoshi Miezaki and Hiroyuki Nakasora. An upper bound of the value of $t$ of the support $t$-designs of extremal binary doubly even self-dual codes. *Designs, Codes, and Cryptography*, 79(1):37–46, April 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-0033-7.

**Gluesing-Luerssen:2016:HWP**

[1938] Heide Gluesing-Luerssen. The homogeneous weight partition and its character-theoretic dual. *Designs, Codes, and Cryptography*, 79(1):47–61, April 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-015-0034-1.

**Park:2016:EIS**

[1939] Jong Hwan Park and Dong Hoon Lee. An efficient IBE scheme with tight security reduction in the random oracle model. *Designs, Codes, and Cryptography*, 79(1):63–85, April 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-015-0035-0.

**Faugere:2016:SCM**

[1940] Jean-Charles Faugère, Ayoub Otmani, Ludovic Perret, Frédéric de Portzamparc, and Jean-Pierre Tillich. Structural cryptanalysis of McEliece schemes with compact keys. *Designs, Codes, and Cryptography*, 79(1):87–112, April 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-015-0036-z.

**Crnkovic:2016:SDC**

[1941] Dean Crnković and Sanja Rukavina. Self-dual codes from extended orbit matrices of symmetric designs. *Designs, Codes, and Cryptography*, 79

(1):113–120, April 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0038-x`.

**Lee:2016:SUE**

[1942] Kwangsu Lee. Self-updatable encryption with short public parameters and its extensions. *Designs, Codes, and Cryptography*, 79(1):121–161, April 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0039-9`.

**Sahoo:2016:BCS**

[1943] Binod Kumar Sahoo and N. S. Narasimha Sastry. Binary codes of the symplectic generalized quadrangle of even order. *Designs, Codes, and Cryptography*, 79(1):163–170, April 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0040-3`.

**Bouyuklieva:2016:AOB**

[1944] Stefka Bouyuklieva, Wolfgang Willems, and Nikolay Yankov. On the automorphisms of order 15 for a binary self-dual $[96, 48, 20]$ code. *Designs, Codes, and Cryptography*, 79(1):171–182, April 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0043-0`.

**Bierbrauer:2016:PPP**

[1945] Jürgen Bierbrauer. Projective polynomials, a projection construction and a family of semifields. *Designs, Codes, and Cryptography*, 79(1):183–200, April 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0044-z`.

**Byrne:2016:TWC**

[1946] Eimear Byrne and Alison Sneyd. Two-weight codes, graphs and orthogonal arrays. *Designs, Codes, and Cryptography*, 79(2):201–217, May 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0042-1`.

**Compton:2016:UHM**

[1947] B. Compton, R. Craigen, and W. de Launey. Unreal $BH(n, 6)$'s and Hadamard matrices. *Designs, Codes, and Cryptography*, 79(2):219–229, May 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0045-y`.

**Ozen:2016:GWB**

[1948] Ibrahim Özen. Generalized weights and the Ball–Blokhuis congruence. *Designs, Codes, and Cryptography*, 79(2):231–235, May 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0046-x`.

**Moody:2016:IIS**

[1949] Dustin Moody, Souradyuti Paul, and Daniel Smith-Tone. Improved indifferentiability security bound for the

JH mode. *Designs, Codes, and Cryptography*, 79(2):237–259, May 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0047-9`.

**Albrecht:2016:PCR**

[1950] Martin R. Albrecht, Jean-Charles Faugère, Pooya Farshim, Gottfried Herold, and Ludovic Perret. Polly Cracker, revisited. *Designs, Codes, and Cryptography*, 79(2):261–302, May 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0048-8`.

**Jiang:2016:SSC**

[1951] Jing Jiang, Minquan Cheng, and Ying Miao. Strongly separable codes. *Designs, Codes, and Cryptography*, 79 (2):303–318, May 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0050-1`.

**Hiramine:2016:AGD**

[1952] Yutaka Hiramine. On automorphism groups of divisible designs acting regularly on the set of point classes. *Designs, Codes, and Cryptography*, 79(2):319–335, May 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0054-x`.

**Alavi:2016:SDA**

[1953] Seyed Hassan Alavi, Mohsen Bayat, and Ashraf Daneshkhah. Symmetric designs admitting flag-transitive and point-primitive automorphism groups associated to two dimensional projective special groups. *Designs, Codes, and Cryptography*, 79(2):337–351, May 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0055-9`.

**Liu:2016:CFW**

[1954] Yan Liu and Haode Yan. A class of five-weight cyclic codes and their weight distribution. *Designs, Codes, and Cryptography*, 79(2):353–366, May 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0056-8`.

**Zhang:2016:OSC**

[1955] Yijin Zhang, Yuan-Hsun Lo, and Wing Shing Wong. Optimal strongly conflict-avoiding codes of even length and weight three. *Designs, Codes, and Cryptography*, 79(2):367–382, May 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0057-7`.

**Semaev:2016:MPS**

[1956] Igor Semaev. MaxMinMax problem and sparse equations over finite fields. *Designs, Codes, and Cryptography*, 79(2):383–404, May 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0058-6`.

**Ghinelli:2016:EFG**

[1957] Dina Ghinelli, Dieter Jungnickel, Michel Lavrauw, and Alexander Pott. Editorial: Finite geometries. *Designs, Codes, and Cryptography*, 79 (3):405–406, June 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-016-0199-2; http://link.springer.com/content/pdf/10.1007/s10623-016-0199-2.pdf`.

**Nakic:2016:EPC**

[1958] Anamari Nakić and Leo Storme. On the extendability of particular classes of constant dimension codes. *Designs, Codes, and Cryptography*, 79 (3):407–422, June 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0115-1`.

**Cosgun:2016:FRR**

[1959] Ayhan Cosgun, Ferruh Özbudak, and Zülfükar Saygi. Further results on rational points of the curve $y^{q^n} - y = \gamma x^{q^h+1} - \alpha$ over $\mathbf{F}_{q^m}$. *Designs, Codes, and Cryptography*, 79(3):423–441, June 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0107-1`.

**Korchmaros:2016:NRD**

[1960] Gábor Korchmáros and Gábor P. Nagy. 3-nets realizing a diassociative loop in a projective plane. *Designs, Codes, and Cryptography*, 79(3):443–449, June 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-016-0176-9`.

**Beelen:2016:SDG**

[1961] Peter Beelen and Fernando Piñero. The structure of dual Grassmann codes. *Designs, Codes, and Cryptography*, 79(3):451–470, June 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0085-3`.

**DeWinter:2016:ASR**

[1962] Stefaan De Winter, Ellen Kamischke, and Zeying Wang. Automorphisms of strongly regular graphs with applications to partial difference sets. *Designs, Codes, and Cryptography*, 79 (3):471–485, June 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0109-z`.

**Bartoli:2016:CAQ**

[1963] Daniele Bartoli, Massimo Giulietti, and Giovanni Zini. Complete $(k, 3)$-arcs from quartic curves. *Designs, Codes, and Cryptography*, 79(3):487–505, June 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0073-7`.

**DeBruyn:2016:HHD**

[1964] Bart De Bruyn. Hyperplanes of Hermitian dual polar spaces of rank 3 containing a quad. *Designs, Codes, and Cryptography*, 79(3):507–533, June 2016. CODEN DCCREC. ISSN

0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-015-0080-8.

**Landjev:2016:EQG**

[1965] Ivan Landjev, Assia Rousseva, and Leo Storme. On the extendability of quasidivisible Griesmer arcs. *Designs, Codes, and Cryptography*, 79 (3):535–547, June 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-015-0114-2.

**Gillespie:2016:EFN**

[1966] Neil I. Gillespie, Michael Giudici, Daniel R. Hawtin, and Cheryl E. Praeger. Entry-faithful 2-neighbour transitive codes. *Designs, Codes, and Cryptography*, 79(3):549–564, June 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-015-0069-3.

**Kusejko:2016:SDC**

[1967] Katharina Kusejko. Simultaneous diagonalization of conics in $PG(2, q)$. *Designs, Codes, and Cryptography*, 79(3):565–581, June 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-015-0097-z.

**Betten:2016:P**

[1968] Anton Betten. The packings of PG$(3, 3)$. *Designs, Codes, and Cryptography*, 79(3):583–595, June 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-015-0074-6.

**Cossidente:2016:NLM**

[1969] Antonio Cossidente, Giuseppe Marino, and Francesco Pavese. Non-linear maximum rank distance codes. *Designs, Codes, and Cryptography*, 79 (3):597–609, June 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-015-0108-0.

**Hui:2016:ESI**

[1970] Alice M. W. Hui. Extending some induced substructures of an inversive plane. *Designs, Codes, and Cryptography*, 79(3):611–617, June 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-015-0083-5.

**Cooper:2016:TH**

[1971] Benjamin C. Cooper and Tim Penttila. Transitive hyperovals. *Designs, Codes, and Cryptography*, 79(3):619–623, June 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-015-0061-y.

**Fancsali:2016:HPS**

[1972] Szabolcs L. Fancsali and Péter Sziklai. Higgledy-piggledy subspaces and uniform subspace designs. *Designs, Codes, and Cryptography*, 79(3):625–645, June 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.

com/article/10.1007/s10623-016-0189-4.

**Chen:2016:NBH**

[1973] Eric Zhi Chen. New binary $h$-generator quasi-cyclic codes by augmentation and new minimum distance bounds. *Designs, Codes, and Cryptography*, 80(1):1–10, July 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0059-5; http://link.springer.com/article/10.1007/s10623-015-0059-5.

**Moreira:2016:ASA**

[1974] José Moreira, Marcel Fernández, and Grigory Kabatiansky. Almost separating and almost secure frameproof codes over $q$-ary alphabets. *Designs, Codes, and Cryptography*, 80(1):11–28, July 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0060-z; http://link.springer.com/article/10.1007/s10623-015-0060-z.

**Hofheinz:2016:TSS**

[1975] Dennis Hofheinz and Tibor Jager. Tightly secure signatures and public-key encryption. *Designs, Codes, and Cryptography*, 80(1):29–61, July 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0062-x; http://link.springer.com/article/10.1007/s10623-015-0062-x.

**Shparlinski:2016:SGB**

[1976] Igor E. Shparlinski. On small gaps between the elements of multiplicative subgroups of finite fields. *Designs, Codes, and Cryptography*, 80(1):63–71, July 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0063-9; http://link.springer.com/article/10.1007/s10623-015-0063-9.

**Jedwab:2016:CCE**

[1977] Jonathan Jedwab and Amy Wiebe. Constructions of complex equiangular lines from mutually unbiased bases. *Designs, Codes, and Cryptography*, 80(1):73–89, July 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0064-8; http://link.springer.com/article/10.1007/s10623-015-0064-8.

**Krotov:2016:PCD**

[1978] Denis S. Krotov. Perfect codes in Doob graphs. *Designs, Codes, and Cryptography*, 80(1):91–102, July 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0066-6; http://link.springer.com/article/10.1007/s10623-015-0066-6.

**Guo:2016:GCS**

[1979] Fuchun Guo, Willy Susilo, and Yi Mu. Generalized closest substring encryption. *Designs, Codes, and Cryptography*, 80(1):103–124, July 2016. CODEN

DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0068-4; http://link.springer.com/article/10.1007/s10623-015-0068-4.

**Davydov:2016:CPS**

[1980] Alexander A. Davydov, Giorgio Faina, Massimo Giulietti, Stefano Marcugini, and Fernanda Pambianco. On constructions and parameters of symmetric configurations $v_k$. *Designs, Codes, and Cryptography*, 80(1):125–147, July 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0070-x; http://link.springer.com/article/10.1007/s10623-015-0070-x.

**Chen:2016:GCD**

[1981] Yanling Chen, Markku Niemenmaa, and A. J. Han Vinck. A general check digit system based on finite groups. *Designs, Codes, and Cryptography*, 80(1):149–163, July 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0072-8; http://link.springer.com/article/10.1007/s10623-015-0072-8.

**Dutta:2016:CAS**

[1982] Sabyasachi Dutta, Raghvendra Singh Rohit, and Avishek Adhikari. Constructions and analysis of some efficient $t$-$(k, n)^*$-visual cryptographic schemes using linear algebraic techniques. *Designs, Codes, and Cryptography*, 80(1):165–196, July 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0075-5; http://link.springer.com/article/10.1007/s10623-015-0075-5.

**Ravagnani:2016:RMC**

[1983] Alberto Ravagnani. Rank-metric codes and their duality theory. *Designs, Codes, and Cryptography*, 80(1):197–216, July 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0077-3; http://link.springer.com/article/10.1007/s10623-015-0077-3.

**Hou:2016:SSM**

[1984] Xiang dong Hou, Ferruh Özbudak, and Yue Zhou. Switchings of semifield multiplications. *Designs, Codes, and Cryptography*, 80(2):217–239, August 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0081-7; http://link.springer.com/article/10.1007/s10623-015-0081-7.

**Ott:2016:JSD**

[1985] Udo Ott. On Jacobi sums, difference sets and partial difference sets in Galois domains. *Designs, Codes, and Cryptography*, 80(2):241–281, August 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0082-6; http://link.springer.com/article/10.1007/s10623-015-0082-6.

**Yamada:2016:CDO**

[1986] Kohei Yamada and Nobuko Miyamoto. A construction and decomposition of orthogonal arrays with non-prime-power numbers of symbols on the complement of a Baer subplane. *Designs, Codes, and Cryptography*, 80 (2):283–294, August 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s10623-015-0086-2; http://link.springer.com/article/10.1007/s10623-015-0086-2`.

**Li:2016:CWEa**

[1987] Chengju Li, Qin Yue, and Fang-Wei Fu. Complete weight enumerators of some cyclic codes. *Designs, Codes, and Cryptography*, 80 (2):295–315, August 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s10623-015-0091-5; http://link.springer.com/article/10.1007/s10623-015-0091-5`.

**Barwick:2016:CPC**

[1988] S. G. Barwick and Wen-Ai Jackson. Characterising pointsets in PG(4, q) that correspond to conics. *Designs, Codes, and Cryptography*, 80(2):317–332, August 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s10623-015-0093-3; http://link.springer.com/article/10.1007/s10623-015-0093-3`.

**Doroz:2016:HAE**

[1989] Yarkin Doröz, Yin Hu, and Berk Sunar. Homomorphic AES evaluation using the modified LTV scheme. *Designs, Codes, and Cryptography*, 80 (2):333–358, August 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s10623-015-0095-1; http://link.springer.com/article/10.1007/s10623-015-0095-1`.

**Londahl:2016:SAM**

[1990] Carl Löndahl, Thomas Johansson, Masoumeh Koochak Shooshtari, Mahmoud Ahmadian-Attari, and Mohammad Reza Aref. Squaring attacks on McEliece public-key cryptosystems using quasi-cyclic codes of even dimension. *Designs, Codes, and Cryptography*, 80(2):359–377, August 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s10623-015-0099-x; http://link.springer.com/article/10.1007/s10623-015-0099-x`.

**Bayram:2016:CSD**

[1991] Aysegul Bayram, Elif Segah Oztas, and Irfan Siap. Codes over $F_4 + vF_4$ and some DNA applications. *Designs, Codes, and Cryptography*, 80 (2):379–393, August 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s10623-015-0100-8; http://link.springer.com/article/10.1007/s10623-015-0100-8`.

**Candau:2016:CBC**

[1992] Marion Candau, Roland Gautier, and Johannes Huisman. Convo-

lutional block codes with cryptographic properties over the semidirect product $\mathbf{Z}/N\mathbf{Z}\times|\mathbf{Z}/M\mathbf{Z}$. *Designs, Codes, and Cryptography*, 80 (2):395–407, August 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0101-7; http://link.springer.com/article/10.1007/s10623-015-0101-7.

**Schmidt:2016:BSO**

[1993] Kai-Uwe Schmidt and Jürgen Willms. Barker sequences of odd length. *Designs, Codes, and Cryptography*, 80 (2):409–414, August 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0104-4; http://link.springer.com/article/10.1007/s10623-015-0104-4.

**Sheekey:2016:DDH**

[1994] John Sheekey. Dimensional dual hyperovals in classical polar spaces. *Designs, Codes, and Cryptography*, 80 (2):415–420, August 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0105-3; http://link.springer.com/article/10.1007/s10623-015-0105-3.

**LeGrow:2016:HCE**

[1995] Jason T. LeGrow, David A. Pike, and Jonathan Poulin. Hamiltonicity and cycle extensions in 0-block-intersection graphs of balanced incomplete block designs. *Designs, Codes, and Cryptography*, 80(3):421–433, September 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0110-6; http://link.springer.com/article/10.1007/s10623-015-0110-6.

**Nowak:2016:PGD**

[1996] Kathleen Nowak and Oktay Olmez. Partial geometric designs with prescribed automorphisms. *Designs, Codes, and Cryptography*, 80(3):435–451, September 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0111-5; http://link.springer.com/article/10.1007/s10623-015-0111-5.

**Ballico:2016:NSS**

[1997] E. Ballico. Non-special subsets of the set of points of a curve defined over a finite field. *Designs, Codes, and Cryptography*, 80(3):453–457, September 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0112-4; http://link.springer.com/article/10.1007/s10623-015-0112-4.

**Li:2016:MMA**

[1998] Rongjia Li and Chenhui Jin. Meet-in-the-middle attacks on 10-round AES-256. *Designs, Codes, and Cryptography*, 80(3):459–471, September 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0113-3; http://link.

springer.com/article/10.1007/s10623-015-0113-3.

**Lee:2016:CPT**

[1999] Ga Won Lee and Jin Hong. Comparison of perfect table cryptanalytic tradeoff algorithms. *Designs, Codes, and Cryptography*, 80(3):473–523, September 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0116-0; http://link.springer.com/article/10.1007/s10623-015-0116-0.

**Gong:2016:EDS**

[2000] Junqing Gong, Zhenfu Cao, Shaohua Tang, and Jie Chen. Extended dual system group and shorter unbounded hierarchical identity based encryption. *Designs, Codes, and Cryptography*, 80 (3):525–559, September 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0117-z; http://link.springer.com/article/10.1007/s10623-015-0117-z.

**Alahmadi:2016:LZC**

[2001] Adel Alahmadi, Hussain Alhazmi, Tor Helleseth, Rola Hijazi, Najat Muthana, and Patrick Solé. On the lifted Zetterberg code. *Designs, Codes, and Cryptography*, 80(3):561–576, September 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0118-y; http://link.springer.com/article/10.1007/s10623-015-0118-y.

**Hachenberger:2016:AER**

[2002] Dirk Hachenberger. Asymptotic existence results for primitive completely normal elements in extensions of Galois fields. *Designs, Codes, and Cryptography*, 80(3):577–586, September 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0119-x; http://link.springer.com/article/10.1007/s10623-015-0119-x.

**Guo:2016:EMM**

[2003] Jian Guo, Jérémy Jean, Ivica Nikolić, and Yu Sasaki. Extended meet-in-the-middle attacks on some Feistel constructions. *Designs, Codes, and Cryptography*, 80(3):587–618, September 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0120-4; http://link.springer.com/article/10.1007/s10623-015-0120-4.

**Ku-Cauich:2016:ACB**

[2004] Juan Carlos Ku-Cauich and Guillermo Morales-Luna. Authentication codes based on resilient Boolean maps. *Designs, Codes, and Cryptography*, 80(3): 619–633, September 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0121-3; http://link.springer.com/article/10.1007/s10623-015-0121-3.

**Stones:2016:LSA**

[2005] Rebecca J. Stones, Ming Su, Xiaoguang

Liu, Gang Wang, and Sheng Lin. A Latin square autotopism secret sharing scheme. *Designs, Codes, and Cryptography*, 80(3):635–650, September 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-015-0123-1; http://link.springer.com/content/pdf/10.1007/s10623-015-0123-1.pdf.

**Yan:2016:TCC**

[2006] Haode Yan and Chunlei Liu. Two classes of cyclic codes and their weight enumerator. *Designs, Codes, and Cryptography*, 81(1):1–9, October 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0125-z; http://link.springer.com/article/10.1007/s10623-015-0125-z.

**Kendall:2016:GTD**

[2007] Michelle Kendall and Keith M. Martin. Graph-theoretic design and analysis of key predistribution schemes. *Designs, Codes, and Cryptography*, 81(1):11–34, October 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0124-0; http://link.springer.com/article/10.1007/s10623-015-0124-0.

**Abiad:2016:SSG**

[2008] Aida Abiad and Willem H. Haemers. Switched symplectic graphs and their 2-ranks. *Designs, Codes, and Cryptography*, 81(1):35–41, October 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-015-0127-x; http://link.springer.com/content/pdf/10.1007/s10623-015-0127-x.pdf.

**Cheng:2016:PBS**

[2009] Shantian Cheng, Khoa Nguyen, and Huaxiong Wang. Policy-based signature scheme from lattices. *Designs, Codes, and Cryptography*, 81(1):43–74, October 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0126-y; http://link.springer.com/article/10.1007/s10623-015-0126-y.

**Banin:2016:RSD**

[2010] Matan Banin and Boaz Tsaban. A reduction of semigroup DLP to classic DLP. *Designs, Codes, and Cryptography*, 81(1):75–82, October 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0130-2; http://link.springer.com/article/10.1007/s10623-015-0130-2.

**Mullan:2016:HHF**

[2011] Ciaran Mullan and Boaz Tsaban. $SL_2$ homomorphic hash functions: worst case to average case reduction and short collision search. *Designs, Codes, and Cryptography*, 81(1):83–107, October 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/

article/10.1007/s10623-015-0129-8; http://link.springer.com/article/10.1007/s10623-015-0129-8.

**Guo:2016:SIK**

[2012] Chun Guo and Dongdai Lin. Separating invertible key derivations from non-invertible ones: sequential indifferentiability of 3-round Even–Mansour. *Designs, Codes, and Cryptography*, 81 (1):109–129, October 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0132-0; http://link.springer.com/article/10.1007/s10623-015-0132-0.

**Bamberg:2016:NRH**

[2013] John Bamberg, Melissa Lee, and Eric Swartz. A note on relative hemisystems of Hermitian generalised quadrangles. *Designs, Codes, and Cryptography*, 81 (1):131–144, October 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0135-x; http://link.springer.com/article/10.1007/s10623-015-0135-x.

**Braun:2016:NIS**

[2014] Michael Braun. New infinite series of 2-designs over the binary and ternary field. *Designs, Codes, and Cryptography*, 81(1):145–152, October 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0133-z; http://link.springer.com/article/10.1007/s10623-015-0133-z.

**Li:2016:CWEb**

[2015] Chengju Li, Sunghan Bae, Jaehyun Ahn, Shudi Yang, and Zheng-An Yao. Complete weight enumerators of some linear codes and their applications. *Designs, Codes, and Cryptography*, 81 (1):153–168, October 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0136-9; http://link.springer.com/article/10.1007/s10623-015-0136-9.

**Johnsen:2016:GKT**

[2016] Trygve Johnsen, Keisuke Shiromoto, and Hugues Verdure. A generalization of Kung's theorem. *Designs, Codes, and Cryptography*, 81 (1):169–178, October 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0139-6; http://link.springer.com/article/10.1007/s10623-015-0139-6.

**Rial:2016:BAB**

[2017] Alfredo Rial. Blind attribute-based encryption and oblivious transfer with fine-grained access control. *Designs, Codes, and Cryptography*, 81(2):179–223, November 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0134-y; http://link.springer.com/article/10.1007/s10623-015-0134-y.

**Liu:2016:CCC**

[2018] Yan Liu and Chunlei Liu. A class of cyclic codes whose duals have five zeros.

*Designs, Codes, and Cryptography*, 81 (2):225–238, November 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0138-7; http://link.springer.com/article/10.1007/s10623-015-0138-7.

**Kim:2016:CES**

[2019] Boran Kim and Yoonjin Lee. Construction of extremal self-dual codes over $\mathbf{z}_8$ and $\mathbf{z}_{16}$. *Designs, Codes, and Cryptography*, 81(2):239–257, November 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0137-8; http://link.springer.com/article/10.1007/s10623-015-0137-8.

**Merai:2016:LCP**

[2020] László Mérai and Arne Winterhof. On the linear complexity profile of some sequences derived from elliptic curves. *Designs, Codes, and Cryptography*, 81 (2):259–267, November 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0140-0; http://link.springer.com/article/10.1007/s10623-015-0140-0.

**Csajbok:2016:ELS**

[2021] Bence Csajbók and Corrado Zanella. On the equivalence of linear sets. *Designs, Codes, and Cryptography*, 81(2): 269–281, November 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0141-z; http://link.springer.com/article/10.1007/s10623-015-0141-z.

**Zhou:2016:LCT**

[2022] Zhengchun Zhou, Nian Li, Cuiling Fan, and Tor Helleseth. Linear codes with two or three weights from quadratic Bent functions. *Designs, Codes, and Cryptography*, 81(2): 283–295, November 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0144-9; http://link.springer.com/article/10.1007/s10623-015-0144-9.

**Liu:2016:FVF**

[2023] Zihui Liu and Xin-Wen Wu. The fullrank value function. *Designs, Codes, and Cryptography*, 81(2):297–315, November 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0159-2; http://link.springer.com/article/10.1007/s10623-015-0159-2.

**Cheng:2016:BCS**

[2024] Minquan Cheng, Jing Jiang, Haiyan Li, Ying Miao, and Xiaohu Tang. Bounds and constructions for $\overline{3}$-separable codes with length 3. *Designs, Codes, and Cryptography*, 81(2): 317–335, November 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0160-9; http://link.springer.com/article/10.1007/s10623-015-0160-9.

**Meidl:2016:MHJ**

[2025] Wilfried Meidl and Harald Niederreiter. Multisequences with high joint nonlinear complexity. *Designs, Codes, and Cryptography*, 81(2):337–346, November 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s10623-015-0142-y; http://link.springer.com/article/10.1007/s10623-015-0142-y`.

**Dougherty:2016:KRC**

[2026] Steven T. Dougherty and Cristina Fernández-Córdoba. Kernels and ranks of cyclic and negacyclic quaternary codes. *Designs, Codes, and Cryptography*, 81(2):347–364, November 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s10623-015-0163-6; http://link.springer.com/article/10.1007/s10623-015-0163-6`.

**Abel:2016:GHD**

[2027] R. Julian R. Abel, Robert F. Bailey, Andrea C. Burgess, Peter Danziger, and Eric Mendelsohn. On generalized Howell designs with block size three. *Designs, Codes, and Cryptography*, 81(2):365–391, November 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s10623-015-0162-7; http://link.springer.com/article/10.1007/s10623-015-0162-7`.

**Wang:2016:NCD**

[2028] Yanfeng Wang and Wenling Wu. New criterion for diffusion property and applications to improved GFS and EGFN. *Designs, Codes, and Cryptography*, 81(3):393–412, December 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s10623-015-0161-8; http://link.springer.com/article/10.1007/s10623-015-0161-8`.

**Eid:2016:SIC**

[2029] Abdulla Eid, Hilaf Hasson, Amy Ksir, and Justin Peachey. Suzuki-invariant codes from the Suzuki curve. *Designs, Codes, and Cryptography*, 81(3):413–425, December 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s10623-015-0164-5; http://link.springer.com/article/10.1007/s10623-015-0164-5`.

**Carvalho:2016:NWH**

[2030] Cícero Carvalho, Rafael Peixoto, and Fernando Torres. Near weights on higher dimensional varieties. *Designs, Codes, and Cryptography*, 81(3):427–443, December 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s10623-015-0165-4; http://link.springer.com/article/10.1007/s10623-015-0165-4`.

**Cossidente:2016:VSC**

[2031] Antonio Cossidente and Francesco Pavese. Veronese subspace codes. *Designs, Codes, and Cryptography*, 81(3):445–457, December 2016. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0166-3; http://link.springer.com/article/10.1007/s10623-015-0166-3.

**Wan:2016:IBC**

[2032] Daqing Wan and Qiang Wang. Index bounds for character sums of polynomials over finite fields. *Designs, Codes, and Cryptography*, 81(3): 459–468, December 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0170-7; http://link.springer.com/article/10.1007/s10623-015-0170-7.

**Kageyama:2016:GCO**

[2033] Yuuki Kageyama and Tatsuya Maruta. On the geometric constructions of optimal linear codes. *Designs, Codes, and Cryptography*, 81(3):469–480, December 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0167-2; http://link.springer.com/article/10.1007/s10623-015-0167-2.

**Zhan:2016:FTN**

[2034] Xiaoqin Zhan and Shenglin Zhou. Flag-transitive non-symmetric 2-designs with $(r, \lambda) = 1$ and sporadic socle. *Designs, Codes, and Cryptography*, 81 (3):481–487, December 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0171-6; http://link.springer.com/article/10.1007/s10623-015-0171-6.

**Zhou:2016:TPC**

[2035] Sanming Zhou. Total perfect codes in Cayley graphs. *Designs, Codes, and Cryptography*, 81(3):489–504, December 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0169-0; http://link.springer.com/article/10.1007/s10623-015-0169-0.

**Zheng:2016:LCP**

[2036] Yanbin Zheng, Pingzhi Yuan, and Dingyi Pei. Large classes of permutation polynomials over $\mathbf{F}_{q^2}$. *Designs, Codes, and Cryptography*, 81(3): 505–521, December 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0172-5; http://link.springer.com/article/10.1007/s10623-015-0172-5.

**Chen:2016:IAM**

[2037] Huaifeng Chen, Tingting Cui, and Meiqin Wang. Improving algorithm 2 in multidimensional (zero-correlation) linear cryptanalysis using $\chi^2$-method. *Designs, Codes, and Cryptography*, 81 (3):523–540, December 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0175-x; http://link.springer.com/article/10.1007/s10623-016-0175-x.

**Kim:2016:CIS**

[2038] Hyun Jin Kim and Yoonjin Lee. Complementary information set codes over GF($p$). *Designs, Codes,*

*and Cryptography*, 81(3):541–555, December 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0174-3; http://link.springer.com/article/10.1007/s10623-015-0174-3.

**Charpin:2017:ESI**

[2039] Pascale Charpin, Thomas Johansson, Gohar Kyureghyan, Nicolas Sendrier, and Jean-Pierre Tillich. Editorial: Special issue on coding and cryptography. *Designs, Codes, and Cryptography*, 82 (1–2):1–2, January 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-016-0307-3; http://link.springer.com/content/pdf/10.1007/s10623-016-0307-3.pdf.

**Boura:2017:RC**

[2040] Christina Boura, Anne Canteaut, Lars R. Knudsen, and Gregor Leander. Reflection ciphers. *Designs, Codes, and Cryptography*, 82 (1–2):3–25, January 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0143-x; http://link.springer.com/article/10.1007/s10623-015-0143-x.

**Ronjom:2017:IAA**

[2041] Sondre Rønjom. Improving algebraic attacks on stream ciphers based on linear feedback shift register over $\mathbf{F}_{2^k}$. *Designs, Codes, and Cryptography*, 82 (1–2):27–41, January 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0212-9; http://link.springer.com/article/10.1007/s10623-016-0212-9.

**Zajac:2017:UBC**

[2042] Pavol Zajac. Upper bounds on the complexity of algebraic cryptanalysis of ciphers with a low multiplicative complexity. *Designs, Codes, and Cryptography*, 82(1–2): 43–56, January 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0256-x; http://link.springer.com/article/10.1007/s10623-016-0256-x.

**Dyshko:2017:MET**

[2043] Serhii Dyshko. MacWilliams Extension Theorem for MDS codes over a vector space alphabet. *Designs, Codes, and Cryptography*, 82(1–2): 57–67, January 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0247-y; http://link.springer.com/article/10.1007/s10623-016-0247-y.

**Bezzateev:2017:LBC**

[2044] Sergey Bezzateev and Natalia Shekhunova. Lower bound of covering radius of binary irreducible Goppa codes. *Designs, Codes, and Cryptography*, 82 (1–2):69–76, January 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0173-

4; http://link.springer.com/article/10.1007/s10623-015-0173-4.

**Gupta:2017:DCR**

[2045] Kishan Chand Gupta, Sumit Kumar Pandey, and Ayineedi Venkateswarlu. On the direct construction of recursive MDS matrices. *Designs, Codes, and Cryptography*, 82(1–2): 77–94, January 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0233-4; http://link.springer.com/article/10.1007/s10623-016-0233-4.

**Chakraborty:2017:RTO**

[2046] Kaushik Chakraborty, Sumanta Sarkar, Subhamoy Maitra, Bodhisatwa Mazumdar, Debdeep Mukhopadhyay, and Emmanuel Prouff. Redefining the transparency order. *Designs, Codes, and Cryptography*, 82(1–2):95–115, January 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0250-3; http://link.springer.com/article/10.1007/s10623-016-0250-3.

**Minier:2017:IID**

[2047] Marine Minier. Improving impossible-differential attacks against Rijndael-160 and Rijndael-224. *Designs, Codes, and Cryptography*, 82(1–2): 117–129, January 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0206-7; http://link.springer.com/article/10.1007/s10623-016-0206-7.

**Sarkar:2017:RNR**

[2048] Santanu Sarkar and Ayineedi Venkateswarlu. Revisiting (nested) Roos bias in RC4 key scheduling algorithm. *Designs, Codes, and Cryptography*, 82(1–2): 131–148, January 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0219-2; http://link.springer.com/article/10.1007/s10623-016-0219-2.

**Bhattacharya:2017:SPB**

[2049] Srimanta Bhattacharya and Sumanta Sarkar. On some permutation binomials and trinomials over $\mathbf{F}_{2^n}$. *Designs, Codes, and Cryptography*, 82(1–2):149–160, January 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0229-0; http://link.springer.com/article/10.1007/s10623-016-0229-0.

**Tibouchi:2017:IEC**

[2050] Mehdi Tibouchi and Taechan Kim. Improved elliptic curve hashing and point representation. *Designs, Codes, and Cryptography*, 82(1–2): 161–177, January 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0288-2; http://link.springer.com/article/10.1007/s10623-016-0288-2.

**Gupta:2017:TGC**

[2051] Kishan Chand Gupta, Sumit Kumar Pandey, and Ayineedi Venkateswarlu.

Towards a general construction of recursive MDS diffusion layers. *Designs, Codes, and Cryptography*, 82(1–2):179–195, January 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0261-0; http://link.springer.com/article/10.1007/s10623-016-0261-0.

**Dyachkov:2017:CFC**

[2052] A. G. D'yachkov, I. V. Vorobyev, N. A. Polyanskii, and V. Yu. Shchukin. Cover-free codes and separating system codes. *Designs, Codes, and Cryptography*, 82(1–2):197–209, January 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0265-9; http://link.springer.com/article/10.1007/s10623-016-0265-9.

**Dyachkov:2017:SDL**

[2053] A. G. D'yachkov, I. V. Vorobyev, N. A. Polyanskii, and V. Yu. Shchukin. Symmetric disjunctive list-decoding codes. *Designs, Codes, and Cryptography*, 82(1–2):211–229, January 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0278-4; http://link.springer.com/article/10.1007/s10623-016-0278-4.

**Dyachkov:2017:ACF**

[2054] Arkadii D'yachkov, Ilya Vorobyev, Nikita Polyanskii, and Vladislav Shchukin. Almost cover-free codes and designs. *Designs, Codes, and Cryptography*, 82(1–2):231–247, January 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0279-3; http://link.springer.com/article/10.1007/s10623-016-0279-3.

**Guneri:2017:HWB**

[2055] Cem Güneri, Ferruh Özbudak, and Funda Özdemir. Hasse–Weil bound for additive cyclic codes. *Designs, Codes, and Cryptography*, 82(1–2):249–263, January 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0198-3; http://link.springer.com/article/10.1007/s10623-016-0198-3.

**Anbar:2017:IPQ**

[2056] Nurdagül Anbar, Wilfried Meidl, and Alev Topuzoglu. Idempotent and $p$-potent quadratic functions: distribution of nonlinearity and co-dimension. *Designs, Codes, and Cryptography*, 82(1–2):265–291, January 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0213-8; http://link.springer.com/article/10.1007/s10623-016-0213-8.

**Gritsenko:2017:SCN**

[2057] Vladimir Gritsenko, Grigory Kabatiansky, Vladimir Lebedev, and Alexey Maevskiy. Signature codes for noisy multiple access adder channel. *Designs, Codes, and Cryptography*, 82(1–2):293–299, January 2017. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0228-1; http://link.springer.com/article/10.1007/s10623-016-0228-1.

**Maitin-Shepard:2017:OSI**

[2058] Jeremy Maitin-Shepard. Optimal software-implemented Itoh–Tsujii inversion for $\mathbf{F}_{2^m}$. *Designs, Codes, and Cryptography*, 82(1–2):301–318, January 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0260-1; http://link.springer.com/article/10.1007/s10623-016-0260-1.

**Michel:2017:GCD**

[2059] Jerod Michel and Baokun Ding. A generalization of combinatorial designs and related codes. *Designs, Codes, and Cryptography*, 82(3):511–529, March 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0179-6; http://link.springer.com/article/10.1007/s10623-016-0179-6.

**Jiang:2017:ASF**

[2060] Yupeng Jiang and Dongdai Lin. On affine sub-families of Grain-like structures. *Designs, Codes, and Cryptography*, 82(3):531–542, March 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0178-7; http://link.springer.com/article/10.1007/s10623-016-0178-7.

**Fan:2017:FTB**

[2061] Yun Fan and Bangteng Xu. Fourier transforms and bent functions on faithful actions of finite abelian groups. *Designs, Codes, and Cryptography*, 82(3):543–558, March 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0177-8; http://link.springer.com/article/10.1007/s10623-016-0177-8.

**Kurosawa:2017:HML**

[2062] Kaoru Kurosawa, Hiroyuki Ohta, and Kenji Kakuta. How to make a linear network code (strongly) secure. *Designs, Codes, and Cryptography*, 82(3):559–582, March 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-016-0180-0; http://link.springer.com/content/pdf/10.1007/s10623-016-0180-0.pdf.

**Li:2017:GCP**

[2063] Shuxing Li, Hengjia Wei, and Gennian Ge. Generic constructions for partitioned difference families with applications: a unified combinatorial approach. *Designs, Codes, and Cryptography*, 82(3):583–599, March 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0182-y; http://link.springer.com/article/10.1007/s10623-016-0182-y.

**Sarkar:2017:NMD**

[2064] Palash Sarkar and Shashank Singh.

A new method for decomposition in the Jacobian of small genus hyperelliptic curves. *Designs, Codes, and Cryptography*, 82(3):601–616, March 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0184-9; http://link.springer.com/article/10.1007/s10623-016-0184-9.

**Delgado:2017:CAF**

[2065] Moises Delgado and Heeralal Janwa. On the conjecture on APN functions and absolute irreducibility of polynomials. *Designs, Codes, and Cryptography*, 82(3):617–627, March 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-015-0168-1; http://link.springer.com/article/10.1007/s10623-015-0168-1.

**Lakshmanan:2017:CVC**

[2066] R. Lakshmanan and S. Arumugam. Construction of a $(k, n)$-visual cryptography scheme. *Designs, Codes, and Cryptography*, 82(3):629–645, March 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0181-z; http://link.springer.com/article/10.1007/s10623-016-0181-z.

**Liu:2017:NGB**

[2067] Haiying Liu, Keqin Feng, and Rongquan Feng. Nonexistence of generalized bent functions from $\mathbf{Z}_2^n$ to $\mathbf{Z}_m$. *Designs, Codes, and Cryptography*, 82(3):647–662, March 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0192-9; http://link.springer.com/article/10.1007/s10623-016-0192-9.

**Yang:2017:CWE**

[2068] Shudi Yang and Zheng-An Yao. Complete weight enumerators of a family of three-weight linear codes. *Designs, Codes, and Cryptography*, 82(3):663–674, March 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0191-x; http://link.springer.com/article/10.1007/s10623-016-0191-x.

**Huggan:2017:SLA**

[2069] M. Huggan, G. L. Mullen, B. Stevens, and D. Thomson. Sudoku-like arrays, codes and orthogonality. *Designs, Codes, and Cryptography*, 82(3):675–693, March 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0190-y; http://link.springer.com/article/10.1007/s10623-016-0190-y.

**Li:2017:AGS**

[2070] Ming Li, Yupeng Jiang, and Dongdai Lin. The adjacency graphs of some feedback shift registers. *Designs, Codes, and Cryptography*, 82(3):695–713, March 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0187-

6; http://link.springer.com/article/10.1007/s10623-016-0187-6.

**Peng:2017:CDR**

[2071] Liqiang Peng, Lei Hu, Yao Lu, Jun Xu, and Zhangjie Huang. Cryptanalysis of Dual RSA. *Designs, Codes, and Cryptography*, 83(1):1–21, April 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0196-5; http://link.springer.com/article/10.1007/s10623-016-0196-5.

**Zheng:2017:DCL**

[2072] Hao Zheng, Yanxun Chang, and Junling Zhou. Direct constructions of large sets of Kirkman triple systems. *Designs, Codes, and Cryptography*, 83(1):23–32, April 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0197-4; http://link.springer.com/article/10.1007/s10623-016-0197-4.

**Lu:2017:AIS**

[2073] Xiao-Nan Lu and Masakazu Jimbo. Affine-invariant strictly cyclic Steiner quadruple systems. *Designs, Codes, and Cryptography*, 83(1):33–69, April 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0201-z; http://link.springer.com/article/10.1007/s10623-016-0201-z.

**Cheng:2017:CIP**

[2074] Minquan Cheng, Hung-Lin Fu, Jing Jiang, Yuan-Hsun Lo, and Ying Miao. Codes with the identifiable parent property for multimedia fingerprinting. *Designs, Codes, and Cryptography*, 83(1):71–82, April 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0203-x; http://link.springer.com/article/10.1007/s10623-016-0203-x.

**Ahn:2017:CWE**

[2075] Jaehyun Ahn, Dongseok Ka, and Chengju Li. Complete weight enumerators of a class of linear codes. *Designs, Codes, and Cryptography*, 83(1):83–99, April 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0205-8; http://link.springer.com/article/10.1007/s10623-016-0205-8.

**Napp:2017:MCC**

[2076] Diego Napp, Raquel Pinto, and Marisa Toste. On MDS convolutional codes over $\mathbf{Z}_{p^r}$. *Designs, Codes, and Cryptography*, 83(1):101–114, April 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0204-9; http://link.springer.com/article/10.1007/s10623-016-0204-9.

**Pace:2017:LCA**

[2077] Nicola Pace and Angelo Sonnino. On linear codes admitting large

automorphism groups. *Designs, Codes, and Cryptography*, 83(1):115–143, April 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0207-6; http://link.springer.com/article/10.1007/s10623-016-0207-6.

**Landerreche:2017:CSA**

[2078] Esteban Landerreche and David Fernández-Duque. A case study in almost-perfect security for unconditionally secure communication. *Designs, Codes, and Cryptography*, 83 (1):145–168, April 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-016-0210-y; http://link.springer.com/content/pdf/10.1007/s10623-016-0210-y.pdf.

**Krotov:2017:AGL**

[2079] Denis S. Krotov. On the automorphism groups of the $Z_2Z_4$-linear 1-perfect and preparata-like codes. *Designs, Codes, and Cryptography*, 83 (1):169–177, April 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0218-3; http://link.springer.com/article/10.1007/s10623-016-0218-3.

**Chen:2017:ACH**

[2080] Xiaotian Chen and Yue Zhou. Asynchronous channel hopping systems from difference sets. *Designs, Codes, and Cryptography*, 83(1):179–196, April 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0221-8; http://link.springer.com/article/10.1007/s10623-016-0221-8.

**Wu:2017:EFC**

[2081] Hongfeng Wu, Li Zhu, Rongquan Feng, and Siman Yang. Explicit factorizations of cyclotomic polynomials over finite fields. *Designs, Codes, and Cryptography*, 83(1):197–217, April 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0224-5; http://link.springer.com/article/10.1007/s10623-016-0224-5.

**Chen:2017:TNC**

[2082] Bocong Chen, Liren Lin, San Ling, and Hongwei Liu. Three new classes of optimal frequency-hopping sequence sets. *Designs, Codes, and Cryptography*, 83 (1):219–232, April 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0220-9; http://link.springer.com/article/10.1007/s10623-016-0220-9.

**Bartoli:2017:CPC**

[2083] Daniele Bartoli, Stefano Marcugini, and Fernanda Pambianco. On the completeness of plane cubic curves over finite fields. *Designs, Codes, and Cryptography*, 83(2):233–267, May 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0215-

6; http://link.springer.com/article/10.1007/s10623-016-0215-6.

**Aguglia:2017:IST**

[2084] Angela Aguglia and Luca Giuzzi. Intersection sets, three-character multisets and associated codes. *Designs, Codes, and Cryptography*, 83 (2):269–282, May 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0302-8; http://link.springer.com/article/10.1007/s10623-016-0302-8.

**Kuijper:2017:IAP**

[2085] M. Kuijper and R. Pinto. An iterative algorithm for parametrization of shortest length linear shift registers over finite chain rings. *Designs, Codes, and Cryptography*, 83 (2):283–305, May 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0226-3; http://link.springer.com/article/10.1007/s10623-016-0226-3.

**Heng:2017:EHW**

[2086] Ziling Heng and Qin Yue. Evaluation of the Hamming weights of a class of linear codes based on Gauss sums. *Designs, Codes, and Cryptography*, 83(2):307–326, May 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0222-7; http://link.springer.com/article/10.1007/s10623-016-0222-7.

**Sajadieh:2017:NCM**

[2087] Mahdi Sajadieh, Arash Mirzaei, Hamid Mala, and Vincent Rijmen. A new counting method to bound the number of active S-boxes in Rijndael and 3D. *Designs, Codes, and Cryptography*, 83(2):327–343, May 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0217-4; http://link.springer.com/article/10.1007/s10623-016-0217-4.

**Rua:2017:PSO**

[2088] I. F. Rúa. Primitive semifields of order $2^{4e}$. *Designs, Codes, and Cryptography*, 83(2):345–356, May 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0231-6; http://link.springer.com/article/10.1007/s10623-016-0231-6.

**Mennink:2017:OCS**

[2089] Bart Mennink. Optimal collision security in double block length hashing with single length key. *Designs, Codes, and Cryptography*, 83 (2):357–406, May 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0227-2; http://link.springer.com/article/10.1007/s10623-016-0227-2.

**Luo:2017:GAL**

[2090] Yiyuan Luo, Xuejia Lai, and Yujie Zhou. Generic attacks on the Lai–Massey scheme. *Designs,*

*Codes, and Cryptography*, 83(2):407–423, May 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0235-2; http://link.springer.com/article/10.1007/s10623-016-0235-2.

**Ma:2017:SNR**

[2091] Jingxue Ma, Tao Zhang, Tao Feng, and Gennian Ge. Some new results on permutation polynomials over finite fields. *Designs, Codes, and Cryptography*, 83(2):425–443, May 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0236-1; http://link.springer.com/article/10.1007/s10623-016-0236-1.

**Jiang:2017:NIL**

[2092] Yupeng Jiang and Jiangshuai Yang. On the number of irreducible linear transformation shift registers. *Designs, Codes, and Cryptography*, 83(2):445–454, May 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0240-5; http://link.springer.com/article/10.1007/s10623-016-0240-5.

**Wang:2017:SBC**

[2093] Xiang Wang and Fang-Wei Fu. On the snake-in-the-box codes for rank modulation under Kendall's $\tau$-metric. *Designs, Codes, and Cryptography*, 83(2):455–465, May 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0239-y; http://link.springer.com/article/10.1007/s10623-016-0239-y.

**Hao:2017:TDB**

[2094] Yonglin Hao and Willi Meier. Truncated differential based known-key attacks on round-reduced SIMON. *Designs, Codes, and Cryptography*, 83(2):467–492, May 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s10623-016-0242-3; http://link.springer.com/article/10.1007/s10623-016-0242-3.

**vanTrung:2017:SDR**

[2095] Tran van Trung. Simple $t$-designs: a recursive construction for arbitrary $t$. *Designs, Codes, and Cryptography*, 83(3):493–502, June 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Zhang:2017:QMC**

[2096] Tao Zhang and Gennian Ge. Quantum MDS codes with large minimum distance. *Designs, Codes, and Cryptography*, 83(3):503–517, June 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Gorla:2017:ORT**

[2097] Elisa Gorla and Maike Massierer. An optimal representation for the trace zero subgroup. *Designs, Codes, and Cryptography*, 83(3):519–548, June 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Nastase:2017:SMS**

[2098] Esmeralda Nastase and Papa Sissokho. The structure of the minimum size supertail of a subspace partition. *Designs, Codes, and Cryptography*, 83(3): 549–563, June 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Fan:2017:MPC**

[2099] Xinxin Fan, Adilet Otemissov, Francesco Sica, and Andrey Sidorenko. Multiple point compression on elliptic curves. *Designs, Codes, and Cryptography*, 83 (3):565–588, June 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Kim:2017:PDB**

[2100] Jon-Lark Kim and Nari Lee. A projection decoding of a binary extremal self-dual code of length 40. *Designs, Codes, and Cryptography*, 83(3):589–609, June 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Erzurumluoglu:2017:TTS**

[2101] Aras Erzurumluoglu and David A. Pike. Twofold triple systems without 2-intersecting Gray codes. *Designs, Codes, and Cryptography*, 83(3): 611–631, June 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Jin:2017:CBL**

[2102] Lingfei Jin and Haibin Kan. Construction of binary linear codes via rational function fields. *Designs, Codes, and Cryptography*, 83(3):633–638, June 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Martinez-Penas:2017:RMR**

[2103] Umberto Martínez-Peñas. On the roots and minimum rank distance of skew cyclic codes. *Designs, Codes, and Cryptography*, 83(3):639–660, June 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Bereg:2017:EPA**

[2104] Sergey Bereg, Linda Morales, and I. Hal Sudborough. Extending permutation arrays: improving MOLS bounds. *Designs, Codes, and Cryptography*, 83(3):661–683, June 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Guo:2017:PCK**

[2105] Victor J. W. Guo and Yiting Yang. Proof of a conjecture of Kløve on permutation codes under the Chebychev distance. *Designs, Codes, and Cryptography*, 83(3):685–690, June 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/content/pdf/10.1007/s10623-016-0255-y.pdf`.

**Tang:2017:LCF**

[2106] Chunming Tang, Can Xiang, and Keqin Feng. Linear codes with few weights from inhomogeneous quadratic functions. *Designs, Codes, and Cryptography*, 83(3):691–714, June 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Anonymous:2017:EN**

[2107] Anonymous. Editor's note. *Designs, Codes, and Cryptography*, 83(3):

715–716, June 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Blokhuis:2017:PSI**

[2108] Aart Blokhuis, Edwin R. van Dam, Willem H. Haemers, and Jack H. Koolen. Preface to the special issue dedicated to Andries E. Brouwer. *Designs, Codes, and Cryptography*, 84(1–2):1–2, July 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/content/pdf/10.1007/s10623-016-0308-2.pdf`.

**Koolen:2017:LTH**

[2109] Jack Koolen and Zhi Qiao. Light tails and the Hermitian dual polar graphs. *Designs, Codes, and Cryptography*, 84 (1–2):3–12, July 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Mathew:2017:NLB**

[2110] K. Ashik Mathew and Patric R. J. Östergård. New lower bounds for the Shannon capacity of odd cycles. *Designs, Codes, and Cryptography*, 84(1–2):13–22, July 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Bannai:2017:RDB**

[2111] Eiichi Bannai, Etsuko Bannai, and Yan Zhu. Relative $t$-designs in binary Hamming association scheme $H(n, 2)$. *Designs, Codes, and Cryptography*, 84(1–2):23–53, July 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Diego:2017:DMR**

[2112] V. Diego and M. A. Fiol. Distance mean-regular graphs. *Designs, Codes, and Cryptography*, 84(1–2):55–71, July 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Abdollahi:2017:DRC**

[2113] Alireza Abdollahi, Edwin R. van Dam, and Mojtaba Jazaeri. Distance-regular Cayley graphs with least eigenvalue $-2$. *Designs, Codes, and Cryptography*, 84(1–2):73–85, July 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/content/pdf/10.1007/s10623-016-0209-4.pdf`.

**Litjens:2017:SBN**

[2114] Bart Litjens, Sven Polak, and Alexander Schrijver. Semidefinite bounds for nonbinary codes based on quadruples. *Designs, Codes, and Cryptography*, 84 (1–2):87–100, July 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/content/pdf/10.1007/s10623-016-0216-5.pdf`.

**Soicher:2017:UDR**

[2115] Leonard H. Soicher. The uniqueness of a distance-regular graph with intersection array $\{32, 27, 8, 1; 1, 4, 27, 32\}$ and related results. *Designs, Codes, and Cryptography*, 84(1–2):101–108, July 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/content/pdf/10.1007/s10623-016-0223-6.pdf`.

**Cameron:2017:CTG**

[2116] Peter J. Cameron, Josephine Kusuma, and Patrick Solé. $\mathbf{Z}_4$-codes and their Gray map images as orthogonal arrays. *Designs, Codes, and Cryptography*, 84 (1–2):109–114, July 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Bishnoi:2017:CST**

[2117] Anurag Bishnoi and Bart De Bruyn. Characterizations of the Suzuki tower near polygons. *Designs, Codes, and Cryptography*, 84(1–2):115–133, July 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Cheng:2017:GTN**

[2118] Xi-Ming Cheng and Jack H. Koolen. A generalization of a theorem of Neumaier. *Designs, Codes, and Cryptography*, 84(1–2):135–142, July 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Dhaeseleer:2017:MSM**

[2119] Jozefien D'haeseleer, Klaus Metsch, Leo Storme, and Geertrui Van de Voorde. On the maximality of a set of mutually orthogonal Sudoku latin squares. *Designs, Codes, and Cryptography*, 84(1–2):143–152, July 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Cioaba:2017:GAT**

[2120] Sebastian M. Cioaba, Willem H. Haemers, and Jason R. Vermette. The graphs with all but two eigenvalues equal to $-2$ or 0. *Designs, Codes, and Cryptography*, 84(1–2):153–163, July 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/content/pdf/10.1007/s10623-016-0241-4.pdf`.

**Tonchev:2017:RSD**

[2121] Vladimir D. Tonchev. On resolvable Steiner 2-designs and maximal arcs in projective planes. *Designs, Codes, and Cryptography*, 84(1–2):165–172, July 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Munemasa:2017:GMS**

[2122] Akihiro Munemasa. Godsil–McKay switching and twisted Grassmann graphs. *Designs, Codes, and Cryptography*, 84(1–2):173–179, July 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Kovacs:2017:IAA**

[2123] István Kovács, Klavdija Kutnar, János Ruff, and Tamás Szőnyi. Integral automorphisms of affine spaces over finite fields. *Designs, Codes, and Cryptography*, 84(1–2):181–188, July 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Ghorbani:2017:ESM**

[2124] Ebrahim Ghorbani. On eigenvalues of Seidel matrices and Haemers' conjecture. *Designs, Codes, and Cryptography*, 84(1–2):189–195, July 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Blokhuis:2017:ASA**

[2125] A. Blokhuis, G. Marino, F. Mazzocca, and O. Polverino. On almost small and almost large super-Vandermonde

sets in GF($q$). *Designs, Codes, and Cryptography*, 84(1–2):197–201, July 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/content/pdf/10.1007/s10623-016-0254-z.pdf`.

**Klin:2017:NSC**

[2126] Mikhail Klin and Matan Ziv-Av. A non-Schurian coherent configuration on 14 points exists. *Designs, Codes, and Cryptography*, 84(1–2):203–221, July 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Cohen:2017:IBD**

[2127] Nathann Cohen and Dmitrii V. Pasechnik. Implementing Brouwer's database of strongly regular graphs. *Designs, Codes, and Cryptography*, 84 (1–2):223–235, July 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/content/pdf/10.1007/s10623-016-0264-x.pdf`.

**Neumaier:2017:BBR**

[2128] Arnold Neumaier. Bounding basis reduction properties. *Designs, Codes, and Cryptography*, 84(1–2): 237–259, July 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/content/pdf/10.1007/s10623-016-0273-9.pdf`.

**Martinez-Penas:2017:REC**

[2129] Umberto Martínez-Peñas and Ruud Pellikaan. Rank error-correcting pairs. *Designs, Codes, and Cryptography*, 84 (1–2):261–281, July 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Chandler:2017:SGH**

[2130] David B. Chandler, Peter Sin, and Qing Xiang. The Smith group of the hypercube graph. *Designs, Codes, and Cryptography*, 84(1–2):283–294, July 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Verhoeff:2017:SDH**

[2131] Tom Verhoeff. The spurs of D. H. Lehmer. *Designs, Codes, and Cryptography*, 84(1–2):295–310, July 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/content/pdf/10.1007/s10623-016-0301-9.pdf`.

**Jia:2017:CMM**

[2132] Huiwen Jia and Yupu Hu. Cryptanalysis of multilinear maps from ideal lattices: revisited. *Designs, Codes, and Cryptography*, 84(3):311–324, September 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Meng:2017:DRS**

[2133] Zhaoping Meng. Doubly resolvable Steiner quadruple systems and related designs. *Designs, Codes, and Cryptography*, 84(3):325–343, September 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Lavrauw:2017:BRF**

[2134] Michel Lavrauw and John Sheekey. The BEL-rank of finite semifields. *Designs, Codes, and Cryptography*, 84(3):345–358, September 2017. CODEN DC-

CREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Li:2017:CMD**

[2135] Shuxing Li and Gennian Ge. Constructions of maximum distance separable symbol-pair codes using cyclic and constacyclic codes. *Designs, Codes, and Cryptography*, 84(3):359–372, September 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**DeCaro:2017:PRS**

[2136] Angelo De Caro and Vincenzo Iovino. On the power of rewinding simulators in functional encryption. *Designs, Codes, and Cryptography*, 84(3):373–399, September 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Han:2017:CLH**

[2137] Hongyu Han, Daiyuan Peng, Udaya Parampalli, Zheng Ma, and Hongbin Liang. Construction of low-hit-zone frequency hopping sequences with optimal partial Hamming correlation by interleaving techniques. *Designs, Codes, and Cryptography*, 84(3):401–414, September 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Davis:2017:NCE**

[2138] James A. Davis, Sophie Huczynska, and Gary L. Mullen. Near-complete external difference families. *Designs, Codes, and Cryptography*, 84(3):415–424, September 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Salagean:2017:HOD**

[2139] Ana Salagean, R. Winter, Matei Mandache-Salagean, and Raphael C.-W. Phan. Higher order differentiation over finite fields with applications to generalising the cube attack. *Designs, Codes, and Cryptography*, 84(3):425–449, September 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/content/pdf/10.1007/s10623-016-0277-5.pdf`.

**DeWinter:2017:CPD**

[2140] Stefaan De Winter and Zeying Wang. Classification of partial difference sets in Abelian groups of order $4p^2$. *Designs, Codes, and Cryptography*, 84(3):451–461, September 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Jin:2017:QMC**

[2141] Lingfei Jin, Haibin Kan, and Jie Wen. Quantum MDS codes with relatively large minimum distance from Hermitian self-orthogonal codes. *Designs, Codes, and Cryptography*, 84(3):463–471, September 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Fan:2017:GSD**

[2142] Yun Fan and Liang Zhang. Galois self-dual constacyclic codes. *Designs, Codes, and Cryptography*, 84(3):473–492, September 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Martinsen:2017:PSV**

[2143] Thor Martinsen, Wilfried Meidl, and Pantelimon Stănică. Partial spread and

vectorial generalized bent functions. *Designs, Codes, and Cryptography*, 85 (1):1–13, October 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Shen:2017:PCX**

[2144] Gang Shen, Feng Liu, Zhengxin Fu, and Bin Yu. Perfect contrast XOR-based visual cryptography schemes via linear algebra. *Designs, Codes, and Cryptography*, 85(1):15–37, October 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Lee:2017:ERI**

[2145] Kwangsu Lee, Dong Hoon Lee, and Jong Hwan Park. Efficient revocable identity-based encryption via subset difference methods. *Designs, Codes, and Cryptography*, 85(1):39–76, October 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Strey:2017:LCG**

[2146] Eleonesio Strey and Sueli I. R. Costa. Lattices from codes over $\mathbf{Z}_q$: generalization of constructions $D$, $D'$ and $\overline{D}$. *Designs, Codes, and Cryptography*, 85 (1):77–95, October 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Kurz:2017:IUB**

[2147] Sascha Kurz. Improved upper bounds for partial spreads. *Designs, Codes, and Cryptography*, 85(1):97–106, October 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Steinke:2017:CFA**

[2148] Günter F. Steinke. Collineations of finite 2-affine planes. *Designs, Codes, and Cryptography*, 85(1):107–120, October 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Isik:2017:CMC**

[2149] Leyla Isik, Alev Topuzoglu, and Arne Winterhof. Complete mappings and Carlitz rank. *Designs, Codes, and Cryptography*, 85(1):121–128, October 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Horak:2017:CPR**

[2150] Peter Horak, Igor Semaev, and Zsolt Tuza. A combinatorial problem related to sparse systems of equations. *Designs, Codes, and Cryptography*, 85(1): 129–144, October 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Chen:2017:SAK**

[2151] Rongmao Chen, Yi Mu, Guomin Yang, Willy Susilo, and Fuchun Guo. Strong authenticated key exchange with auxiliary inputs. *Designs, Codes, and Cryptography*, 85(1):145–173, October 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Chen:2017:NSA**

[2152] Rongmao Chen, Yi Mu, Guomin Yang, Willy Susilo, Fuchun Guo, and Yang Zheng. A note on the strong authenticated key exchange with auxiliary inputs. *Designs, Codes, and Cryptography*, 85(1):175–178, October 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Yuan:2017:CQC**

[2153] Jian Yuan, Shixin Zhu, Xiaoshan Kai, and Ping Li. On the construction of quantum constacyclic codes. *Designs, Codes, and Cryptography*, 85(1): 179–190, October 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

**Otal:2017:CSC**

[2154] Kamil Otal and Ferruh Özbudak. Cyclic subspace codes via subspace polynomials. *Designs, Codes, and Cryptography*, 85(2):191–204, November 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-016-0297-1`.

**Yoshiara:2017:EAP**

[2155] Satoshi Yoshiara. Equivalences among plateaued APN functions. *Designs, Codes, and Cryptography*, 85(2):205–217, November 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-016-0298-0`.

**Zhou:2017:COL**

[2156] Limengnan Zhou, Daiyuan Peng, Hongbin Liang, Changyuan Wang, and Zheng Ma. Constructions of optimal low-hit-zone frequency hopping sequence sets. *Designs, Codes, and Cryptography*, 85(2):219–232, November 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-016-0299-z`.

**Tonchev:2017:LED**

[2157] Vladimir D. Tonchev. Linearly embeddable designs. *Designs, Codes, and Cryptography*, 85(2):233–247, November 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-016-0304-6`.

**Zhou:2017:BCS**

[2158] Junling Zhou and Yanxun Chang. Bounds and constructions of $t$-spontaneous emission error designs. *Designs, Codes, and Cryptography*, 85 (2):249–271, November 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-016-0300-x`.

**Kurosawa:2017:ALR**

[2159] Kaoru Kurosawa and Le Trieu Phong. Anonymous and leakage resilient IBE and IPE. *Designs, Codes, and Cryptography*, 85(2):273–298, November 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-016-0303-7`.

**Chen:2017:NOO**

[2160] Jingyuan Chen, Lijun Ji, and Yun Li. New optical orthogonal signature pattern codes with maximum collision parameter 2 and weight 4. *Designs, Codes, and Cryptography*, 85(2): 299–318, November 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-016-0310-8`.

**Fan:2017:NFD**

[2161] Yun Fan and Bangteng Xu. Nonlinear functions and difference sets on group actions. *Designs, Codes, and Cryptography*, 85(2):319–341, November 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-016-0312-6.

**Dong:2017:CBS**

[2162] Junwu Dong and Dingyi Pei. Construction for de Bruijn sequences with large stage. *Designs, Codes, and Cryptography*, 85(2):343–358, November 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-016-0309-1.

**Cuitino:2017:SPS**

[2163] Luis Felipe Tapia Cuitiño and Andrea Luigi Tironi. Some properties of skew codes over finite fields. *Designs, Codes, and Cryptography*, 85(2):359–380, November 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-016-0311-7.

**Alhakim:2017:SBS**

[2164] Abbas Alhakim and Maher Nouiehed. Stretching de Bruijn sequences. *Designs, Codes, and Cryptography*, 85(2):381–394, November 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-016-0314-4.

**Kolomeec:2017:GMD**

[2165] Nikolay Kolomeec. The graph of minimal distances of bent functions and its properties. *Designs, Codes, and Cryptography*, 85(3):395–410, December 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-016-0306-4.

**Zheng:2017:LSK**

[2166] Hao Zheng, Yanxun Chang, and Junling Zhou. Large sets of Kirkman triple systems of prime power sizes. *Designs, Codes, and Cryptography*, 85(3):411–423, December 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-016-0315-3.

**Chen:2017:SBS**

[2167] Zongchen Chen and Da Zhao. On symmetric BIBDs with the same 3-concurrence. *Designs, Codes, and Cryptography*, 85(3):425–436, December 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-016-0317-1.

**Tzanakis:2017:CAM**

[2168] Georgios Tzanakis, Lucia Moura, Daniel Panario, and Brett Stevens. Covering arrays from m-sequences and character sums. *Designs, Codes, and Cryptography*, 85(3):437–456, December 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https:

//link.springer.com/article/10.1007/s10623-016-0316-2.

**Cossidente:2017:SRG**

[2169] Antonio Cossidente and Francesco Pavese. Strongly regular graphs from classical generalized quadrangles. *Designs, Codes, and Cryptography*, 85(3): 457–470, December 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-016-0318-0.

**Li:2017:NTC**

[2170] Jianing Li and Yingpu Deng. Nonexistence of two classes of generalized bent functions. *Designs, Codes, and Cryptography*, 85(3):471–482, December 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-016-0319-z.

**Hagiwara:2017:CCC**

[2171] Manabu Hagiwara and Justin Kong. Consolidation for compact constraints and Kendall tau LP decodable permutation codes. *Designs, Codes, and Cryptography*, 85(3):483–521, December 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-016-0313-5.

**Egan:2017:ENG**

[2172] Ronan Egan. On equivalence of negaperiodic Golay pairs. *Designs, Codes, and Cryptography*, 85(3):523–532, December 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-016-0320-6.

**Wang:2017:NBP**

[2173] Xin Wang, Yiwei Zhang, Yiting Yang, and Gennian Ge. New bounds of permutation codes under Hamming metric and Kendall's $\tau$-metric. *Designs, Codes, and Cryptography*, 85(3): 533–545, December 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-016-0321-5.

**Rubin:2017:MPO**

[2174] Amir Rubin and Gera Weiss. Mapping prefer-opposite to prefer-one de Bruijn sequences. *Designs, Codes, and Cryptography*, 85(3):547–555, December 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-016-0322-4.

**Borges:2017:TEO**

[2175] Joaquim Borges and Cristina Fernández-Córdoba. There is exactly one $\mathbf{Z}_2\mathbf{Z}_4$-cyclic 1-perfect code. *Designs, Codes, and Cryptography*, 85(3):557–566, December 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-016-0323-3.

**delaCruz:2018:WDR**

[2176] Javier de la Cruz, Elisa Gorla, Hiram H. López, and Alberto Ravagnani. Weight distribution of rank-metric codes. *Designs, Codes, and Cryptography*, 86(1):1–16, January

2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-016-0325-1`.

**Watanabe:2018:TRC**

[2177] Yohei Watanabe and Junji Shikata. Timed-release computational secret sharing and threshold encryption. *Designs, Codes, and Cryptography*, 86 (1):17–54, January 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-016-0324-2`.

**Herold:2018:ACS**

[2178] Gottfried Herold, Elena Kirshanova, and Alexander May. On the asymptotic complexity of solving LWE. *Designs, Codes, and Cryptography*, 86 (1):55–83, January 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-016-0326-0`.

**Gnilke:2018:MCD**

[2179] Oliver Wilhelm Gnilke, Marcus Greferath, and Mario Osvin Pavcević. Mosaics of combinatorial designs. *Designs, Codes, and Cryptography*, 86 (1):85–95, January 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0328-6`.

**Kim:2018:FEC**

[2180] Jongkil Kim, Willy Susilo, Fuchun Guo, and Man Ho Au. Functional encryption for computational hiding in prime order groups via pair encodings. *Designs, Codes, and Cryptography*, 86 (1):97–120, January 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0327-7`.

**Guenda:2018:CGE**

[2181] Kenza Guenda, Somphong Jitman, and T. Aaron Gulliver. Constructions of good entanglement-assisted quantum error correcting codes. *Designs, Codes, and Cryptography*, 86 (1):121–136, January 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0330-z`.

**Ducas:2018:CVP**

[2182] Léo Ducas and Wessel P. J. van Woerden. The closest vector problem in tensored root lattices of type A and in their duals. *Designs, Codes, and Cryptography*, 86(1):137–150, January 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0332-x`.

**Wang:2018:CRT**

[2183] Qichun Wang, Chik How Tan, and Theo Fanuela Prabowo. On the covering radius of the third order Reed–Muller code RM(3, 7). *Designs, Codes, and Cryptography*, 86 (1):151–159, January 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0329-5`.

**Bartoli:2018:MPA**

[2184] Daniele Bartoli, Maria Montanucci, and Giovanni Zini. Multi point AG codes on the GK maximal curve. *Designs, Codes, and Cryptography*, 86 (1):161–177, January 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0333-9`.

**Hui:2018:SGS**

[2185] Alice M. W. Hui and B. G. Rodrigues. Switched graphs of some strongly regular graphs related to the symplectic graph. *Designs, Codes, and Cryptography*, 86(1):179–194, January 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0340-x`.

**Stinson:2018:CRT**

[2186] Douglas R. Stinson and Ruizhong Wei. Combinatorial repairability for threshold schemes. *Designs, Codes, and Cryptography*, 86(1):195–210, January 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0336-6`.

**Hu:2018:MPC**

[2187] Chuangqiang Hu and Shudi Yang. Multi-point codes over Kummer extensions. *Designs, Codes, and Cryptography*, 86(1):211–230, January 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0335-7`.

**Gavrilyuk:2018:DCL**

[2188] Alexander L. Gavrilyuk, Ilia Matkin, and Tim Penttila. Derivation of Cameron–Liebler line classes. *Designs, Codes, and Cryptography*, 86 (1):231–236, January 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0338-4`.

**Blackburn:2018:PSI**

[2189] Simon R. Blackburn, Marcus Greferath, Camilla Hollanti, Mario Osvin Pavcević, Joachim Rosenthal, Leo Storme, Ángeles Vázquez-Castro, and Alfred Wassermann. Preface to the special issue on network coding and designs. *Designs, Codes, and Cryptography*, 86 (2):237–238, February 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0443-4; https://link.springer.com/content/pdf/10.1007/s10623-017-0443-4.pdf`.

**Kiermaier:2018:OAG**

[2190] Michael Kiermaier, Sascha Kurz, and Alfred Wassermann. The order of the automorphism group of a binary $\vec{q}$-analog of the Fano plane is at most two. *Designs, Codes, and Cryptography*, 86 (2):239–250, February 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0360-6`.

**Kiermaier:2018:NSL**

[2191] Michael Kiermaier, Reinhard Laue, and Alfred Wassermann. A new series of large sets of subspace designs over the binary field. *Designs, Codes, and Cryptography*, 86(2):251–268, February 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0349-1.

**Liebhold:2018:NCF**

[2192] Dirk Liebhold, Gabriele Nebe, and Angeles Vazquez-Castro. Network coding with flags. *Designs, Codes, and Cryptography*, 86(2):269–284, February 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0361-5.

**Almeida:2018:MCC**

[2193] Paulo Almeida, Diego Napp, and Raquel Pinto. MDS 2D convolutional codes with optimal 1D horizontal projections. *Designs, Codes, and Cryptography*, 86(2):285–302, February 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0357-1.

**Napp:2018:CCC**

[2194] D. Napp, R. Pinto, and V. Sidorenko. Concatenation of convolutional codes and rank metric codes for multi-shot network coding. *Designs, Codes, and Cryptography*, 86(2):303–318, February 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0346-4.

**Horlemann-Trautmann:2018:EOA**

[2195] Anna-Lena Horlemann-Trautmann, Kyle Marshall, and Joachim Rosenthal. Extension of Overbeck's attack for Gabidulin-based cryptosystems. *Designs, Codes, and Cryptography*, 86(2):319–340, February 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0343-7.

**Neri:2018:GMR**

[2196] Alessandro Neri, Anna-Lena Horlemann-Trautmann, Tovohery Randrianarisoa, and Joachim Rosenthal. On the genericity of maximum rank distance and Gabidulin codes. *Designs, Codes, and Cryptography*, 86(2):341–363, February 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0354-4.

**Horlemann-Trautmann:2018:MER**

[2197] Anna-Lena Horlemann-Trautmann. Message encoding and retrieval for spread and cyclic orbit codes. *Designs, Codes, and Cryptography*, 86(2):365–386, February 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0377-x.

**Raviv:2018:CLR**

[2198] Netanel Raviv, Eitan Yaakobi, and Muriel Médard. Coding for locality

in reconstructing permutations. *Designs, Codes, and Cryptography*, 86 (2):387–418, February 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0378-9`.

**Silberstein:2018:ABL**

[2199] Natalia Silberstein and Alexander Zeh. Anticode-based locally repairable codes with high availability. *Designs, Codes, and Cryptography*, 86 (2):419–445, February 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0358-0`.

**Anonymous:2018:EN**

[2200] Anonymous. Editor's note. *Designs, Codes, and Cryptography*, 86 (3):447, March 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0467-4; https://link.springer.com/content/pdf/10.1007/s10623-018-0467-4.pdf`.

**Jungnickel:2018:BTB**

[2201] Dieter Jungnickel and Vladimir D. Tonchev. On Bonisoli's theorem and the block codes of Steiner triple systems. *Designs, Codes, and Cryptography*, 86(3):449–462, March 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0406-9; https://link.springer.com/content/pdf/10.1007/s10623-017-0406-9.pdf`.

**Borges:2018:DCC**

[2202] Joaquim Borges, Cristina Fernández-Córdoba, and Roger Ten-Valls. $\mathbf{Z}_2$-double cyclic codes. *Designs, Codes, and Cryptography*, 86(3):463–479, March 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0334-8`.

**Feltz:2018:SSA**

[2203] Michèle Feltz and Cas Cremers. Strengthening the security of authenticated key exchange against bad randomness. *Designs, Codes, and Cryptography*, 86(3):481–516, March 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0337-5`.

**Han:2018:TCS**

[2204] Shuai Han, Shengli Liu, Baodong Qin, and Dawu Gu. Tightly CCA-secure identity-based encryption with ciphertext pseudorandomness. *Designs, Codes, and Cryptography*, 86 (3):517–554, March 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0339-3`.

**Drapal:2018:FAT**

[2205] Ales Drápal and Viliam Valent. Few associative triples, isotopisms and groups. *Designs, Codes, and Cryptography*, 86(3):555–568, March 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

URL https://link.springer.com/article/10.1007/s10623-017-0341-9.

**Barrolleta:2018:PPD**

[2206] Roland D. Barrolleta and Mercè Villanueva. Partial permutation decoding for binary linear and $Z_4$-linear Hadamard codes. *Designs, Codes, and Cryptography*, 86(3):569–586, March 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0342-8.

**Jungnickel:2018:ESA**

[2207] Dieter Jungnickel, Yue Zhou, and Vladimir D. Tonchev. Extension sets, affine designs, and Hamada's conjecture. *Designs, Codes, and Cryptography*, 86(3):587–610, March 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0344-6.

**Bierbrauer:2018:FSO**

[2208] Jürgen Bierbrauer, Daniele Bartoli, Giorgio Faina, Stefano Marcugini, and Fernanda Pambianco. A family of semifields in odd characteristic. *Designs, Codes, and Cryptography*, 86(3):611–621, March 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0345-5.

**Lee:2018:CTM**

[2209] Jooyoung Lee, Atul Luykx, Bart Mennink, and Kazuhiko Minematsu. Connecting tweakable and multi-key blockcipher security. *Designs, Codes, and Cryptography*, 86(3):623–640, March 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0347-3; https://link.springer.com/content/pdf/10.1007/s10623-017-0347-3.pdf.

**Choi:2018:IBB**

[2210] Seung Geol Choi, Dana Dachman-Soled, Tal Malkin, and Hoeteck Wee. Improved, black-box, non-malleable encryption from semantic security. *Designs, Codes, and Cryptography*, 86(3):641–663, March 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0348-2.

**Dempwolff:2018:CEP**

[2211] Ulrich Dempwolff. CCZ equivalence of power functions. *Designs, Codes, and Cryptography*, 86(3):665–692, March 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0350-8. See [2760].

**Arce-Nazario:2018:NFB**

[2212] Rafael A. Arce-Nazario, Francis N. Castro, Oscar E. González, Luis A. Medina, and Ivelisse M. Rubio. New families of balanced symmetric functions and a generalization of Cusick, Li and Stănică's conjecture. *Designs, Codes, and Cryptography*, 86(3):693–701, March 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https:

//link.springer.com/article/10.1007/s10623-017-0351-7.

**Ding:2018:IFD**

[2213] Cunsheng Ding. Infinite families of 3-designs from a type of five-weight code. *Designs, Codes, and Cryptography*, 86 (3):703–719, March 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0352-6.

**Lin:2018:IMM**

[2214] Li Lin and Wenling Wu. Improved meet-in-the-middle attacks on reduced-round Kalyna-128/256 and Kalyna-256/512. *Designs, Codes, and Cryptography*, 86(4):721–741, April 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0353-5.

**Bricout:2018:AEM**

[2215] Remi Bricout, Sean Murphy, Kenneth G. Paterson, and Thyla van der Merwe. Analysing and exploiting the Mantin biases in RC4. *Designs, Codes, and Cryptography*, 86 (4):743–770, April 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0355-3; https://link.springer.com/content/pdf/10.1007/s10623-017-0355-3.pdf.

**Li:2018:PIW**

[2216] Fengwei Li and Qin Yue. The primitive idempotents and weight distributions of irreducible constacyclic codes. *Designs, Codes, and Cryptography*, 86 (4):771–784, April 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0356-2.

**Moreira:2018:CAS**

[2217] José Moreira, Marcel Fernández, and Grigory Kabatiansky. Constructions of almost secure frameproof codes with applications to fingerprinting schemes. *Designs, Codes, and Cryptography*, 86 (4):785–802, April 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0359-z.

**Zhang:2018:CCP**

[2218] Tao Zhang and Gennian Ge. Combinatorial constructions of packings in Grassmannian spaces. *Designs, Codes, and Cryptography*, 86(4):803–815, April 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0362-4.

**Olmez:2018:LBC**

[2219] Oktay Olmez. A link between combinatorial designs and three-weight linear codes. *Designs, Codes, and Cryptography*, 86(4):817–833, April 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0363-3.

**Vega:2018:CDW**

[2220] Gerardo Vega. A correction on the determination of the weight enumer-

ator polynomial of some irreducible cyclic codes. *Designs, Codes, and Cryptography*, 86(4):835–840, April 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0364-2`.

**Ding:2018:NCM**

[2221] Baokun Ding, Gennian Ge, Jun Zhang, Tao Zhang, and Yiwei Zhang. New constructions of MDS symbol-pair codes. *Designs, Codes, and Cryptography*, 86 (4):841–859, April 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0365-1`.

**Polak:2018:NNC**

[2222] Sven C. Polak. New nonbinary code bounds based on divisibility arguments. *Designs, Codes, and Cryptography*, 86 (4):861–874, April 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0366-0; https://link.springer.com/content/pdf/10.1007/s10623-017-0366-0.pdf`.

**Sudha:2018:CPM**

[2223] Irrinki Gnana Sudha and R. S. Selvaraj. Codes with a pomset metric and constructions. *Designs, Codes, and Cryptography*, 86(4):875–892, April 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0367-z`.

**Hou:2018:CNB**

[2224] Xiang-Dong Hou. Complexities of normal bases constructed from Gauss periods. *Designs, Codes, and Cryptography*, 86(4):893–905, April 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0368-y`.

**Colbourn:2018:ACM**

[2225] Charles J. Colbourn, Erin Lanus, and Kaushik Sarkar. Asymptotic and constructive methods for covering perfect hash families and covering arrays. *Designs, Codes, and Cryptography*, 86 (4):907–937, April 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0369-x`.

**Lin:2018:FCB**

[2226] Zhiqiang Lin, Dingyi Pei, Dongdai Lin, and Xiaolei Zhang. Fast construction of binary ring FCSRs for hardware stream ciphers. *Designs, Codes, and Cryptography*, 86(4):939–953, April 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0370-4`.

**Lee:2018:KAC**

[2227] Jooyoung Lee. Key alternating ciphers based on involutions. *Designs, Codes, and Cryptography*, 86(5):955–988, May 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/`

article/10.1007/s10623-017-0371-3.

**Ryabko:2018:PTS**

[2228] Boris Ryabko. Properties of two Shannon's ciphers. *Designs, Codes, and Cryptography*, 86(5):989–995, May 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0372-2.

**Bamberg:2018:ORN**

[2229] John Bamberg, Jesse Lansdown, and Melissa Lee. On $m$-ovoids of regular near polygons. *Designs, Codes, and Cryptography*, 86(5):997–1006, May 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0373-1.

**Zheng:2018:FCL**

[2230] Dabin Zheng and Jingjun Bao. Four classes of linear codes from cyclotomic cosets. *Designs, Codes, and Cryptography*, 86(5):1007–1022, May 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0374-0.

**Liu:2018:SFS**

[2231] Weihua Liu, Andrew Klapper, and Zhixiong Chen. Solving the FCSR synthesis problem for multi-sequences by lattice basis reduction. *Designs, Codes, and Cryptography*, 86(5):1023–1038, May 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0375-z.

**Morales:2018:AMT**

[2232] John Vincent S. Morales and Hajime Tanaka. An Assmus–Mattson theorem for codes over commutative association schemes. *Designs, Codes, and Cryptography*, 86(5):1039–1062, May 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0376-y.

**Lan:2018:CCQ**

[2233] Liantao Lan, Yanxun Chang, and Lidong Wang. Constructions of cyclic quaternary constant-weight codes of weight three and distance four. *Designs, Codes, and Cryptography*, 86(5):1063–1083, May 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0379-8.

**Harada:2018:BES**

[2234] Masaaki Harada. Binary extremal self-dual codes of length 60 and related codes. *Designs, Codes, and Cryptography*, 86(5):1085–1094, May 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0380-2.

**Bereg:2018:CPA**

[2235] Sergey Bereg, Avi Levy, and I. Hal Sudborough. Constructing permutation arrays from groups. *Designs, Codes, and*

*Cryptography*, 86(5):1095–1111, May 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0381-1`.

**Merai:2018:ECE**

[2236] László Mérai. On the elliptic curve endomorphism generator. *Designs, Codes, and Cryptography*, 86(5):1113–1129, May 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0382-0`.

**Gangopadhyay:2018:GNS**

[2237] Sugata Gangopadhyay, Bimal Mandal, and Pantelimon Stănică. Gowers $U_3$ norm of some classes of bent Boolean functions. *Designs, Codes, and Cryptography*, 86(5):1131–1148, May 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0383-z`.

**Wen:2018:CCS**

[2238] Jiejing Wen, Minghui Yang, Fangwei Fu, and Keqin Feng. Cyclotomic construction of strong external difference families in finite fields. *Designs, Codes, and Cryptography*, 86(5):1149–1159, May 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0384-y`.

**Cossidente:2018:ISF**

[2239] Antonio Cossidente and Francesco Pavese. On intriguing sets of finite symplectic spaces. *Designs, Codes, and Cryptography*, 86(5):1161–1174, May 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0387-8`.

**Donati:2018:GNR**

[2240] Giorgio Donati and Nicola Durante. A generalization of the normal rational curve in $\mathrm{PG}(\mathrm{d}, \mathrm{q}^{\mathrm{n}})$ and its associated non-linear MRD codes. *Designs, Codes, and Cryptography*, 86(6):1175–1184, June 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0388-7`.

**vanTrung:2018:RCS**

[2241] Tran van Trung. A recursive construction for simple $t$-designs using resolutions. *Designs, Codes, and Cryptography*, 86(6):1185–1200, June 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0389-6`.

**Shi:2018:TWC**

[2242] Minjia Shi, Zahra Sepasdar, Adel Alahmadi, and Patrick Solé. On two-weight $\mathbf{Z}_{2^k}$-codes. *Designs, Codes, and Cryptography*, 86(6):1201–1209, June 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0390-0`.

**Paul:2018:DCD**

[2243] Goutam Paul and Souvik Ray. On data complexity of distinguishing attacks versus message recovery attacks on stream ciphers. *Designs, Codes, and Cryptography*, 86(6):1211–1247, June 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0391-z`.

**Aydin:2018:SCC**

[2244] Nuh Aydin, Yasemin Cengellenmis, and Abdullah Dertli. On some constacyclic codes over $\mathbf{Z}_4[u]/\langle u^2-1\rangle$, their $\mathbf{Z}_4$ images, and new codes. *Designs, Codes, and Cryptography*, 86 (6):1249–1255, June 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0392-y`.

**Alahmadi:2018:SDD**

[2245] Adel Alahmadi, Funda Özdemir, and Patrick Solé. On self-dual double circulant codes. *Designs, Codes, and Cryptography*, 86(6):1257–1265, June 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0393-x`.

**Chen:2018:CCC**

[2246] Bocong Chen and Hongwei Liu. Constructions of cyclic constant dimension codes. *Designs, Codes, and Cryptography*, 86(6):1267–1279, June 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0394-9`.

**Lee:2018:CGD**

[2247] Chong-Dao Lee, Yaotsu Chang, and Chia an Liu. A construction of group divisible designs with block sizes 3 to 7. *Designs, Codes, and Cryptography*, 86(6):1281–1293, June 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0395-8`.

**Bi:2018:CCA**

[2248] Wenquan Bi, Zheng Li, Xiaoyang Dong, Lu Li, and Xiaoyun Wang. Conditional cube attack on round-reduced River Keyak. *Designs, Codes, and Cryptography*, 86(6):1295–1310, June 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0396-7`.

**Ihringer:2018:MMS**

[2249] Ferdinand Ihringer and Karen Meagher. Miklós–Manickam–Singhi conjectures on partial geometries. *Designs, Codes, and Cryptography*, 86(6):1311–1327, June 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0397-6`. See correction [2388].

**Su:2018:NOB**

[2250] Wei Su, Yang Yang, and Cuiling Fan. New optimal binary sequences with period $4p$ via interleaving Ding–Helleseth–Lam sequences. *Designs,*

*Codes, and Cryptography*, 86(6):1329–1338, June 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0398-5`.

**Zhang:2018:LRA**

[2251] Jie Zhang, Jie Chen, Junqing Gong, Aijun Ge, and Chuangui Ma. Leakage-resilient attribute based encryption in prime-order groups via predicate encodings. *Designs, Codes, and Cryptography*, 86(6):1339–1366, June 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0399-4`.

**Davis:2018:FCP**

[2252] James A. Davis and Oktay Olmez. A framework for constructing partial geometric difference sets. *Designs, Codes, and Cryptography*, 86(6):1367–1375, June 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0400-2`.

**Borges:2018:CLC**

[2253] Joaquim Borges and Cristina Fernández-Córdoba. A characterization of $\mathbf{Z}_2\mathbf{Z}_2[u]$-linear codes. *Designs, Codes, and Cryptography*, 86(7):1377–1389, July 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0401-1`.

**Gaborit:2018:PTK**

[2254] Philippe Gaborit, Ayoub Otmani, and Hervé Talé Kalachi. Polynomial-time key recovery attack on the Faure–Loidreau scheme based on Gabidulin codes. *Designs, Codes, and Cryptography*, 86(7):1391–1403, July 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0402-0`.

**Clayton:2018:NAD**

[2255] David Clayton. A note on almost difference sets in nonabelian groups. *Designs, Codes, and Cryptography*, 86(7):1405–1410, July 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0403-z`.

**Han:2018:SSR**

[2256] Shuai Han, Shengli Liu, and Lin Lyu. Super-strong RKA secure MAC, PKE and SE from tag-based hash proof system. *Designs, Codes, and Cryptography*, 86(7):1411–1449, July 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0404-y`.

**Dinh:2018:CDC**

[2257] Hai Q. Dinh, Abhay Kumar Singh, Sukhamoy Pattanayak, and Songsak Sriboonchitta. Cyclic DNA codes over the ring $\mathbf{F}_2 + u\mathbf{F}_2 + v\mathbf{F}_2 + uv\mathbf{F}_2 + v^2\mathbf{F}_2 + uv^2\mathbf{F}_2$. *Designs, Codes, and Cryptography*, 86(7):1451–1467, July

2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0405-x.

**Schmidt:2018:HRD**

[2258] Kai-Uwe Schmidt. Hermitian rank distance codes. *Designs, Codes, and Cryptography*, 86(7):1469–1481, July 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0407-8.

**Xiao:2018:NGC**

[2259] Zibi Xiao, Xiangyong Zeng, Chunlei Li, and Tor Helleseth. New generalized cyclotomic binary sequences of period $p^2$. *Designs, Codes, and Cryptography*, 86(7):1483–1497, July 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0408-7.

**Chen:2018:CCO**

[2260] Jingyuan Chen, Lijun Ji, and Yun Li. Combinatorial constructions of optimal $(m, n, 4, 2)$ optical orthogonal signature pattern codes. *Designs, Codes, and Cryptography*, 86(7):1499–1525, July 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0409-6.

**Wang:2018:APS**

[2261] SenPeng Wang, Bin Hu, and Yan Liu. The autocorrelation properties of single cycle polynomial $T$-functions. *Designs, Codes, and Cryptography*, 86(7):1527–1540, July 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0410-0.

**Wang:2018:UBL**

[2262] Qian Wang and Chenhui Jin. Upper bound of the length of truncated impossible differentials for AES. *Designs, Codes, and Cryptography*, 86(7):1541–1552, July 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0411-z.

**Shuai:2018:MCD**

[2263] Li Shuai and Miao Li. A method to calculate differential uniformity for permutations. *Designs, Codes, and Cryptography*, 86(7):1553–1563, July 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0412-y.

**Qian:2018:MLC**

[2264] Jianfa Qian and Lina Zhang. On MDS linear complementary dual codes and entanglement-assisted quantum codes. *Designs, Codes, and Cryptography*, 86(7):1565–1572, July 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0413-x.

**Kharaghani:2018:UOD**

[2265] Hadi Kharaghani and Sho Suda. Unbiased orthogonal designs. *Designs, Codes, and Cryptography*, 86

(7):1573–1588, July 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0414-9.

**Bartoli:2018:PPT**

[2266] Daniele Bartoli and Luciane Quoos. Permutation polynomials of the type $x^r g(x^s)$ over $\mathbf{F}_{q^{2n}}$. *Designs, Codes, and Cryptography*, 86(8):1589–1599, August 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0415-8.

**Xiong:2018:CDU**

[2267] Maosheng Xiong, Haode Yan, and Pingzhi Yuan. On a conjecture of differentially 8-uniform power functions. *Designs, Codes, and Cryptography*, 86(8):1601–1621, August 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0416-7.

**Emura:2018:CCS**

[2268] Keita Emura, Goichiro Hanaoka, Koji Nuida, Go Ohtake, Takahiro Matsuda, and Shota Yamada. Chosen ciphertext secure keyed-homomorphic public-key cryptosystems. *Designs, Codes, and Cryptography*, 86(8):1623–1683, August 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0417-6.

**Limniotis:2018:BFM**

[2269] Konstantinos Limniotis and Nicholas Kolokotronis. Boolean functions with maximum algebraic immunity: further extensions of the Carlet–Feng construction. *Designs, Codes, and Cryptography*, 86(8):1685–1706, August 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0418-5.

**Fernando:2018:SRP**

[2270] Neranga Fernando. Self-reciprocal polynomials and coterm polynomials. *Designs, Codes, and Cryptography*, 86(8):1707–1726, August 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0419-4.

**Shangguan:2018:NUB**

[2271] Chong Shangguan, Jingxue Ma, and Gennian Ge. New upper bounds for parent-identifying codes and traceability codes. *Designs, Codes, and Cryptography*, 86(8):1727–1737, August 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0420-y.

**Li:2018:COS**

[2272] Mingchao Li, Miao Liang, Beiliang Du, and Jingyuan Chen. A construction for optimal $c$-splitting authentication and secrecy codes. *Designs, Codes, and Cryptography*, 86(8):1739–1755, August 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0421-x.

**Liang:2018:FTP**

[2273] Hongxue Liang and Shenglin Zhou. Flag-transitive point-primitive automorphism groups of non-symmetric 2-$(v, k, 3)$ designs. *Designs, Codes, and Cryptography*, 86(8):1757–1766, August 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0422-9.

**Blanco-Chacon:2018:RMC**

[2274] I. Blanco-Chacón, E. Byrne, I. Duursma, and J. Sheekey. Rank metric codes and zeta functions. *Designs, Codes, and Cryptography*, 86(8):1767–1792, August 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0423-8.

**Yoshida:2018:ENI**

[2275] Maki Yoshida and Satoshi Obana. On the (in)efficiency of non-interactive secure multiparty computation. *Designs, Codes, and Cryptography*, 86(8):1793–1805, August 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0424-7; https://link.springer.com/content/pdf/10.1007/s10623-017-0424-7.pdf.

**Augot:2018:GGC**

[2276] Daniel Augot, Pierre Loidreau, and Gwezheneg Robert. Generalized Gabidulin codes over fields of any characteristic. *Designs, Codes, and Cryptography*, 86(8):1807–1848, August 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0425-6.

**Farran:2018:SFRa**

[2277] José I. Farrán, Pedro A. García-Sánchez, Benjamín A. Heredia, and Micah J. Leamer. The second Feng–Rao number for codes coming from telescopic semigroups. *Designs, Codes, and Cryptography*, 86(8):1849–1864, August 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0426-5.

**Mesnager:2018:ACB**

[2278] Sihem Mesnager, Ferruh Özbudak, and Ahmet Sinak. On the $p$-ary (cubic) bent and plateaued (vectorial) functions. *Designs, Codes, and Cryptography*, 86(8):1865–1892, August 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0427-4.

**Bibak:2018:ULC**

[2279] Khodakhast Bibak, Bruce M. Kapron, and Venkatesh Srinivasan. Unweighted linear congruences with distinct coordinates and the Varshamov–Tenengolts codes. *Designs, Codes, and Cryptography*, 86(9):1893–1904, September 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0428-3.

**Rifa:2018:HFP**

[2280] J. Rifà and Emilio Suárez Canedo. Hadamard full propelinear codes of type $Q$; rank and kernel. *Designs, Codes, and Cryptography*, 86(9):1905–1921, September 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0429-2.

**Sun:2018:ZCA**

[2281] Ling Sun, Huaifeng Chen, and Meiqin Wang. Zero-correlation attacks: statistical models independent of the number of approximations. *Designs, Codes, and Cryptography*, 86(9):1923–1945, September 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0430-9.

**Koga:2018:CED**

[2282] Yoshitaka Koga, Tatsuya Maruta, and Keisuke Shiromoto. On critical exponents of Dowling matroids. *Designs, Codes, and Cryptography*, 86(9):1947–1962, September 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0431-8.

**Zhang:2018:FTP**

[2283] Zhilin Zhang and Shenglin Zhou. Flag-transitive point-quasiprimitive 2-$(v, k, 2)$ designs. *Designs, Codes, and Cryptography*, 86(9):1963–1971, September 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0432-7.

**Schmidt:2018:NIG**

[2284] Kai-Uwe Schmidt and Yue Zhou. On the number of inequivalent Gabidulin codes. *Designs, Codes, and Cryptography*, 86(9):1973–1982, September 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0433-6.

**Otmani:2018:ICR**

[2285] Ayoub Otmani, Hervé Talé Kalachi, and Sélestin Ndjeya. Improved cryptanalysis of rank metric schemes based on Gabidulin codes. *Designs, Codes, and Cryptography*, 86(9):1983–1996, September 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0434-5.

**Xu:2018:SCM**

[2286] Jun Xu, Santanu Sarkar, Lei Hu, Zhangjie Huang, and Liqiang Peng. Solving a class of modular polynomial equations and its relation to modular inversion hidden number problem and inversive congruential generator. *Designs, Codes, and Cryptography*, 86(9):1997–2033, September 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0435-4.

**Ravagnani:2018:DCS**

[2287] Alberto Ravagnani. Duality of codes supported on regular lattices, with an

application to enumerative combinatorics. *Designs, Codes, and Cryptography*, 86(9):2035–2063, September 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0436-3`.

**delaCruz:2018:GCC**

[2288] Javier de la Cruz and Wolfgang Willems. On group codes with complementary duals. *Designs, Codes, and Cryptography*, 86(9):2065–2073, September 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0437-2`.

**Johnsen:2018:FAA**

[2289] Trygve Johnsen and Hugues Verdure. Flags of almost affine codes and the two-party wire-tap channel of type II. *Designs, Codes, and Cryptography*, 86(9):2075–2090, September 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0438-1`.

**Fan:2018:FTB**

[2290] Yun Fan and Bangteng Xu. Fourier transforms and bent functions on finite groups. *Designs, Codes, and Cryptography*, 86(9):2091–2113, September 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0439-0`.

**Dougherty:2018:GRC**

[2291] Steven T. Dougherty, Joseph Gildea, Rhian Taylor, and Alexander Tylyshchak. Group rings, $G$-codes and constructions of self-dual and formally self-dual codes. *Designs, Codes, and Cryptography*, 86(9):2115–2138, September 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0440-7`.

**Zhu:2018:CNB**

[2292] Shixin Zhu, Zhonghua Sun, and Ping Li. A class of negacyclic BCH codes and its application to quantum codes. *Designs, Codes, and Cryptography*, 86(10):2139–2165, October 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0441-6`.

**Chang:2018:LCS**

[2293] Seunghwan Chang and Jong Yoon Hyun. Linear codes from simplicial complexes. *Designs, Codes, and Cryptography*, 86(10):2167–2181, October 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0442-5`.

**Hodaj:2018:SNK**

[2294] Jezerca Hodaj, Melissa S. Keranen, Donald L. Kreher, and Leah Tollefson. Some new Kirkman signal sets. *Designs, Codes, and Cryptography*, 86(10):2183–2195, October 2018. CODEN DCCREC. ISSN 0925-

1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0445-2.

**Catalano:2018:HSS**

[2295] Dario Catalano, Dario Fiore, and Luca Nizzardo. Homomorphic signatures with sublinear public keys via asymmetric programmable hash functions. *Designs, Codes, and Cryptography*, 86(10):2197–2246, October 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0444-3.

**Bandi:2018:CSS**

[2296] Ramakrishna Bandi, Alexandre Fotue Tabue, and Edgar Martínez-Moro. On counting subring-submodules of free modules over finite commutative Frobenius rings. *Designs, Codes, and Cryptography*, 86(10):2247–2254, October 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0446-1.

**Ji:2018:GDD**

[2297] Lijun Ji. Group divisible designs with large block sizes. *Designs, Codes, and Cryptography*, 86(10):2255–2260, October 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0448-z.

**Li:2018:HLC**

[2298] Chengju Li. Hermitian LCD codes from cyclic codes. *Designs, Codes, and Cryptography*, 86(10):2261–2278, October 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0447-0.

**Faugere:2018:PDP**

[2299] Jean-Charles Faugère and Alexandre Wallet. The point decomposition problem over hyperelliptic curves. *Designs, Codes, and Cryptography*, 86(10):2279–2314, October 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0449-y.

**Bartoli:2018:ACA**

[2300] Daniele Bartoli, Maria Montanucci, and Giovanni Zini. AG codes and AG quantum codes from the GGS curve. *Designs, Codes, and Cryptography*, 86(10):2315–2344, October 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0450-5.

**Bagheri:2018:NCC**

[2301] Khadijeh Bagheri, Mohammad-Reza Sadeghi, and Daniel Panario. A non-commutative cryptosystem based on quaternion algebras. *Designs, Codes, and Cryptography*, 86(10):2345–2377, October 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0451-4.

**Li:2018:NCP**

[2302] Kangquan Li, Longjiang Qu, and Qiang Wang. New constructions of permutation polynomials of the form $x^r h\left(x^{q-1}\right)$ over $\mathbf{F}_{q^2}$. *Designs, Codes, and Cryptography*, 86(10):2379–2405, October 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0452-3`.

**Lee:2018:RHI**

[2303] Kwangsu Lee and Seunghwan Park. Revocable hierarchical identity-based encryption with shorter private keys and update keys. *Designs, Codes, and Cryptography*, 86(10):2407–2440, October 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0453-2`.

**Fan:2018:LCC**

[2304] Cuiling Fan. The linear complexity of a class of binary sequences with optimal autocorrelation. *Designs, Codes, and Cryptography*, 86(10):2441–2450, October 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0456-7`.

**Tian:2018:CAE**

[2305] Song Tian, Bao Li, Kunpeng Wang, and Wei Yu. Cover attacks for elliptic curves with cofactor two. *Designs, Codes, and Cryptography*, 86(11):2451–2468, November 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0457-6`.

**Liu:2018:NDL**

[2306] Yunwen Liu, Vincent Rijmen, and Gregor Leander. Nonlinear diffusion layers. *Designs, Codes, and Cryptography*, 86(11):2469–2484, November 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0458-5`.

**Shi:2018:SDN**

[2307] Minjia Shi, Liqin Qian, and Patrick Solé. On self-dual negacirculant codes of index two and four. *Designs, Codes, and Cryptography*, 86(11):2485–2494, November 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0455-0`.

**Wen:2018:RFE**

[2308] Yunhua Wen, Shengli Liu, and Shuai Han. Reusable fuzzy extractor from the decisional Diffie–Hellman assumption. *Designs, Codes, and Cryptography*, 86(11):2495–2512, November 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0459-4`.

**Zhou:2018:TWT**

[2309] Zhengchun Zhou. Three-weight ternary linear codes from a family of cyclic difference sets. *Designs, Codes, and Cryptography*, 86(11):2513–2523, November

2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0454-1.

**Derler:2018:PWE**

[2310] David Derler and Daniel Slamanig. Practical witness encryption for algebraic languages or how to encrypt under Groth–Sahai proofs. *Designs, Codes, and Cryptography*, 86(11):2525–2547, November 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0460-y.

**Liu:2018:HBT**

[2311] Jia Liu, Tibor Jager, Saqib A. Kakvi, and Bogdan Warinschi. How to build time-lock encryption. *Designs, Codes, and Cryptography*, 86(11):2549–2586, November 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0461-x; https://link.springer.com/content/pdf/10.1007/s10623-018-0461-x.pdf.

**Ge:2018:CSK**

[2312] Chunpeng Ge, Willy Susilo, Liming Fang, Jiandong Wang, and Yunqing Shi. A CCA-secure key-policy attribute-based proxy re-encryption in the adaptive corruption model for dropbox data sharing system. *Designs, Codes, and Cryptography*, 86(11):2587–2603, November 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0462-9.

**Carlet:2018:EHL**

[2313] Claude Carlet, Sihem Mesnager, Chunming Tang, and Yanfeng Qi. Euclidean and Hermitian LCD MDS codes. *Designs, Codes, and Cryptography*, 86(11):2605–2618, November 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0463-8.

**Mogilnykh:2018:EMW**

[2314] I. Yu. Mogilnykh and F. I. Solov'eva. On explicit minimum weight bases for extended cyclic codes related to Gold functions. *Designs, Codes, and Cryptography*, 86(11):2619–2627, November 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0464-7.

**Torres-Jimenez:2018:CAS**

[2315] Jose Torres-Jimenez and Idelfonso Izquierdo-Marquez. Covering arrays of strength three from extended permutation vectors. *Designs, Codes, and Cryptography*, 86(11):2629–2643, November 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0465-6.

**Zhang:2018:MCB**

[2316] Hui Zhang, Eitan Yaakobi, and Natalia Silberstein. Multiset combinatorial batch codes. *Designs, Codes, and Cryptography*, 86(11):2645–2660, November 2018. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0468-3.

**Antrobus:2018:LFP**

[2317] Jared Antrobus and Heide Gluesing-Luerssen. Lexicodes over finite principal ideal rings. *Designs, Codes, and Cryptography*, 86(11):2661–2676, November 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0469-2.

**Tan:2018:GIW**

[2318] Ming Ming Tan. Group invariant weighing matrices. *Designs, Codes, and Cryptography*, 86(12):2677–2702, December 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0466-5.

**Cogliati:2018:ASP**

[2319] Benoît Cogliati and Yannick Seurin. Analysis of the single-permutation encrypted Davies–Meyer construction. *Designs, Codes, and Cryptography*, 86(12):2703–2723, December 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0470-9.

**Costa:2018:FDF**

[2320] Simone Costa, Tao Feng, and Xiaomiao Wang. Frame difference families and resolvable balanced incomplete block designs. *Designs, Codes, and Cryptography*, 86(12):2725–2745, December 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0472-7.

**Cogliati:2018:TBC**

[2321] Benoît Cogliati. Tweaking a block cipher: multi-user beyond-birthday-bound security in the standard model. *Designs, Codes, and Cryptography*, 86(12):2747–2763, December 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0471-8.

**Zhan:2018:NSD**

[2322] Xiaoqin Zhan and Shenglin Zhou. Non-symmetric 2-designs admitting a two-dimensional projective linear group. *Designs, Codes, and Cryptography*, 86(12):2765–2773, December 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0474-5.

**Zhao:2018:RLC**

[2323] Xiao-Xin Zhao, Tian Tian, and Wen-Feng Qi. A ring-like cascade connection and a class of NFSRs with the same cycle structures. *Designs, Codes, and Cryptography*, 86(12):2775–2790, December 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0473-6.

**Kositwattanarerk:2018:PFC**

[2324] Wittawat Kositwattanarerk. Pseudocodeword-free criterion for codes with cycle-free Tanner graph. *Designs, Codes, and Cryptography*, 86(12):2791–2805, December 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0476-3`.

**Orhon:2018:SHF**

[2325] Neriman Gamze Orhon and Huseyin Hisil. Speeding up Huff form of elliptic curves. *Designs, Codes, and Cryptography*, 86(12):2807–2823, December 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0475-4`.

**Pinero:2018:NWS**

[2326] Fernando L. Piñero and Prasant Singh. A note on the weight spectrum of the Schubert code $C_\alpha(2, m)$. *Designs, Codes, and Cryptography*, 86(12):2825–2836, December 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0477-2`.

**Li:2018:LCR**

[2327] Jin Li, Aixian Zhang, and Keqin Feng. Linear codes over $\mathbf{F}_q[x]/(x^2)$ and $GR(p^2, m)$ reaching the Griesmer bound. *Designs, Codes, and Cryptography*, 86(12):2837–2855, December 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0479-0`.

**Lu:2018:SRG**

[2328] Xiaojuan Lu, Xiaolei Niu, and Haitao Cao. Some results on generalized strong external difference families. *Designs, Codes, and Cryptography*, 86(12):2857–2868, December 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0481-6`.

**Xu:2018:CCP**

[2329] Xiaofang Xu, Chunlei Li, Xiangyong Zeng, and Tor Helleseth. Constructions of complete permutation polynomials. *Designs, Codes, and Cryptography*, 86(12):2869–2892, December 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0480-7`.

**Farran:2018:SFRb**

[2330] José I. Farrán, Pedro A. García-Sánchez, and Benjamín A. Heredia. On the second Feng–Rao distance of algebraic geometry codes related to Arf semigroups. *Designs, Codes, and Cryptography*, 86(12):2893–2916, December 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0483-4`.

**Fan:2019:SSB**

[2331] Xinxin Fan, Guang Gong, Berry Schoenmakers, Francesco Sica, and Andrey Sidorenko. Secure simultaneous

bit extraction from Koblitz curves. *Designs, Codes, and Cryptography*, 87(1):1–13, January 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0484-3`.

**Liu:2019:SCL**

[2332] Haibo Liu and Qunying Liao. Several classes of linear codes with a few weights from defining sets over $\mathbf{F}_p + u\mathbf{F}_p$. *Designs, Codes, and Cryptography*, 87(1):15–29, January 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0478-1`.

**Fu:2019:IDU**

[2333] Shihui Fu and Xiutao Feng. Involutory differentially 4-uniform permutations from known constructions. *Designs, Codes, and Cryptography*, 87(1):31–56, January 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0482-5`.

**Ethier:2019:SMO**

[2334] John T. Ethier and Gary L. Mullen. Sets of mutually orthogonal Sudoku frequency squares. *Designs, Codes, and Cryptography*, 87(1):57–65, January 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0487-0`.

**Egan:2019:PUG**

[2335] Ronan Egan. Phased unitary Golay pairs, Butson Hadamard matrices and a conjecture of Ito's. *Designs, Codes, and Cryptography*, 87(1):67–74, January 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0485-2`.

**Mefenza:2019:PIG**

[2336] Thierry Mefenza and Damien Vergnaud. Polynomial interpolation of the generalized Diffie–Hellman and Naor–Reingold functions. *Designs, Codes, and Cryptography*, 87(1):75–85, January 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0486-1`.

**Shi:2019:HMW**

[2337] Minjia Shi, Hongwei Zhu, Patrick Solé, and Gérard D. Cohen. How many weights can a linear code have? *Designs, Codes, and Cryptography*, 87(1):87–95, January 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0488-z`.

**Cheng:2019:IBF**

[2338] Minquan Cheng, Jing Jiang, and Qiang Wang. Improved bounds on 2-frameproof codes with length 4. *Designs, Codes, and Cryptography*, 87(1):97–106, January 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https:`

//link.springer.com/article/10.1007/s10623-018-0490-5.

**Zhang:2019:COF**

[2339] Tao Zhang and Gennian Ge. Constructions of optimal Ferrers diagram rank metric codes. *Designs, Codes, and Cryptography*, 87(1):107–121, January 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0491-4.

**Soleimanian:2019:PVS**

[2340] Azam Soleimanian and Shahram Khazaei. Publicly verifiable searchable symmetric encryption based on efficient cryptographic components. *Designs, Codes, and Cryptography*, 87(1):123–147, January 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0489-y.

**Zhang:2019:NRS**

[2341] Shiyong Zhang and Gongliang Chen. New results on the state cycles of Trivium. *Designs, Codes, and Cryptography*, 87(1):149–162, January 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0493-2.

**Chen:2019:BBF**

[2342] Zhixiong Chen, Ting Gu, and Andrew Klapper. On the $q$-bentness of Boolean functions. *Designs, Codes, and Cryptography*, 87(1):163–171, January 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0494-1.

**Bassa:2019:SDC**

[2343] Alp Bassa and Henning Stichtenoth. Self-dual codes better than the Gilbert–varshamov bound. *Designs, Codes, and Cryptography*, 87(1):173–182, January 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0497-y.

**Cardinali:2019:PSI**

[2344] Ilaria Cardinali, Michel Lavrauw, Klaus Metsch, and Alexander Pott. Preface to the special issue on finite geometries. *Designs, Codes, and Cryptography*, 87(4):715–716, April 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-00600-x; https://link.springer.com/content/pdf/10.1007/s10623-018-00600-x.pdf.

**Meagher:2019:EKR**

[2345] Karen Meagher. An Erdős–Ko–Rado theorem for the group PSU$(3, q)$. *Designs, Codes, and Cryptography*, 87(4):717–744, April 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0537-7.

**Buratti:2019:DDF**

[2346] Marco Buratti. On disjoint $(v, k, k-1)$ difference families. *Designs, Codes, and Cryptography*, 87(4):745–755, April

2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0511-4.

**DeWinter:2019:NEP**

[2347] Stefaan De Winter and Zeying Wang. Non-existence of partial difference sets in Abelian groups of order $8p^3$. *Designs, Codes, and Cryptography*, 87 (4):757–768, April 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0508-z.

**Buratti:2019:FKT**

[2348] Marco Buratti and Francesca Merola. Fano kaleidoscopes and their generalizations. *Designs, Codes, and Cryptography*, 87(4):769–784, April 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0538-6.

**Landjev:2019:CES**

[2349] Ivan Landjev and Nevyana Georgieva. Conditions for the existence of spreads in projective Hjelmslev spaces. *Designs, Codes, and Cryptography*, 87 (4):785–794, April 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0540-z.

**Bartoli:2019:LCD**

[2350] Daniele Bartoli, Massimo Giulietti, and Maria Montanucci. Linear codes from Denniston maximal arcs. *Designs, Codes, and Cryptography*, 87 (4):795–806, April 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0515-0.

**DeWinter:2019:MAE**

[2351] Stefaan De Winter, Cunsheng Ding, and Vladimir D. Tonchev. Maximal arcs and extended cyclic codes. *Designs, Codes, and Cryptography*, 87 (4):807–816, April 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0514-1.

**Pinero:2019:WSC**

[2352] Fernando Piñero and Prasant Singh. The weight spectrum of certain affine Grassmann codes. *Designs, Codes, and Cryptography*, 87(4):817–830, April 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0567-1.

**Jungnickel:2019:CST**

[2353] Dieter Jungnickel, Spyros S. Magliveras, Vladimir D. Tonchev, and Alfred Wassermann. The classification of Steiner triple systems on 27 points with 3-rank 24. *Designs, Codes, and Cryptography*, 87(4):831–839, April 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0502-5.

**Rousseva:2019:LCC**

[2354] Assia Rousseva and Ivan Landjev. Linear codes close to the Griesmer bound

and the related geometric structures. *Designs, Codes, and Cryptography*, 87 (4):841–854, April 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0565-3`.

**Shparlinski:2019:CCR**

[2355] Igor E. Shparlinski and Arne Winterhof. Codes correcting restricted errors. *Designs, Codes, and Cryptography*, 87 (4):855–863, April 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0585-z`.

**Blokhuis:2019:RBS**

[2356] Aart Blokhuis, Leo Storme, and Tamás Szőnyi. Relative blocking sets of unions of Baer subplanes. *Designs, Codes, and Cryptography*, 87(4):865–877, April 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0575-1`.

**DeBeule:2019:CC**

[2357] Jan De Beule, Jeroen Demeyer, Sam Mattheus, and Péter Sziklai. On the cylinder conjecture. *Designs, Codes, and Cryptography*, 87(4):879–893, April 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0571-5`.

**Taniguchi:2019:VDH**

[2358] Hiroaki Taniguchi. A variation of the dual hyperoval $\mathcal{S}_c$ using presemifields. *Designs, Codes, and Cryptography*, 87 (4):895–908, April 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0539-5`.

**DeBruyn:2019:THE**

[2359] Bart De Bruyn. Three homogeneous embeddings of $\mathrm{DW}(2n-1,2)$. *Designs, Codes, and Cryptography*, 87 (4):909–929, April 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0531-0`.

**Betten:2019:CSS**

[2360] Anton Betten and Fatma Karaoglu. Cubic surfaces over small finite fields. *Designs, Codes, and Cryptography*, 87 (4):931–953, April 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0590-2`.

**Charpin:2019:OJW**

[2361] Pascale Charpin and Philippe Langevin. Obituary of Jacques Wolfmann (1932–2018). *Designs, Codes, and Cryptography*, 87(5):955–956, May 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00631-y; https://link.springer.com/content/pdf/10.1007/s10623-019-00631-y.pdf`.

**Hui:2019:VIN**

[2362] Alice M. W. Hui, Muhammad Adib Surani, and Sanming Zhou. The vertex-isoperimetric number of the incidence

and non-incidence graphs of unitals. *Designs, Codes, and Cryptography*, 87(5):957–970, May 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0498-x.

**Zhu:2019:VGR**

[2363] Yuqing Zhu, Jincheng Zhuang, Hairong Yi, Chang Lv, and Dongdai Lin. A variant of the Galbraith–Ruprai algorithm for discrete logarithms with improved complexity. *Designs, Codes, and Cryptography*, 87(5):971–986, May 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0492-3.

**Meszka:2019:OOF**

[2364] Mariusz Meszka and Magdalena Tyniec. Orthogonal one-factorizations of complete multipartite graphs. *Designs, Codes, and Cryptography*, 87(5):987–993, May 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0504-3; https://link.springer.com/content/pdf/10.1007/s10623-018-0504-3.pdf.

**Romanov:2019:NFR**

[2365] Alexander M. Romanov. On non-full-rank perfect codes over finite fields. *Designs, Codes, and Cryptography*, 87(5):995–1003, May 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0506-1.

**Shikata:2019:IBE**

[2366] Junji Shikata and Yohei Watanabe. Identity-based encryption with hierarchical key-insulation in the standard model. *Designs, Codes, and Cryptography*, 87(5):1005–1033, May 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0503-4.

**Li:2019:CM**

[2367] Yanbin Li and Meiqin Wang. Cryptanalysis of MORUS. *Designs, Codes, and Cryptography*, 87(5):1035–1058, May 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0501-6.

**Chisaki:2019:RCD**

[2368] Shoko Chisaki, Yui Kimura, and Nobuko Miyamoto. A recursive construction for difference systems of sets. *Designs, Codes, and Cryptography*, 87(5):1059–1068, May 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0505-2.

**Micheli:2019:CCC**

[2369] Giacomo Micheli and Violetta Weger. Cryptanalysis of the CLR-cryptosystem. *Designs, Codes, and Cryptography*, 87(5):1069–1086, May 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0500-7.

**Heng:2019:CAL**

[2370] Ziling Heng and Cunsheng Ding. A construction of $q$-ary linear codes with irreducible cyclic codes. *Designs, Codes, and Cryptography*, 87 (5):1087–1108, May 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0507-0`.

**Best:2019:CPT**

[2371] Darcy Best, Trent Marbach, Rebecca J. Stones, and Ian M. Wanless. Covers and partial transversals of Latin squares. *Designs, Codes, and Cryptography*, 87(5):1109–1136, May 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0499-9; https://link.springer.com/content/pdf/10.1007/s10623-018-0499-9.pdf`.

**Chang:2019:BBS**

[2372] Zuling Chang, Martianus Frederic Ezerman, San Ling, and Huaxiong Wang. On binary de Bruijn sequences from LFSRs with arbitrary characteristic polynomials. *Designs, Codes, and Cryptography*, 87(5):1137–1160, May 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0509-y`.

**Xie:2019:UBV**

[2373] Huiqin Xie and Li Yang. Using Bernstein–Vazirani algorithm to attack block ciphers. *Designs, Codes, and Cryptography*, 87(5):1161–1182, May 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0510-5; https://link.springer.com/content/pdf/10.1007/s10623-018-0510-5.pdf`.

**Edemskiy:2019:LCG**

[2374] Vladimir Edemskiy, Chunlei Li, Xiangyong Zeng, and Tor Helleseth. The linear complexity of generalized cyclotomic binary sequences of period $p^n$. *Designs, Codes, and Cryptography*, 87 (5):1183–1197, May 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0513-2`.

**vanZanten:2019:PIT**

[2375] A. J. van Zanten. Primitive idempotent tables of cyclic and constacyclic codes. *Designs, Codes, and Cryptography*, 87 (6):1199–1225, June 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0495-0; https://link.springer.com/content/pdf/10.1007/s10623-018-0495-0.pdf`.

**Koike:2019:CGC**

[2376] Hiroki Koike, István Kovács, Dragan Marušič, and Mikhail Muzychuk. Cyclic groups are CI-groups for balanced configurations. *Designs, Codes, and Cryptography*, 87 (6):1227–1235, June 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0517-y`.

**Miezaki:2019:CIW**

[2377] Tsuyoshi Miezaki and Manabu Oura. On the cycle index and the weight enumerator. *Designs, Codes, and Cryptography*, 87(6):1237–1242, June 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0518-x`.

**Michel:2019:ADS**

[2378] Jerod Michel and Qi Wang. Almost difference sets in nonabelian groups. *Designs, Codes, and Cryptography*, 87 (6):1243–1251, June 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0519-9`.

**Dyshko:2019:ETL**

[2379] Serhii Dyshko. The extension theorem for Lee and Euclidean weight codes over integer residue rings. *Designs, Codes, and Cryptography*, 87 (6):1253–1269, June 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0521-2`.

**Bi:2019:MAC**

[2380] Wenquan Bi, Xiaoyang Dong, Zheng Li, Rui Zong, and Xiaoyun Wang. MILP-aided cube-attack-like cryptanalysis on Keccak Keyed modes. *Designs, Codes, and Cryptography*, 87 (6):1271–1296, June 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0526-x`.

**Guo:2019:BBS**

[2381] Chun Guo, Yaobin Shen, Lei Wang, and Dawu Gu. Beyond-birthday secure domain-preserving PRFs from a single permutation. *Designs, Codes, and Cryptography*, 87(6):1297–1322, June 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0528-8`.

**Farras:2019:LBO**

[2382] Oriol Farràs, Jordi Ribes-González, and Sara Ricci. Local bounds for the optimal information ratio of secret sharing schemes. *Designs, Codes, and Cryptography*, 87(6):1323–1344, June 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0529-7`.

**Huang:2019:SBS**

[2383] Zhengan Huang, Junzuo Lai, Wenbin Chen, Man Ho Au, Zhen Peng, and Jin Li. Simulation-based selective opening security for receivers under chosen-ciphertext attacks. *Designs, Codes, and Cryptography*, 87 (6):1345–1371, June 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-018-0530-1`.

**Derler:2019:KHS**

[2384] David Derler and Daniel Slamanig. Key-homomorphic signatures: definitions and applications to multiparty signatures and non-interactive zero-knowledge. *Designs, Codes, and*

*Cryptography*, 87(6):1373–1413, June 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0535-9.

**Chang:2019:EFD**

[2385] Yanxun Chang, Hao Zheng, and Junling Zhou. Existence of frame-derived $H$-designs. *Designs, Codes, and Cryptography*, 87(6):1415–1431, June 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0536-8.

**Bartoli:2019:MWC**

[2386] Daniele Bartoli and Matteo Bonini. Minimum weight codewords in dual algebraic-geometric codes from the Giulietti–Korchmáros curve. *Designs, Codes, and Cryptography*, 87(6):1433–1445, June 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0541-y.

**Shi:2019:TCB**

[2387] Minjia Shi, Yan Liu, Hugues Randriam, Lin Sok, and Patrick Solé. Trace codes over $\mathbf{Z}_4$, and Boolean functions. *Designs, Codes, and Cryptography*, 87(6):1447–1455, June 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0542-x.

**Ihringer:2019:CMM**

[2388] Ferdinand Ihringer and Karen Meagher. Correction to: Miklós–Manickam–Singhi conjectures on partial geometries. *Designs, Codes, and Cryptography*, 87(6):1457, June 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00611-2; https://link.springer.com/content/pdf/10.1007/s10623-019-00611-2.pdf. See [2249].

**Kapetanakis:2019:VPN**

[2389] Giorgos Kapetanakis and Lucas Reis. Variations of the Primitive Normal Basis Theorem. *Designs, Codes, and Cryptography*, 87(7):1459–1480, July 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0543-9.

**Fu:2019:RCP**

[2390] Shihui Fu, Xiutao Feng, Dongdai Lin, and Qiang Wang. A recursive construction of permutation polynomials over $\mathbf{F}_{q^2}$ with odd characteristic related to Rédei functions. *Designs, Codes, and Cryptography*, 87(7):1481–1498, July 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0548-4.

**Feng:2019:ODO**

[2391] Tao Feng, Lidong Wang, and Xiaomiao Wang. Optimal 2-D $(n \times m, 3, 2, 1)$-optical orthogonal codes and related equi-difference conflict avoiding codes. *Designs, Codes, and Cryptography*, 87(7):1499–1520, July 2019. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0549-3.

**vanTrung:2019:ETS**

[2392] Tran van Trung. On existence theorems for simple $t$-designs. *Designs, Codes, and Cryptography*, 87 (7):1521–1540, July 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0550-x.

**Lavauzelle:2019:LPR**

[2393] Julien Lavauzelle. Lifted projective Reed–Solomon codes. *Designs, Codes, and Cryptography*, 87(7):1541–1575, July 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0552-8.

**Carlet:2019:CIF**

[2394] Claude Carlet, Xi Chen, and Longjiang Qu. Constructing infinite families of low differential uniformity $(n, m)$-functions with $m > n/2$. *Designs, Codes, and Cryptography*, 87 (7):1577–1599, July 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0553-7.

**Meng:2019:SEL**

[2395] Keju Meng, Fuyou Miao, and Yue Yu. A secure and efficient on-line/off-line group key distribution protocol. *Designs, Codes, and Cryptography*, 87 (7):1601–1620, July 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0554-6.

**Cogliati:2019:MUS**

[2396] Benoît Cogliati and Titouan Tanguy. Multi-user security bound for filter permutators in the random oracle model. *Designs, Codes, and Cryptography*, 87 (7):1621–1638, July 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0555-5.

**Polhill:2019:NFP**

[2397] John Polhill. A new family of partial difference sets in 3-groups. *Designs, Codes, and Cryptography*, 87 (7):1639–1646, July 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0562-6.

**Jia:2019:ECB**

[2398] Dongdong Jia, Sumei Zhang, and Gengsheng Zhang. Erasure combinatorial batch codes based on nonadaptive group testing. *Designs, Codes, and Cryptography*, 87(7):1647–1656, July 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0564-4.

**Reis:2019:FCC**

[2399] Lucas Reis. Factorization of a class of composed polynomials. *Designs, Codes, and Cryptography*, 87 (7):1657–1671, July 2019. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0568-0.

**Fickus:2019:ETF**

[2400] Matthew Fickus and John Jasper. Equiangular tight frames from group divisible designs. *Designs, Codes, and Cryptography*, 87(7):1673–1697, July 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0569-z.

**Dutta:2019:MCC**

[2401] Sabyasachi Dutta, Avishek Adhikari, and Sushmita Ruj. Maximal contrast color visual secret sharing schemes. *Designs, Codes, and Cryptography*, 87(7):1699–1711, July 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0570-6.

**Liu:2019:ISB**

[2402] Xing Liu and Liang Zhou. Improved singleton bound on frequency hopping sequences and optimal constructions. *Designs, Codes, and Cryptography*, 87(8):1713–1733, August 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0572-4. See correction [2403].

**Liu:2019:CIS**

[2403] Xing Liu and Liang Zhou. Correction to: Improved Singleton bound on frequency hopping sequences and optimal constructions. *Designs, Codes, and Cryptography*, 87(8):1735–1736, August 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00618-9; https://link.springer.com/content/pdf/10.1007/s10623-019-00618-9.pdf. See [2402].

**Ducas:2019:PTB**

[2404] Léo Ducas and Cécile Pierrot. Polynomial time bounded distance decoding near Minkowski's bound in discrete logarithm lattices. *Designs, Codes, and Cryptography*, 87(8):1737–1748, August 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0573-3.

**Wang:2019:TSS**

[2405] Qichun Wang and Pantelimon Stănică. A trigonometric sum sharp estimate and new bounds on the nonlinearity of some cryptographic Boolean functions. *Designs, Codes, and Cryptography*, 87(8):1749–1763, August 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0574-2.

**Shiromoto:2019:CRM**

[2406] Keisuke Shiromoto. Codes with the rank metric and matroids. *Designs, Codes, and Cryptography*, 87(8):1765–1776, August 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0576-0.

**Cheraghchi:2019:NOR**

[2407] Mahdi Cheraghchi. Nearly optimal robust secret sharing. *Designs, Codes, and Cryptography*, 87(8):1777–1796, August 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0578-y; https://link.springer.com/content/pdf/10.1007/s10623-018-0578-y.pdf.

**Liu:2019:WPB**

[2408] Jian Liu and Sihem Mesnager. Weightwise perfectly balanced functions with high weightwise nonlinearity profile. *Designs, Codes, and Cryptography*, 87(8):1797–1813, August 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0579-x.

**Hou:2019:OBC**

[2409] Xiang-Dong Hou. Optimal binary constant weight codes and affine linear groups over finite fields. *Designs, Codes, and Cryptography*, 87(8):1815–1838, August 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0581-3.

**Blokhuis:2019:CLS**

[2410] A. Blokhuis, M. De Boeck, and J. D'haeseleer. Cameron–Liebler sets of $k$-spaces in PG$(n, q)$. *Designs, Codes, and Cryptography*, 87(8):1839–1856, August 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0583-1. See correction [2761].

**Shi:2019:APC**

[2411] Minjia Shi, Daitao Huang, and Denis S. Krotov. Additive perfect codes in Doob graphs. *Designs, Codes, and Cryptography*, 87(8):1857–1869, August 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0586-y.

**Olson:2019:TPI**

[2412] Torger Olson and Eric Swartz. Transitive PSL(2,11)-invariant $k$-arcs in PG(4,q). *Designs, Codes, and Cryptography*, 87(8):1871–1879, August 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0588-9.

**Brouwer:2019:UCU**

[2413] Andries E. Brouwer and Sven C. Polak. Uniqueness of codes using semidefinite programming. *Designs, Codes, and Cryptography*, 87(8):1881–1895, August 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0589-8; https://link.springer.com/content/pdf/10.1007/s10623-018-0589-8.pdf.

**Dinur:2019:AFG**

[2414] Itai Dinur. An algorithmic framework for the generalized birthday problem. *Designs, Codes, and Cryptography*, 87(8):1897–1926, August 2019. CODEN

DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-00594-6.

**Wu:2019:MTW**

[2415] Yansheng Wu, Qin Yue, and Xueying Shi. At most three-weight binary linear codes from generalized Moisio's exponential sums. *Designs, Codes, and Cryptography*, 87(8):1927–1943, August 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-00595-5.

**Michel:2019:ADT**

[2416] Jerod Michel and Qi Wang. Almost designs and their links with balanced incomplete block designs. *Designs, Codes, and Cryptography*, 87(9):1945–1960, September 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-00596-4.

**Lai:2019:QEG**

[2417] Ching-Yi Lai and Kai-Min Chung. Quantum encryption and generalized Shannon impossibility. *Designs, Codes, and Cryptography*, 87(9):1961–1972, September 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-00597-3.

**Taniguchi:2019:SQA**

[2418] Hiroaki Taniguchi. On some quadratic APN functions. *Designs, Codes, and Cryptography*, 87(9):1973–1983, September 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-00598-2.

**Cossidente:2019:LCF**

[2419] Antonio Cossidente and Francesco Pavese. On line covers of finite projective and polar spaces. *Designs, Codes, and Cryptography*, 87(9):1985–2002, September 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-00599-1.

**Liang:2019:FPA**

[2420] Miao Liang and Lijun Ji. On $(t, L)$-fold perfect authentication and secrecy codes with arbitration. *Designs, Codes, and Cryptography*, 87(9):2003–2026, September 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-00602-9.

**Carvalho:2019:PRM**

[2421] Cícero Carvalho, Xavier Ramírez-Mondragón, Victor G. L. Neumann, and Horacio Tapia-Recillas. Projective Reed–Muller type codes on higher dimensional scrolls. *Designs, Codes, and Cryptography*, 87(9):2027–2042, September 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-00603-8.

**Wang:2019:TOB**

[2422] Qichun Wang and Pantelimon Stănică. Transparency order for Boolean func-

tions: analysis and construction. *Designs, Codes, and Cryptography*, 87(9): 2043–2059, September 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00604-1.

**Zhou:2019:CLR**

[2423] Yanwei Zhou, Bo Yang, and Yi Mu. Continuous leakage-resilient identity-based encryption with leakage amplification. *Designs, Codes, and Cryptography*, 87(9):2061–2090, September 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00605-0.

**Shi:2019:NDR**

[2424] Minjia Shi, Denis S. Krotov, and Patrick Solé. A new distance-regular graph of diameter 3 on 1024 vertices. *Designs, Codes, and Cryptography*, 87(9):2091–2101, September 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00609-w; https://link.springer.com/content/pdf/10.1007/s10623-019-00609-w.pdf. See correction [2425].

**Shi:2019:CND**

[2425] Minjia Shi, Denis S. Krotov, and Patrick Solé. Correction to: A new distance-regular graph of diameter 3 on 1024 vertices. *Designs, Codes, and Cryptography*, 87 (9):2103, September 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00672-3; https://link.springer.com/content/pdf/10.1007/s10623-019-00672-3.pdf. See [2424].

**Bereg:2019:NLB**

[2426] Sergey Bereg, Zevi Miller, Luis Gerardo Mojica, Linda Morales, and I. H. Sudborough. New lower bounds for permutation arrays using contraction. *Designs, Codes, and Cryptography*, 87(9): 2105–2128, September 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00607-y.

**Vandendriessche:2019:KAN**

[2427] Peter Vandendriessche. On KM-arcs in non-Desarguesian projective planes. *Designs, Codes, and Cryptography*, 87(9):2129–2137, September 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00606-z.

**Maxwell:2019:SSM**

[2428] Gregory Maxwell, Andrew Poelstra, Yannick Seurin, and Pieter Wuille. Simple Schnorr multi-signatures with applications to Bitcoin. *Designs, Codes, and Cryptography*, 87(9):2139–2164, September 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00608-x.

**Shi:2019:DCP**

[2429] Xueying Shi, Qin Yue, and Yansheng Wu. The dual-containing primitive BCH codes with the maximum designed distance and their applications to quantum codes. *Designs, Codes, and Cryptography*, 87(9):2165–2183, September 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00610-3`.

**Wang:2019:LAE**

[2430] Xin Wang, Jie Cui, and Lijun Ji. Linear $(2, p, p)$-AONTs exist for all primes $p$. *Designs, Codes, and Cryptography*, 87(10):2185–2197, October 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00612-1`.

**Aydin:2019:ECC**

[2431] Nuh Aydin, Jonathan Lambrinos, and Oliver VandenBerg. On equivalence of cyclic codes, generalization of a quasi-twisted search algorithm, and new linear codes. *Designs, Codes, and Cryptography*, 87(10):2199–2212, October 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00613-0`.

**Bai:2019:TGW**

[2432] Liang Bai and Zihui Liu. On the third greedy weight of 4-dimensional codes. *Designs, Codes, and Cryptography*, 87(10):2213–2230, October 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00614-z`.

**Kotov:2019:AWD**

[2433] Matvei Kotov, Anton Menshov, and Alexander Ushakov. An attack on the Walnut digital signature algorithm. *Designs, Codes, and Cryptography*, 87(10):2231–2250, October 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00615-y`.

**Liu:2019:NCZ**

[2434] Junying Liu, Yupeng Jiang, Qunxiong Zheng, and Dongdai Lin. A new construction of zero-difference balanced functions and two applications. *Designs, Codes, and Cryptography*, 87(10):2251–2265, October 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00616-x`.

**Tian:2019:UTC**

[2435] Tian Tian, Jia-Min Zhang, and Wen-Feng Qi. On the uniqueness of a type of cascade connection representations for NFSRs. *Designs, Codes, and Cryptography*, 87(10):2267–2294, October 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00617-w`.

**Martinez-Penas:2019:TSL**

[2436] Umberto Martínez-Peñas. Theory of supports for linear codes endowed with the sum-rank metric. *Designs, Codes, and Cryptography*, 87(10):2295–2320, October 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00619-8.

**Wang:2019:HML**

[2437] Qichun Wang. Hadamard matrices, $d$-linearly independent sets and correlation-immune Boolean functions with minimum Hamming weights. *Designs, Codes, and Cryptography*, 87(10):2321–2333, October 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00620-1.

**Sobhani:2019:NGP**

[2438] R. Sobhani, A. Abdollahi, J. Bagherian, and M. Khatami. A note on good permutation codes from Reed–Solomon codes. *Designs, Codes, and Cryptography*, 87(10):2335–2340, October 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00621-0.

**Kharaghani:2019:LSS**

[2439] Hadi Kharaghani and Sho Suda. Linked systems of symmetric group divisible designs of type II. *Designs, Codes, and Cryptography*, 87(10):2341–2360, October 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00622-z.

**Kim:2019:SSP**

[2440] Jon-Lark Kim, Junyong Park, and Soohak Choi. Steganographic schemes from perfect codes on Cayley graphs. *Designs, Codes, and Cryptography*, 87(10):2361–2374, October 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00624-x.

**Bagchi:2019:CTA**

[2441] Bhaskar Bagchi. A coding theoretic approach to the uniqueness conjecture for projective planes of prime order. *Designs, Codes, and Cryptography*, 87(10):2375–2389, October 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00623-y.

**Qi:2019:CLC**

[2442] Minglong Qi and Shengwu Xiong. A correction to: On the linear complexity of the Sidelnikov–Lempel–Cohn–Eastman sequences. *Designs, Codes, and Cryptography*, 87(10):2391–2393, October 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00625-w. See [639].

**Shi:2019:TWC**

[2443] Minjia Shi and Patrick Solé. Three-weight codes, triple sum sets, and

strongly walk regular graphs. *Designs, Codes, and Cryptography*, 87(10):2395–2404, October 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00628-7`.

**Armario:2019:GBA**

[2444] J. A. Armario and D. L. Flannery. Generalized binary arrays from quasi-orthogonal cocycles. *Designs, Codes, and Cryptography*, 87(10):2405–2417, October 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00626-9`.

**Cao:2019:CES**

[2445] Yuan Cao, Yonglin Cao, Steven T. Dougherty, and San Ling. Construction and enumeration for self-dual cyclic codes over $\mathbf{Z}_4$ of oddly even length. *Designs, Codes, and Cryptography*, 87(10):2419–2446, October 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00629-6`.

**Li:2019:WDS**

[2446] Shuxing Li. On the weight distribution of second order Reed–Muller codes and their relatives. *Designs, Codes, and Cryptography*, 87(10):2447–2460, October 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00630-z`.

**Buratti:2019:PDF**

[2447] Marco Buratti and Dieter Jungnickel. Partitioned difference families versus zero-difference balanced functions. *Designs, Codes, and Cryptography*, 87(11):2461–2467, November 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00632-x`.

**Gomez:2019:PAL**

[2448] Ana I. Gomez, Domingo Gomez-Perez, and Guénaël Renault. A probabilistic analysis on a lattice attack against DSA. *Designs, Codes, and Cryptography*, 87(11):2469–2488, November 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00633-w`.

**Yasuda:2019:NPT**

[2449] Masaya Yasuda and Junpei Yamaguchi. A new polynomial-time variant of LLL with deep insertions for decreasing the squared-sum of Gram–Schmidt lengths. *Designs, Codes, and Cryptography*, 87(11):2489–2505, November 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00634-9`.

**Duursma:2019:MTM**

[2450] Iwan M. Duursma. Matrix theory for minimal trellises. *Designs, Codes, and Cryptography*, 87(11):2507–2536, November 2019. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00627-8.

**Song:2019:HCP**

[2451] Min Kyu Song and Hong-Yeop Song. Hamming correlation properties of the array structure of Sidelnikov sequences. *Designs, Codes, and Cryptography*, 87(11):2537–2551, November 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00636-7.

**Hu:2019:NGS**

[2452] Yupu Hu and Huiwen Jia. A new Gaussian sampling for trapdoor lattices with arbitrary modulus. *Designs, Codes, and Cryptography*, 87(11):2553–2570, November 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00635-8.

**Sheekey:2019:BAM**

[2453] John Sheekey. Binary additive MRD codes with minimum distance $n - 1$ must contain a semifield spread set. *Designs, Codes, and Cryptography*, 87(11):2571–2583, November 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00637-6.

**Ouyang:2019:LCG**

[2454] Yi Ouyang and Xianhong Xie. Linear complexity of generalized cyclotomic sequences of period $2p^m$. *Designs, Codes, and Cryptography*, 87(11):2585–2596, November 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00638-5.

**Mesnager:2019:FSM**

[2455] Sihem Mesnager, Fengrong Zhang, Chunming Tang, and Yong Zhou. Further study on the maximum number of bent components of vectorial functions. *Designs, Codes, and Cryptography*, 87(11):2597–2610, November 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00639-4.

**Zhang:2019:GPI**

[2456] Yiwei Zhang and Gennian Ge. A general private information retrieval scheme for MDS coded databases with colluding servers. *Designs, Codes, and Cryptography*, 87(11):2611–2623, November 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00640-x.

**Xu:2019:NTB**

[2457] Zixiang Xu, Yiwei Zhang, and Gennian Ge. New theoretical bounds and constructions of permutation codes under block permutation metric. *Designs, Codes, and Cryptography*, 87(11):2625–2637, November 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00641-w.

**Garefalakis:2019:FRM**

[2458] Theodoulos Garefalakis and Giorgos Kapetanakis. Further results on the Morgan–Mullen conjecture. *Designs, Codes, and Cryptography*, 87(11):2639–2654, November 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00643-8`.

**Michel:2019:PGD**

[2459] Jerod Michel and Qi Wang. Partial geometric designs from group actions. *Designs, Codes, and Cryptography*, 87(11):2655–2670, November 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00644-7`.

**Byrnes:2019:MLC**

[2460] Kevin M. Byrnes. The maximum length of circuit codes with long bit runs and a new characterization theorem. *Designs, Codes, and Cryptography*, 87(11):2671–2681, November 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00646-5`.

**Yang:2019:PSA**

[2461] Dong Yang, Wen-Feng Qi, and Hua-Jin Chen. Provable security against impossible differential and zero correlation linear cryptanalysis of some Feistel structures. *Designs, Codes, and Cryptography*, 87(11):2683–2700, November 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00642-9`.

**Ng:2019:FRC**

[2462] Siaw-Lynn Ng and Maura B. Paterson. Functional repair codes: a view from projective geometry. *Designs, Codes, and Cryptography*, 87(11):2701–2722, November 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00647-4`.

**Zhan:2019:FTD**

[2463] Xiaoqin Zhan, Suyun Ding, and Shuyi Bai. Flag-transitive 2-designs from $\mathrm{PSL}(2, 40q)$ with block size 4. *Designs, Codes, and Cryptography*, 87(11):2723–2728, November 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00648-3`.

**Dukes:2019:CUI**

[2464] Peter J. Dukes and Esther R. Lamken. Constructions and uses of incomplete pairwise balanced designs. *Designs, Codes, and Cryptography*, 87(12):2729–2751, December 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00645-6`.

**Shangguan:2019:NPD**

[2465] Chong Shangguan and Gennian Ge. A new piggybacking design for systematic MDS storage codes. *Designs, Codes, and Cryptography*, 87(12):2753–2770, December 2019. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00650-9.

**Davydov:2019:NCC**

[2466] Alexander A. Davydov, Stefano Marcugini, and Fernanda Pambianco. New covering codes of radius $R$, codimension tR and $tR + \frac{R}{2}$, and saturating sets in projective spaces. *Designs, Codes, and Cryptography*, 87(12):2771–2792, December 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00649-2.

**Tang:2019:SSD**

[2467] Chunming Tang, Cunsheng Ding, and Maosheng Xiong. Steiner systems $S(2, 4, \frac{3^m-1}{2})$ and 2-designs from ternary linear codes of length $\frac{3^m-1}{2}$. *Designs, Codes, and Cryptography*, 87(12):2793–2811, December 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00651-8.

**Carlet:2019:SAO**

[2468] Claude Carlet, Chengju Li, and Sihem Mesnager. Some (almost) optimally extendable linear codes. *Designs, Codes, and Cryptography*, 87(12):2813–2834, December 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00652-7.

**vanTrung:2019:RCR**

[2469] Tran van Trung. Recursive constructions for $s$-resolvable $t$-designs. *Designs, Codes, and Cryptography*, 87(12):2835–2845, December 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00653-6.

**Steinfeld:2019:PBE**

[2470] Ron Steinfeld, Amin Sakzad, and Raymond K. Zhao. Practical MP–LWE-based encryption balancing security-risk versus efficiency. *Designs, Codes, and Cryptography*, 87(12):2847–2884, December 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00654-5.

**Yang:2019:SLR**

[2471] Guomin Yang, Rongmao Chen, Yi Mu, Willy Susilo, Fuchun Guo, and Jie Li. Strongly leakage resilient authenticated key exchange, revisited. *Designs, Codes, and Cryptography*, 87(12):2885–2911, December 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00656-3.

**Chen:2019:EEC**

[2472] Qi Chen, Chunming Tang, and Zhiqiang Lin. Efficient explicit constructions of compartmented secret sharing schemes. *Designs, Codes, and Cryptography*, 87(12):2913–2940, December 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00657-2.

**Ling:2019:MQT**

[2473] San Ling and Buket Özkaya. Multidimensional quasi-twisted codes: equivalent characterizations and their relation to multidimensional convolutional codes. *Designs, Codes, and Cryptography*, 87(12):2941–2965, December 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00655-4`.

**Mezofi:2019:GFP**

[2474] Dávid Mezőfi and Gábor P. Nagy. On the geometry of full points of abstract unitals. *Designs, Codes, and Cryptography*, 87(12):2967–2978, December 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00658-1`.

**Lau:2019:NRC**

[2475] Terry Shue Chien Lau and Chik How Tan. New rank codes based encryption scheme using partial circulant matrices. *Designs, Codes, and Cryptography*, 87(12):2979–2999, December 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00659-0`.

**Wang:2019:MAR**

[2476] Qian Wang and Chenhui Jin. More accurate results on the provable security of AES against impossible differential cryptanalysis. *Designs, Codes, and Cryptography*, 87(12):3001–3018, December 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00660-7`.

**Lieb:2019:NFS**

[2477] Julia Lieb. Necessary field size and probability for MDP and complete MDP convolutional codes. *Designs, Codes, and Cryptography*, 87(12):3019–3043, December 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00661-6`.

**Sun:2019:CRB**

[2478] Yujuan Sun, Jiafang Zhang, and Sugata Gangopadhyay. Construction of resilient Boolean functions in odd variables with strictly almost optimal nonlinearity. *Designs, Codes, and Cryptography*, 87(12):3045–3062, December 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00662-5`.

**Carlet:2019:LCS**

[2479] Claude Carlet, Chengju Li, and Sihem Mesnager. Linear codes with small hulls in semi-primitive case. *Designs, Codes, and Cryptography*, 87(12):3063–3075, December 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00663-4`.

**Liu:2019:LCD**

[2480] Zihui Liu and Jinliang Wang. Linear complementary dual codes over

rings. *Designs, Codes, and Cryptography*, 87(12):3077–3086, December 2019. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00664-3.

**Gomez-Torrecillas:2020:SRN**

[2481] José Gómez-Torrecillas, Erik Hieta-Aho, F. J. Lobillo, Sergio López-Permouth, and Gabriel Navarro. Some remarks on non projective Frobenius algebras and linear codes. *Designs, Codes, and Cryptography*, 88 (1):1–15, January 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00666-1.

**Ball:2020:AT**

[2482] Simeon Ball and Michel Lavrauw. Arcs and tensors. *Designs, Codes, and Cryptography*, 88(1):17–31, January 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00668-z.

**Barwick:2020:CHH**

[2483] S. G. Barwick, Alice M. W. Hui, Wen-Ai Jackson, and Jeroen Schillewaert. Characterising hyperbolic hyperplanes of a non-singular quadric in PG(4, q). *Designs, Codes, and Cryptography*, 88 (1):33–39, January 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00669-y.

**Singh:2020:CGQ**

[2484] Jasvinder Singh, Manish Gupta, and Jaskarn Singh Bhullar. Construction of girth-8 $(3, L)$-QC-LDPC codes of smallest CPM size using column multipliers. *Designs, Codes, and Cryptography*, 88(1):41–49, January 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00667-0.

**Mesnager:2020:PBK**

[2485] Sihem Mesnager, Kwang Ho Kim, Dujin Jo, Junyop Choe, Munhyon Han, and Dok Nam Lee. A proof of the Beierle–Kranz–Leander conjecture related to lightweight multiplication in $\mathbf{F}_{2^n}$. *Designs, Codes, and Cryptography*, 88(1):51–62, January 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00665-2.

**Bereg:2020:LBP**

[2486] Sergey Bereg and Peter J. Dukes. A lower bound on permutation codes of distance $n - 1$. *Designs, Codes, and Cryptography*, 88(1):63–72, January 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00670-5.

**Duc:2020:NCE**

[2487] Tai Do Duc. Necessary conditions for the existence of group-invariant Butson Hadamard matrices and a

new family of perfect arrays. *Designs, Codes, and Cryptography*, 88 (1):73–90, January 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00671-4`.

**Kolbl:2020:TTC**

[2488] Stefan Kölbl, Elmar Tischhauser, Patrick Derbez, and Andrey Bogdanov. Troika: a ternary cryptographic hash function. *Designs, Codes, and Cryptography*, 88(1):91–117, January 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00673-2`.

**Pan:2020:OOO**

[2489] Rong Pan, Tao Feng, Lidong Wang, and Xiaomiao Wang. Optimal optical orthogonal signature pattern codes with weight three and cross-correlation constraint one. *Designs, Codes, and Cryptography*, 88(1):119–131, January 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00675-0`.

**Guenda:2020:LIP**

[2490] Kenza Guenda, T. Aaron Gulliver, Somphong Jitman, and Satanan Thipworawimon. Linear $\ell$-intersection pairs of codes and their applications. *Designs, Codes, and Cryptography*, 88 (1):133–152, January 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00676-z`.

**Zhao:2020:FRE**

[2491] Xiao-Xin Zhao, Wen-Feng Qi, and Jia-Min Zhang. Further results on the equivalence between Galois NFSRs and Fibonacci NFSRs. *Designs, Codes, and Cryptography*, 88 (1):153–171, January 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00677-y`.

**Kesarwani:2020:NCD**

[2492] Abhishek Kesarwani, Dibyendu Roy, Santanu Sarkar, and Willi Meier. New cube distinguishers on NFSR-based stream ciphers. *Designs, Codes, and Cryptography*, 88(1):173–199, January 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00674-1`.

**Kutsenko:2020:MPS**

[2493] Aleksandr Kutsenko. Metrical properties of self-dual bent functions. *Designs, Codes, and Cryptography*, 88 (1):201–222, January 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00678-x`.

**Gupta:2020:SNP**

[2494] Rohit Gupta. Several new permutation quadrinomials over finite fields of odd characteristic. *Designs, Codes, and Cryptography*, 88 (1):223–239, January 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https:`

//link.springer.com/article/10.1007/s10623-019-00680-3.

**Liu:2020:GHL**

[2495] Hongwei Liu and Xu Pan. Galois hulls of linear codes over finite fields. *Designs, Codes, and Cryptography*, 88 (2):241–255, February 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00681-2.

**Li:2020:FCM**

[2496] Xia Li and Qin Yue. Four classes of minimal binary linear codes with $w_{\min}/w_{\max} < 1/2$ derived from Boolean functions. *Designs, Codes, and Cryptography*, 88(2):257–271, February 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00682-1.

**Martinez-Bernal:2020:LCS**

[2497] José Martínez-Bernal, Miguel A. Valencia-Bucio, and Rafael H. Villarreal. Linear codes over signed graphs. *Designs, Codes, and Cryptography*, 88 (2):273–296, February 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00683-0.

**Liu:2020:SCA**

[2498] Yan Liu, Xiwang Cao, and Wei Lu. On some conjectures about optimal ternary cyclic codes. *Designs, Codes, and Cryptography*, 88 (2):297–309, February 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00679-w.

**Bereg:2020:CPA**

[2499] Sergey Bereg, Luis Gerardo Mojica, Linda Morales, and Hal Sudborough. Constructing permutation arrays using partition and extension. *Designs, Codes, and Cryptography*, 88 (2):311–339, February 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00684-z.

**Xu:2020:CEC**

[2500] Jun Xu, Lei Hu, and Santanu Sarkar. Cryptanalysis of elliptic curve hidden number problem from PKC 2017. *Designs, Codes, and Cryptography*, 88 (2):341–361, February 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00685-y.

**vandeKamp:2020:MAA**

[2501] Tim van de Kamp, Andreas Peter, and Willem Jonker. A multi-authority approach to various predicate encryption types. *Designs, Codes, and Cryptography*, 88(2):363–390, February 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00686-x; https://link.springer.com/content/pdf/10.1007/s10623-019-00686-x.pdf.

**Mariot:2020:MOL**

[2502] Luca Mariot, Maximilien Gadouleau, Enrico Formenti, and Alberto Lepo-

rati. Mutually orthogonal latin squares based on cellular automata. *Designs, Codes, and Cryptography*, 88 (2):391–411, February 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00689-8.

**Ling:2020:CNS**

[2503] Xin Ling, Sihem Mesnager, Yanfeng Qi, and Chunming Tang. A class of narrow-sense BCH codes over $\mathbf{F}_q$ of length $\frac{q^m-1}{2}$. *Designs, Codes, and Cryptography*, 88(2):413–427, February 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00691-0.

**DeBruyn:2020:FCA**

[2504] Bart De Bruyn and Mou Gao. On four codes with automorphism group $P\Sigma L(3,4)$ and pseudo-embeddings of the large Witt designs. *Designs, Codes, and Cryptography*, 88(2):429–452, February 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00690-1.

**Hyun:2020:RGE**

[2505] Jong Yoon Hyun, Jungyun Lee, and Yoonjin Lee. Ramanujan graphs and expander families constructed from $p$-ary bent functions. *Designs, Codes, and Cryptography*, 88(2):453–470, February 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00692-z.

**Salagean:2020:DAF**

[2506] Ana Salagean. Discrete antiderivatives for functions over $\mathbf{F}_p^n$. *Designs, Codes, and Cryptography*, 88 (3):471–486, March 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00687-w; https://link.springer.com/content/pdf/10.1007/s10623-019-00687-w.pdf.

**Wang:2020:SBC**

[2507] Xiang Wang and Fang-Wei Fu. Snake-in-the-box codes under the $\ell_\infty$-metric for rank modulation. *Designs, Codes, and Cryptography*, 88 (3):487–503, March 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00693-y.

**Das:2020:MLS**

[2508] Dipayan Das, Jeffrey Hoffstein, Jill Pipher, William Whyte, and Zhenfei Zhang. Modular lattice signatures, revisited. *Designs, Codes, and Cryptography*, 88(3):505–532, March 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00694-x.

**Li:2020:NAM**

[2509] Yubo Li, Zhichao Yang, Kangquan Li, and Longjiang Qu. A new algorithm on the minimal rational fraction representation of feedback with carry shift registers. *Designs, Codes, and Cryptography*, 88(3):533–552, March 2020. CODEN DC-

CREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00695-w.

**Xiang:2020:CDQ**

[2510] Can Xiang, Xin Ling, and Qi Wang. Combinatorial $t$-designs from quadratic functions. *Designs, Codes, and Cryptography*, 88(3):553–565, March 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00696-9.

**Alaca:2020:SID**

[2511] Saban Alaca and Goldwyn Millar. Shift-inequivalent decimations of the Sidelnikov–Lempel–Cohn–Eastman sequences. *Designs, Codes, and Cryptography*, 88(3):567–583, March 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00697-8.

**Yuster:2020:PSC**

[2512] Raphael Yuster. Perfect sequence covering arrays. *Designs, Codes, and Cryptography*, 88(3):585–593, March 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00698-7.

**Kurz:2020:SIM**

[2513] Sascha Kurz. Subspaces intersecting in at most a point. *Designs, Codes, and Cryptography*, 88(3):595–599, March 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00699-6.

**Hodzic:2020:GCB**

[2514] S. Hodžić, E. Pasalic, and S. Gangopadhyay. Generic constructions of $\mathbf{Z}$-bent functions. *Designs, Codes, and Cryptography*, 88(3):601–623, March 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00700-2.

**Ding:2020:LCD**

[2515] Cunsheng Ding, Chunming Tang, and Vladimir D. Tonchev. Linear codes of 2-designs associated with subcodes of the ternary generalized Reed–Muller codes. *Designs, Codes, and Cryptography*, 88(4):625–641, April 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00701-1.

**Aragon:2020:CRB**

[2516] Nicolas Aragon, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Terry Shue Chien Lau, Chik How Tan, and Keita Xagawa. Cryptanalysis of a rank-based signature with short public keys. *Designs, Codes, and Cryptography*, 88(4):643–653, April 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00702-0.

**Sheekey:2020:RMC**

[2517] John Sheekey and Geertrui Van de Voorde. Rank-metric codes, linear sets, and their duality. *Designs, Codes, and Cryptography*, 88 (4):655–675, April 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00703-z`.

**Zhang:2020:PDP**

[2518] Liang Feng Zhang and Reihaneh Safavi-Naini. Protecting data privacy in publicly verifiable delegation of matrix and polynomial functions. *Designs, Codes, and Cryptography*, 88 (4):677–709, April 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00704-y`.

**Neri:2020:RCP**

[2519] Alessandro Neri and Anna-Lena Horlemann-Trautmann. Random construction of partial MDS codes. *Designs, Codes, and Cryptography*, 88 (4):711–725, April 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00705-x`.

**Liu:2020:LCF**

[2520] Xiusheng Liu and Hualu Liu. $\sigma$-LCD codes over finite chain rings. *Designs, Codes, and Cryptography*, 88 (4):727–746, April 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00706-w`.

**Kroll:2020:LCR**

[2521] Hans-Joachim Kroll and Rita Vincenti. Linear codes from ruled sets in finite projective spaces. *Designs, Codes, and Cryptography*, 88 (4):747–754, April 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00707-9`.

**Leung:2020:NNR**

[2522] Ka Hin Leung and Qi Wang. New nonexistence results on $(m, 40n)$-generalized bent functions. *Designs, Codes, and Cryptography*, 88 (4):755–770, April 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00708-8`.

**Adriaensen:2020:SWC**

[2523] Sam Adriaensen, Lins Denaux, Leo Storme, and Zsuzsa Weiner. Small weight code words arising from the incidence of points and hyperplanes in PG$(n, q)$. *Designs, Codes, and Cryptography*, 88(4):771–788, April 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00710-0`.

**Dietrich:2020:DCN**

[2524] Heiko Dietrich and Jeroen Schillewaert. On a duality for codes over non-abelian groups. *Designs, Codes, and Cryptography*, 88(5):789–805, May 2020. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00711-z.

**Fang:2020:SMO**

[2525] Zenghui Fang and Junling Zhou. The sizes of maximal $(v, k, k-2, k-1)$ optical orthogonal codes. *Designs, Codes, and Cryptography*, 88 (5):807–824, May 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00714-1.

**Bhowmick:2020:DNF**

[2526] Sanjit Bhowmick, Alexandre Fotue-Tabue, Edgar Martínez-Moro, Ramakrishna Bandi, and Satya Bagchi. Do non-free LCD codes over finite commutative Frobenius rings exist? *Designs, Codes, and Cryptography*, 88(5):825–840, May 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00713-x.

**Zhou:2020:EMA**

[2527] Yue Zhou. On equivalence of maximum additive symmetric rank-distance codes. *Designs, Codes, and Cryptography*, 88(5):841–850, May 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00716-z.

**Jiang:2020:MIC**

[2528] Jing Jiang, Yujie Gu, and Minquan Cheng. Multimedia IPP codes with efficient tracing. *Designs, Codes, and Cryptography*, 88 (5):851–866, May 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00717-y.

**Ferraguti:2020:FCP**

[2529] Andrea Ferraguti and Giacomo Micheli. Full classification of permutation rational functions and complete rational functions of degree three over finite fields. *Designs, Codes, and Cryptography*, 88(5):867–886, May 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00715-0.

**Wang:2020:ISF**

[2530] Gaoli Wang, Fukang Liu, Binbin Cui, Florian Mendel, and Christoph Dobraunig. Improved (semi-free-start/near-) collision and distinguishing attacks on round-reduced RIPEMD-160. *Designs, Codes, and Cryptography*, 88(5):887–930, May 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00718-x.

**Kirshanova:2020:SPL**

[2531] Elena Kirshanova, Huyen Nguyen, Damien Stehlé, and Alexandre Wallet. On the smoothing parameter and last minimum of random orthogonal lattices. *Designs, Codes, and Cryptography*, 88(5):931–950, May 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00719-w.

**Zhu:2020:SEE**

[2532] Bohua Zhu, Junling Zhou, and Yanxun Chang. $2-(v, 405; 40m)$ spontaneous emission error designs. *Designs, Codes, and Cryptography*, 88 (5):951–970, May 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-020-00722-1`.

**Alavi:2020:FTB**

[2533] Seyed Hassan Alavi, Mohsen Bayat, Jalal Choulaki, and Ashraf Daneshkhah. Flag-transitive block designs with prime replication number and almost simple groups. *Designs, Codes, and Cryptography*, 88(5):971–992, May 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-020-00724-z`.

**Falk:2020:PCC**

[2534] Brett Hemenway Falk, Nadia Heninger, and Michael Rudow. Properties of constacyclic codes under the Schur product. *Designs, Codes, and Cryptography*, 88(6):993–1021, June 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-020-00720-3`.

**Cartor:2020:AF**

[2535] Ryann Cartor and Daniel Smith-Tone. All in the $C^*$ family. *Designs, Codes, and Cryptography*, 88 (6):1023–1036, June 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-020-00723-0`.

**Shi:2020:NRS**

[2536] Minjia Shi, Li Xu, and Denis S. Krotov. On the number of resolvable Steiner triple systems of small 3-rank. *Designs, Codes, and Cryptography*, 88 (6):1037–1046, June 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-020-00725-y`.

**Guillevic:2020:CPC**

[2537] Aurore Guillevic, Simon Masson, and Emmanuel Thomé. Cocks–Pinch curves of embedding degrees five to eight and optimal ate pairing computation. *Designs, Codes, and Cryptography*, 88(6):1047–1081, June 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-020-00727-w`.

**Sun:2020:PTM**

[2538] Hong-Yu Sun, Xuan-Yong Zhu, and Qun-Xiong Zheng. Predicting truncated multiple recursive generators with unknown parameters. *Designs, Codes, and Cryptography*, 88(6):1083–1102, June 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-020-00729-8`.

**Zhao:2020:GRK**

[2539] Boxin Zhao, Xiaoyang Dong, Willi Meier, Keting Jia, and Gaoli Wang. Generalized related-key rectangle at-

tacks on block ciphers with linear key schedule: applications to SKINNY and GIFT. *Designs, Codes, and Cryptography*, 88(6):1103–1126, June 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-020-00730-1`.

**Fang:2020:NMS**

[2540] Xiaolei Fang, Khawla Lebed, Hongwei Liu, and Jinquan Luo. New MDS self-dual codes over finite fields of odd characteristic. *Designs, Codes, and Cryptography*, 88(6):1127–1138, June 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-020-00734-x`.

**Lu:2020:SCA**

[2541] Wei Lu, Xia Wu, Xiwang Cao, and Ming Chen. Six constructions of asymptotically optimal codebooks via the character sums. *Designs, Codes, and Cryptography*, 88(6):1139–1158, June 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-020-00735-w`.

**Budaghyan:2020:PAF**

[2542] Lilya Budaghyan, Nikolay Kaleyski, Constanza Riera, and Pantelimon Stănică. Partially APN functions with APN-like polynomial representations. *Designs, Codes, and Cryptography*, 88(6):1159–1177, June 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-020-00739-6`.

**Dong:2020:QAS**

[2543] Xiaoyang Dong, Bingyou Dong, and Xiaoyun Wang. Quantum attacks on some Feistel block ciphers. *Designs, Codes, and Cryptography*, 88(6):1179–1203, June 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-020-00741-y`.

**Zhao:2020:CIN**

[2544] Xiao-Xin Zhao, Qun-Xiong Zheng, Zhong-Xiao Wang, and Wen-Feng Qi. On a class of isomorphic NFSRs. *Designs, Codes, and Cryptography*, 88(6):1205–1226, June 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-020-00742-x`.

**Chara:2020:BTC**

[2545] María Chara, Ricardo Podestá, and Ricardo Toledano. Block transitive codes attaining the Tsfasman–Vladut–Zink bound. *Designs, Codes, and Cryptography*, 88(6):1227–1253, June 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-020-00743-w`.

**Wu:2020:LCF**

[2546] Yanan Wu, Nian Li, and Xiangyong Zeng. Linear codes with few weights from cyclotomic classes and weakly regular bent functions. *Designs, Codes, and Cryptography*, 88

(6):1255–1272, June 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00744-9.

**Datta:2020:RGH**

[2547] Mrinmoy Datta. Relative generalized Hamming weights of affine Cartesian codes. *Designs, Codes, and Cryptography*, 88(6):1273–1284, June 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00745-8; https://link.springer.com/content/pdf/10.1007/s10623-020-00745-8.pdf.

**Hodzic:2020:GFS**

[2548] S. Hodzić, E. Pasalic, and Y. Wei. A general framework for secondary constructions of bent and plateaued functions. *Designs, Codes, and Cryptography*, 88(10):2007–2035, October 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00760-9.

**Potapov:2020:ABP**

[2549] Vladimir N. Potapov. On $q$-ary bent and plateaued functions. *Designs, Codes, and Cryptography*, 88(10):2037–2049, October 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00761-8.

**Ong:2020:EZD**

[2550] Kai Lin Ong and Miin Huey Ang. On equivalency of zero-divisor codes via classifying their idempotent generator. *Designs, Codes, and Cryptography*, 88(10):2051–2065, October 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00762-7.

**Gu:2020:PIS**

[2551] Yujie Gu and Shohei Satake. On 2-parent-identifying set systems of block size 4. *Designs, Codes, and Cryptography*, 88(10):2067–2076, October 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00763-6.

**Yasuda:2020:ADR**

[2552] Masaya Yasuda, Satoshi Nakamura, and Junpei Yamaguchi. Analysis of DeepBKZ reduction for finding short lattice vectors. *Designs, Codes, and Cryptography*, 88(10):2077–2100, October 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00765-4.

**Zhu:2020:RDJ**

[2553] Yan Zhu and Naoki Watamura. Relative $t$-designs in Johnson association schemes for $P$-polynomial structure. *Designs, Codes, and Cryptography*, 88(10):2101–2118, October 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00766-3.

**Wu:2020:CCT**

[2554] Mengna Wu, Chengju Li, and Zilong Wang. Characterizations and constructions of triple-cycle permutations of the form $x^r h(x^s)$. *Designs, Codes, and Cryptography*, 88(10):2119–2132, October 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00768-1.

**Elsholtz:2020:CPF**

[2555] Christian Elsholtz and Péter Pál Pach. Caps and progression-free sets in $\mathbf{Z}_m^n$. *Designs, Codes, and Cryptography*, 88(10):2133–2170, October 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00769-0; https://link.springer.com/content/pdf/10.1007/s10623-020-00769-0.pdf.

**Zheng:2020:CPF**

[2556] Lijing Zheng, Jie Peng, Haibin Kan, Yanjun Li, and Juan Luo. On constructions and properties of $(n, m)$-functions with maximal number of bent components. *Designs, Codes, and Cryptography*, 88(10):2171–2186, October 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00770-7.

**Boyadzhiyska:2020:EEM**

[2557] Simona Boyadzhiyska, Shagnik Das, and Tibor Szabó. Enumerating extensions of mutually orthogonal Latin squares. *Designs, Codes, and Cryptography*, 88(10):2187–2206, October 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00771-6; https://link.springer.com/content/pdf/10.1007/s10623-020-00771-6.pdf.

**Lambin:2020:LEB**

[2558] Baptiste Lambin, Patrick Derbez, and Pierre-Alain Fouque. Linearly equivalent S-boxes and the division property. *Designs, Codes, and Cryptography*, 88(10):2207–2231, October 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00773-4; https://link.springer.com/content/pdf/10.1007/s10623-020-00773-4.pdf.

**Mesnager:2020:BUQ**

[2559] Sihem Mesnager, Chunming Tang, and Maosheng Xiong. On the boomerang uniformity of quadratic permutations. *Designs, Codes, and Cryptography*, 88(10):2233–2246, October 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00775-2.

**Kim:2020:CSD**

[2560] Boran Kim and Yoonjin Lee. Classification of self-dual cyclic codes over the chain ring $\mathbf{Z}_p[u]/\langle u^3 \rangle$. *Designs, Codes, and Cryptography*, 88(10):2247–2273, October 2020. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00776-1.

**Gao:2020:LCS**

[2561] Yanyan Gao, Qin Yue, and Yansheng Wu. LCD codes and self-orthogonal codes in generalized dihedral group algebras. *Designs, Codes, and Cryptography*, 88(11):2275–2287, November 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00778-z.

**Liu:2020:PDC**

[2562] Yunwen Liu, Wenying Zhang, Bing Sun, Vincent Rijmen, Guoqiang Liu, Chao Li, Shaojing Fu, and Meichun Cao. The phantom of differential characteristics. *Designs, Codes, and Cryptography*, 88(11):2289–2311, November 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00782-3.

**Ekeraa:2020:PPQ**

[2563] Martin Ekerå. On post-processing in the quantum algorithm for computing short discrete logarithms. *Designs, Codes, and Cryptography*, 88(11):2313–2335, November 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00783-2; https://link.springer.com/content/pdf/10.1007/s10623-020-00783-2.pdf.

**Alavi:2020:SB**

[2564] Seyed Hassan Alavi, Ashraf Daneshkhah, and Cheryl E. Praeger. Symmetries of biplanes. *Designs, Codes, and Cryptography*, 88(11):2337–2359, November 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00784-1.

**Chee:2020:ABS**

[2565] Yeow Meng Chee, Charles J. Colbourn, Hoang Dau, Ryan Gabrys, Alan C. H. Ling, Dylan Lusi, and Olgica Milenkovic. Access balancing in storage systems by labeling partial Steiner systems. *Designs, Codes, and Cryptography*, 88(11):2361–2376, November 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00786-z.

**Xu:2020:DRS**

[2566] Juanjuan Xu, Jingjun Bao, and Lijun Ji. Doubly resolvable Steiner quadruple systems of orders $2^{2n+1}$. *Designs, Codes, and Cryptography*, 88(11):2377–2386, November 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00788-x.

**Bibak:2020:DCC**

[2567] Khodakhast Bibak. Deletion correcting codes meet the Littlewood–Offord problem. *Designs, Codes, and Cryptography*, 88(11):2387–2396, November 2020. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00787-y.

**Guneri:2020:LCP**

[2568] Cem Güneri, Edgar Martínez-Moro, and Selcen Sayici. Linear complementary pair of group codes over finite chain rings. *Designs, Codes, and Cryptography*, 88(11):2397–2405, November 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00792-1.

**Gong:2020:FCL**

[2569] Xinxin Gong and Bin Zhang. Fast computation of linear approximation over certain composition functions and applications to SNOW 2.0 and SNOW 3G. *Designs, Codes, and Cryptography*, 88(11):2407–2431, November 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00790-3.

**Lee:2020:TCS**

[2570] Youngkyung Lee, Dong Hoon Lee, and Jong Hwan Park. Tightly CCA-secure encryption scheme in a multi-user setting with corruptions. *Designs, Codes, and Cryptography*, 88(11):2433–2452, November 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00794-z.

**Huang:2020:BPL**

[2571] Xinmei Huang, Qin Yue, Yansheng Wu, Xiaoping Shi, and Jerod Michel. Binary primitive LCD BCH codes. *Designs, Codes, and Cryptography*, 88(12):2453–2473, December 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00795-y.

**Hyun:2020:OML**

[2572] Jong Yoon Hyun, Hyun Kwang Kim, Yansheng Wu, and Qin Yue. Optimal minimal linear codes from posets. *Designs, Codes, and Cryptography*, 88(12):2475–2492, December 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00793-0.

**Shi:2020:TFT**

[2573] Minjia Shi, Wang Xuan, and Patrick Solé. Two families of two-weight codes over $\mathbf{Z}_4$. *Designs, Codes, and Cryptography*, 88(12):2493–2505, December 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00796-x.

**Zhou:2020:WSF**

[2574] Junling Zhou and Wenling Zhou. Wide-sense 2-frameproof codes. *Designs, Codes, and Cryptography*, 88(12):2507–2519, December 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00797-w.

**Lisonek:2020:MNF**

[2575] Petr Lisonek. Maximal nonassociativity via fields. *Designs, Codes,*

*and Cryptography*, 88(12):2521–2530, December 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00800-4.

**Ghorpade:2020:PAG**

[2576] Sudhir R. Ghorpade and Trygve Johnsen. A polymatroid approach to generalized weights of rank metric codes. *Designs, Codes, and Cryptography*, 88(12):2531–2546, December 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00798-9; https://link.springer.com/content/pdf/10.1007/s10623-020-00798-9.pdf.

**Shi:2020:CIC**

[2577] Minjia Shi, Li Xu, and Patrick Solé. Construction of isodual codes from polycirculant matrices. *Designs, Codes, and Cryptography*, 88(12):2547–2560, December 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00799-8.

**Capaverde:2020:RPC**

[2578] Juliane Capaverde, Ariane M. Masuda, and Virgínia M. Rodrigues. Rédei permutations with cycles of the same length. *Designs, Codes, and Cryptography*, 88(12):2561–2579, December 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00801-3.

**Choi:2020:CSD**

[2579] Whan-Hyuk Choi, Hyun Jin Kim, and Yoonjin Lee. Construction of single-deletion-correcting DNA codes using CIS codes. *Designs, Codes, and Cryptography*, 88(12):2581–2596, December 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00802-2.

**Kolsch:2020:IKB**

[2580] Lukas Kölsch. On the inverses of Kasami and Bracken–Leander exponents. *Designs, Codes, and Cryptography*, 88(12):2597–2621, December 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00804-0; https://link.springer.com/content/pdf/10.1007/s10623-020-00804-0.pdf.

**Lavauzelle:2020:CSB**

[2581] Julien Lavauzelle and Julian Renner. Cryptanalysis of a system based on twisted Reed–Solomon codes. *Designs, Codes, and Cryptography*, 88(7):1285–1300, July 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00747-6.

**Chirvasitu:2020:AEQ**

[2582] Alexandru Chirvasitu and Thomas W. Cusick. Affine equivalence for quadratic rotation symmetric Boolean functions. *Designs, Codes, and Cryptography*, 88(7):1301–1329, July 2020.

CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00748-5.

**Randrianarisoa:2020:GAR**

[2583] Tovohery Hajatiana Randrianarisoa. A geometric approach to rank metric codes and a classification of constant weight codes. *Designs, Codes, and Cryptography*, 88(7):1331–1348, July 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00750-x.

**Shao:2020:OWA**

[2584] Minfeng Shao and Ying Miao. On optimal weak algebraic manipulation detection codes and weighted external difference families. *Designs, Codes, and Cryptography*, 88(7):1349–1369, July 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00754-7.

**Jia:2020:ITS**

[2585] Dingding Jia, Yamin Liu, and Bao Li. IBE with tight security against selective opening and chosen-ciphertext attacks. *Designs, Codes, and Cryptography*, 88(7):1371–1400, July 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00755-6.

**Grassi:2020:RGK**

[2586] Lorenzo Grassi and Christian Rechberger. Revisiting Gilbert's known-key distinguisher. *Designs, Codes, and Cryptography*, 88(7):1401–1445, July 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00756-5; https://link.springer.com/content/pdf/10.1007/s10623-020-00756-5.pdf.

**Ma:2020:SPC**

[2587] Xuanlong Ma, Min Feng, and Kaishun Wang. Subgroup perfect codes in Cayley sum graphs. *Designs, Codes, and Cryptography*, 88(7):1447–1461, July 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00758-3.

**Jiang:2020:LSS**

[2588] Yupeng Jiang and Dongdai Lin. Longest subsequences shared by two de Bruijn sequences. *Designs, Codes, and Cryptography*, 88(7):1463–1475, July 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00759-2.

**Beelen:2020:FSI**

[2589] Peter Beelen, Olav Geil, Edgar Martínez-Moro, and Xin-Wen Wu. Foreword-special issue: Codes, cryptology and curves in honour of Ruud Pellikaan. *Designs, Codes, and Cryptography*, 88(8):1477–1478, August 2020.

CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00780-5; https://link.springer.com/content/pdf/10.1007/s10623-020-00780-5.pdf.

**Fadavi:2020:UEE**

[2590] Mojtaba Fadavi and Reza Rezaeian Farashahi. Uniform encodings to elliptic curves and indistinguishable point representation. *Designs, Codes, and Cryptography*, 88(8):1479–1502, August 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00753-8.

**Britz:2020:WTD**

[2591] Thomas Britz, Adam Mammoliti, and Keisuke Shiromoto. Wei-type duality theorems for rank metric codes. *Designs, Codes, and Cryptography*, 88 (8):1503–1519, August 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-019-00688-9.

**Martinez-Penas:2020:HSC**

[2592] Umberto Martínez-Peñas. Hamming and simplex codes for the sum-rank metric. *Designs, Codes, and Cryptography*, 88(8):1521–1539, August 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00772-5.

**Galvez:2020:CSD**

[2593] Lucky Erap Galvez and Jon-Lark Kim. Construction of self-dual matrix codes. *Designs, Codes, and Cryptography*, 88 (8):1541–1560, August 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00740-z.

**Couvreur:2020:PEL**

[2594] Alain Couvreur and Isabella Panaccione. Power error locating pairs. *Designs, Codes, and Cryptography*, 88 (8):1561–1593, August 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00774-3.

**Castellanos:2020:WSR**

[2595] Alonso Sepúlveda Castellanos and Maria Bras-Amorós. Weierstrass semigroup at $m + 1$ rational points in maximal curves which cannot be covered by the Hermitian curve. *Designs, Codes, and Cryptography*, 88 (8):1595–1616, August 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00757-4.

**Bras-Amoros:2020:IDF**

[2596] Maria Bras-Amorós, Iwan Duursma, and Euijin Hong. Isometry-dual flags of AG codes. *Designs, Codes, and Cryptography*, 88(8):1617–1638, August 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00752-9.

**Christensen:2020:SEQ**

[2597] René Bødker Christensen and Olav Geil. Steane-enlargement of quantum codes from the Hermitian function field. *Designs, Codes, and Cryptography*, 88(8):1639–1652, August 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00709-7`.

**Garcia-Marco:2020:HDA**

[2598] Ignacio García-Marco, Irene Márquez-Corbella, and Diego Ruano. High dimensional affine codes whose square has a designed minimum distance. *Designs, Codes, and Cryptography*, 88(8):1653–1672, August 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-020-00764-5`.

**Lopez:2020:MCC**

[2599] Hiram H. López, Gretchen L. Matthews, and Ivan Soprunov. Monomial-Cartesian codes and their duals, with applications to LCD codes, quantum codes, and locally recoverable codes. *Designs, Codes, and Cryptography*, 88(8):1673–1685, August 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-020-00726-x`.

**Marquez-Corbella:2020:CSR**

[2600] Irene Márquez-Corbella, Edgar Martínez-Moro, and Carlos Munuera. Computing sharp recovery structures for locally recoverable codes. *Designs, Codes, and Cryptography*, 88(8):1687–1698, August 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-020-00746-7`.

**Canteaut:2020:ECC**

[2601] Anne Canteaut, Gohar Kyureghyan, Alexander Pott, and Felix Ulmer. Editorial: Coding and cryptography 2019. *Designs, Codes, and Cryptography*, 88(9):1699, September 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-020-00791-2; https://link.springer.com/content/pdf/10.1007/s10623-020-00791-2.pdf`.

**Polujan:2020:CBF**

[2602] Alexandr A. Polujan and Alexander Pott. Cubic bent functions outside the completed Maiorana–McFarland class. *Designs, Codes, and Cryptography*, 88(9):1701–1722, September 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00712-y`. See correction [2682].

**Gerike:2020:PFF**

[2603] Daniel Gerike and Gohar M. Kyureghyan. Permutations on finite fields with invariant cycle structure on lines. *Designs, Codes, and Cryptography*, 88(9):1723–1740, September 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-020-00721-2; https:`

//link.springer.com/content/pdf/10.1007/s10623-020-00721-2.pdf.

**Tan:2020:TCO**

[2604] Pan Tan, Zhengchun Zhou, Vladimir Sidorenko, and Udaya Parampalli. Two classes of optimal LRCs with information $(r, t)$-locality. *Designs, Codes, and Cryptography*, 88(9):1741–1757, September 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00728-9.

**Liu:2020:COL**

[2605] Jian Liu, Sihem Mesnager, and Deng Tang. Constructions of optimal locally recoverable codes via Dickson polynomials. *Designs, Codes, and Cryptography*, 88(9):1759–1780, September 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00731-0.

**Etzion:2020:SPC**

[2606] Tuvi Etzion, Sascha Kurz, Kamil Otal, and Ferruh Özbudak. Subspace packings: constructions and bounds. *Designs, Codes, and Cryptography*, 88(9):1781–1810, September 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00732-z.

**Boyvalenkov:2020:UBE**

[2607] P. G. Boyvalenkov, P. D. Dragnev, D. P. Hardin, E. B. Saff, and M. M. Stoyanova. Upper bounds for energies of spherical codes of given cardinality and separation. *Designs, Codes, and Cryptography*, 88(9):1811–1826, September 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00733-y.

**Dey:2020:PBS**

[2608] Sabyasachi Dey and Santanu Sarkar. Proving the biases of Salsa and ChaCha in differential attack. *Designs, Codes, and Cryptography*, 88(9):1827–1856, September 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00736-9.

**Deneuville:2020:CCB**

[2609] Jean-Christophe Deneuville and Philippe Gaborit. Cryptanalysis of a code-based one-time signature. *Designs, Codes, and Cryptography*, 88(9):1857–1866, September 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00737-8.

**Salagean:2020:CBF**

[2610] Ana Salagean and Ferruh Özbudak. Counting Boolean functions with faster points. *Designs, Codes, and Cryptography*, 88(9):1867–1883, September 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00738-7; https://link.springer.com/content/pdf/10.1007/s10623-020-00738-7.pdf.

**Egorova:2020:NBT**

[2611] Elena Egorova, Marcel Fernandez, and Grigory Kabatiansky. On non-binary traceability set systems. *Designs, Codes, and Cryptography*, 88(9): 1885–1892, September 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-020-00749-4`.

**Matsumoto:2020:MRS**

[2612] Ryutaroh Matsumoto. Message randomization and strong security in quantum stabilizer-based secret sharing for classical secrets. *Designs, Codes, and Cryptography*, 88(9):1893–1907, September 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-020-00751-w`; `https://link.springer.com/content/pdf/10.1007/s10623-020-00751-w.pdf`.

**Matthews:2020:CLC**

[2613] Gretchen L. Matthews and Fernando Piñero. Codes with locality from cyclic extensions of Deligne–Lusztig curves. *Designs, Codes, and Cryptography*, 88(9):1909–1924, September 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-020-00767-2`.

**Rousseva:2020:GAE**

[2614] Assia Rousseva and Ivan Landjev. The geometric approach to the existence of some quaternary Griesmer codes. *Designs, Codes, and Cryptography*, 88(9): 1925–1940, September 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-020-00777-0`.

**Coggia:2020:SLR**

[2615] Daniel Coggia and Alain Couvreur. On the security of a loidreau rank metric code based encryption scheme. *Designs, Codes, and Cryptography*, 88(9): 1941–1957, September 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-020-00781-4`.

**Tian:2020:BUP**

[2616] Shizhu Tian, Christina Boura, and Léo Perrin. Boomerang uniformity of popular S-box constructions. *Designs, Codes, and Cryptography*, 88(9): 1959–1989, September 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-020-00785-0`.

**Boucher:2020:ADS**

[2617] Delphine Boucher. An algorithm for decoding skew Reed–Solomon codes with respect to the skew metric. *Designs, Codes, and Cryptography*, 88(9): 1991–2005, September 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-020-00789-w`.

**Mesnager:2021:CMB**

[2618] Sihem Mesnager, Sihong Su, and Hui Zhang. A construction method of balanced rotation symmetric Boolean functions on arbitrary even number of

variables with optimal algebraic immunity. *Designs, Codes, and Cryptography*, 89(1):1–17, January 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00806-y.

**Budaghyan:2021:GIS**

[2619] Lilya Budaghyan, Marco Calderini, Claude Carlet, Robert Coulter, and Irene Villa. Generalized isotopic shift construction for APN functions. *Designs, Codes, and Cryptography*, 89(1):19–32, January 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00803-1; https://link.springer.com/content/pdf/10.1007/s10623-020-00803-1.pdf.

**Calderini:2021:DLU**

[2620] Marco Calderini. Differentially low uniform permutations from known 4-uniform functions. *Designs, Codes, and Cryptography*, 89(1):33–52, January 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00807-x; https://link.springer.com/content/pdf/10.1007/s10623-020-00807-x.pdf.

**Almeida:2021:NRM**

[2621] P. Almeida and D. Napp. A new rank metric for convolutional codes. *Designs, Codes, and Cryptography*, 89(1):53–73, January 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00808-w.

**Meidl:2021:BBF**

[2622] Wilfried Meidl and Isabel Pirsic. Bent and $\mathbf{Z}_{2^k}$-bent functions from spread-like partitions. *Designs, Codes, and Cryptography*, 89(1):75–89, January 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00805-z.

**Wang:2021:IUB**

[2623] Xin Wang. Improved upper bounds for parent-identifying set systems and separable codes. *Designs, Codes, and Cryptography*, 89(1):91–104, January 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00809-9.

**Grezet:2021:CHL**

[2624] Matthias Grezet and Camilla Hollanti. The complete hierarchical locality of the punctured simplex code. *Designs, Codes, and Cryptography*, 89(1):105–125, January 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00810-2; https://link.springer.com/content/pdf/10.1007/s10623-020-00810-2.pdf.

**Chakraborty:2021:FCM**

[2625] Pranab Chakraborty and Subhamoy Maitra. Further clarification on Mantin's digraph repetition bias in RC4. *Designs, Codes, and Cryptography*, 89(1):127–141, January 2021.

CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00814-y.

**Bamiloshin:2021:CIM**

[2626] Michael Bamiloshin, Aner Ben-Efraim, Oriol Farràs, and Carles Padró. Common information, matroid representation, and secret sharing for matroid ports. *Designs, Codes, and Cryptography*, 89(1):143–166, January 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00811-1.

**Oblaukhov:2021:MRR**

[2627] Alexey Oblaukhov. On metric regularity of Reed–Muller codes. *Designs, Codes, and Cryptography*, 89(1):167–197, January 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00813-z.

**Ballico:2021:SSC**

[2628] Edoardo Ballico, Giuseppe Favacchio, Elena Guardo, and Lorenzo Milazzo. Steiner systems and configurations of points. *Designs, Codes, and Cryptography*, 89(2):199–219, February 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00815-x; https://link.springer.com/content/pdf/10.1007/s10623-020-00815-x.pdf.

**Hasan:2021:DUC**

[2629] Sartaj Ul Hasan, Mohit Pal, Constanza Riera, and Pantelimon Stănică. On the $c$-differential uniformity of certain maps over finite fields. *Designs, Codes, and Cryptography*, 89(2):221–239, February 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00812-0.

**Zhao:2021:EGT**

[2630] Xiaopeng Zhao, Zhenfu Cao, Xiaolei Dong, and Jun Shao. Extended Galbraith's test on the anonymity of IBE schemes from higher residuosity. *Designs, Codes, and Cryptography*, 89(2):241–253, February 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00816-w.

**Zhou:2021:TKC**

[2631] Jingkun Zhou, Zhiwen He, and Zhao Chai. Two kinds of constructions of directed strongly regular graphs. *Designs, Codes, and Cryptography*, 89(2):255–268, February 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00817-9.

**Jaramillo:2021:ECT**

[2632] Delio Jaramillo, Maria Vaz Pinto, and Rafael H. Villarreal. Evaluation codes and their basic parameters. *Designs, Codes, and Cryptography*, 89(2):269–300, February 2021. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00818-8.

**Carvalho:2021:TCD**

[2633] Cícero Carvalho and Victor G. L. Neumann. Towards the complete determination of next-to-minimal weights of projective Reed–Muller codes. *Designs, Codes, and Cryptography*, 89 (2):301–315, February 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00821-z.

**Ye:2021:MAC**

[2634] Chen-Dong Ye, Tian Tian, and Fan-Yang Zeng. The MILP-aided conditional differential attack and its application to Trivium. *Designs, Codes, and Cryptography*, 89(2):317–339, February 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00822-y.

**Bannai:2021:CCI**

[2635] Eiichi Bannai, Manabu Oura, and Da Zhao. The complex conjugate invariants of Clifford groups. *Designs, Codes, and Cryptography*, 89 (2):341–350, February 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00819-7.

**Renner:2021:LRP**

[2636] Julian Renner, Alessandro Neri, and Sven Puchinger. Low-rank parity-check codes over Galois rings. *Designs, Codes, and Cryptography*, 89 (2):351–386, February 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00825-9; https://link.springer.com/content/pdf/10.1007/s10623-020-00825-9.pdf.

**Johnsen:2021:GWM**

[2637] Trygve Johnsen and Hugues Verdure. Greedy weights for matroids. *Designs, Codes, and Cryptography*, 89 (2):387–405, February 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00824-w; https://link.springer.com/content/pdf/10.1007/s10623-020-00824-w.pdf.

**Guo:2021:BBS**

[2638] Chun Guo and Guoyan Zhang. Beyond-birthday security for permutation-based Feistel networks. *Designs, Codes, and Cryptography*, 89(3):407–440, March 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00820-0.

**Carlet:2021:DPA**

[2639] Claude Carlet, Kwang Ho Kim, and Sihem Mesnager. A direct proof of APN-ness of the Kasami functions. *Designs, Codes, and Cryptography*, 89 (3):441–446, March 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00830-y.

**Gluesing-Luerssen:2021:DDC**

[2640] Heide Gluesing-Luerssen and Hunter Lehmann. Distance distributions of cyclic orbit codes. *Designs, Codes, and Cryptography*, 89(3):447–470, March 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00823-x.

**Bartoli:2021:WDS**

[2641] Daniele Bartoli, Matteo Bonini, and Marco Timpanella. On the weight distribution of some minimal codes. *Designs, Codes, and Cryptography*, 89(3):471–487, March 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00826-8.

**Innamorati:2021:CSC**

[2642] Stefano Innamorati and Fulvio Zuanni. Classifying sets of class $[1, q+1, 2q+1, q^2+q+1]_2$ in $\mathrm{PG}(r, q)$, $r \geq 3$. *Designs, Codes, and Cryptography*, 89(3):489–496, March 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00833-9.

**Lopez:2021:HLC**

[2643] Hiram H. López, Beth Malmskog, Gretchen L. Matthews, Fernando Piñero-González, and Mary Wootters. Hermitian-lifted codes. *Designs, Codes, and Cryptography*, 89(3):497–515, March 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00836-6.

**Davis:2021:ADS**

[2644] James A. Davis, J. J. Hoo, Connor Kissane, Ziming Liu, Calvin Reedy, Kartikey Sharma, Ken Smith, and Yiwei Sun. Abelian difference sets with the symmetric difference property. *Designs, Codes, and Cryptography*, 89(3):517–523, March 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00829-5.

**Cavenagh:2021:MSM**

[2645] Nicholas J. Cavenagh, Adam Mammoliti, and Ian M. Wanless. Maximal sets of mutually orthogonal frequency squares. *Designs, Codes, and Cryptography*, 89(3):525–558, March 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00832-w.

**Kurz:2021:PCS**

[2646] Sascha Kurz and Eitan Yaakobi. PIR codes with short block length. *Designs, Codes, and Cryptography*, 89(3):559–587, March 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00828-6.

**vanTrung:2021:ETR**

[2647] Tran van Trung. An extending theorem for $s$-resolvable $t$-designs. *Designs, Codes, and Cryptography*, 89(3):589–597, March 2021. CODEN

DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00835-7.

**Armario:2021:GHF**

[2648] José Andrés Armario, Ivan Bailera, and Ronan Egan. Generalized Hadamard full propelinear codes. *Designs, Codes, and Cryptography*, 89 (4):599–615, April 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00827-7.

**Araya:2021:CCO**

[2649] Makoto Araya, Masaaki Harada, and Ken Saito. Characterization and classification of optimal LCD codes. *Designs, Codes, and Cryptography*, 89 (4):617–640, April 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00834-8.

**Sidana:2021:RGD**

[2650] Tania Sidana and Anuradha Sharma. Roulette games and depths of words over finite commutative rings. *Designs, Codes, and Cryptography*, 89 (4):641–678, April 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00838-4.

**Wang:2021:GLS**

[2651] Zhongxiao Wang, Qunxiong Zheng, Xiaoxin Zhao, and Xiutao Feng. Grain-like structures with minimal and maximal period sequences. *Designs, Codes, and Cryptography*, 89 (4):679–693, April 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00839-3.

**Sun:2021:ACY**

[2652] Yuhua Sun, Tongjiang Yan, and Qiuyan Wang. The 2-adic complexity of Yu–gong sequences with interleaved structure and optimal autocorrelation magnitude. *Designs, Codes, and Cryptography*, 89(4):695–707, April 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00841-9.

**Ghosh:2021:VWC**

[2653] Sebati Ghosh and Palash Sarkar. Variants of Wegman–Carter message authentication code supporting variable tag lengths. *Designs, Codes, and Cryptography*, 89(4):709–736, April 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00840-w.

**Li:2021:CSP**

[2654] Kangquan Li, Chunlei Li, Tor Helleseth, and Longjiang Qu. Cryptographically strong permutations from the butterfly structure. *Designs, Codes, and Cryptography*, 89(4):737–761, April 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00837-5. See note [2751].

**Miezaki:2021:DTA**

[2655] Tsuyoshi Miezaki. Design-theoretic analogies between codes, lattices, and vertex operator algebras. *Designs, Codes, and Cryptography*, 89 (5):763–780, May 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00842-2`.

**Meng:2021:CDR**

[2656] Zhaoping Meng, Bin Zhang, and Zhanggui Wu. Constructions of doubly resolvable Steiner quadruple systems. *Designs, Codes, and Cryptography*, 89(5):781–795, May 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00844-0`.

**Liu:2021:AEA**

[2657] Hualu Liu, Peng Hu, and Xiusheng Liu. Asymmetric entanglement-assisted quantum codes: bound and constructions. *Designs, Codes, and Cryptography*, 89(5):797–809, May 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00845-z`.

**Ball:2021:SCQ**

[2658] Simeon Ball. Some constructions of quantum MDS codes. *Designs, Codes, and Cryptography*, 89(5):811–821, May 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00846-y`.

**Sok:2021:NFS**

[2659] Lin Sok. New families of self-dual codes. *Designs, Codes, and Cryptography*, 89(5):823–841, May 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00847-x`.

**Miezaki:2021:NAM**

[2660] Tsuyoshi Miezaki, Akihiro Munemasa, and Hiroyuki Nakasora. A note on Assmus–Mattson type theorems. *Designs, Codes, and Cryptography*, 89 (5):843–858, May 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00848-w`.

**Mennink:2021:REM**

[2661] Bart Mennink and Samuel Neves. On the resilience of Even–Mansour to invariant permutations. *Designs, Codes, and Cryptography*, 89 (5):859–893, May 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00850-2`; `https://link.springer.com/content/pdf/10.1007/s10623-021-00850-2.pdf`.

**Jia:2021:CSP**

[2662] Dingding Jia and Benoît Libert. SO-CCA secure PKE from pairing based all-but-many lossy trapdoor functions. *Designs, Codes, and Cryptography*, 89(5):895–923, May 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https:`

//link.springer.com/article/10.1007/s10623-021-00849-9.

**Kuchta:2021:LBZ**

[2663] Veronika Kuchta, Amin Sakzad, Ron Steinfeld, and Joseph K. Liu. Lattice-based zero-knowledge arguments for additive and multiplicative relations. *Designs, Codes, and Cryptography*, 89(5):925–963, May 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00851-1.

**Aguglia:2021:NMC**

[2664] Angela Aguglia, Luca Giuzzi, and Angelo Sonnino. Near-MDS codes from elliptic curves. *Designs, Codes, and Cryptography*, 89(5):965–972, May 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00852-0; https://link.springer.com/content/pdf/10.1007/s10623-021-00852-0.pdf.

**Cho:2021:SCI**

[2665] Wonhee Cho, Jiseung Kim, and Changmin Lee. (In)security of concrete instantiation of Lin17's functional encryption scheme from noisy multilinear maps. *Designs, Codes, and Cryptography*, 89(5):973–1016, May 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00854-y.

**Cui:2021:RRF**

[2666] Nan Cui, Shengli Liu, Dawu Gu, and Jian Weng. Robustly reusable fuzzy extractor with imperfect randomness. *Designs, Codes, and Cryptography*, 89(5):1017–1059, May 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00843-1.

**Shafieinejad:2021:SPQ**

[2667] Masoumeh Shafieinejad and Navid Nasr Esfahani. A scalable post-quantum hash-based group signature. *Designs, Codes, and Cryptography*, 89(5):1061–1090, May 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00857-9.

**Ankur:2021:SDC**

[2668] Ankur and Pramod Kumar Kewat. Self-dual codes over $\mathbf{F}_2[u]/\langle u^4\rangle$ and Jacobi forms over a totally real subfield of $\mathbf{Q}(\zeta_8)$. *Designs, Codes, and Cryptography*, 89(5):1091–1109, May 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00860-0.

**Feng:2021:TRS**

[2669] Hanwen Feng, Jianwei Liu, and Qianhong Wu. Traceable ring signatures: general framework and post-quantum security. *Designs, Codes, and Cryptography*, 89(6):1111–1145, June 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00863-x.

**Dong:2021:FTD**

[2670] Huili Dong. Flag-transitive 4-designs and $PSL(2, q)$ groups. *Designs, Codes, and Cryptography*, 89(6):1147–1157, June 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00867-7`.

**Guo:2021:CLS**

[2671] Jun Guo. Cameron–Liebler sets in bilinear forms graphs. *Designs, Codes, and Cryptography*, 89(6):1159–1180, June 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00864-w`.

**Yan:2021:DSC**

[2672] Haode Yan and Chengju Li. Differential spectra of a class of power permutations with characteristic 5. *Designs, Codes, and Cryptography*, 89(6):1181–1191, June 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00865-9`.

**Zha:2021:SCP**

[2673] Zhengbang Zha and Lei Hu. Some classes of power functions with low $c$-differential uniformity over finite fields. *Designs, Codes, and Cryptography*, 89(6):1193–1210, June 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00866-8`.

**Hawtin:2021:EEC**

[2674] Daniel R. Hawtin. $s$-elusive codes in Hamming graphs. *Designs, Codes, and Cryptography*, 89(6):1211–1220, June 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00868-6`.

**Bartoli:2021:CSO**

[2675] Daniele Bartoli, Maria Montanucci, and Giovanni Zini. On certain self-orthogonal AG codes with applications to quantum error-correcting codes. *Designs, Codes, and Cryptography*, 89(6):1221–1239, June 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00870-y`.

**Chakraborty:2021:ACJ**

[2676] Himadri Shekhar Chakraborty and Tsuyoshi Miezaki. Average of complete joint weight enumerators and self-dual codes. *Designs, Codes, and Cryptography*, 89(6):1241–1254, June 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00874-8`.

**Chen:2021:FTP**

[2677] Jianfu Chen and Shenglin Zhou. Flag-transitive, point-imprimitive $2-(v, k, \lambda)$ symmetric designs with $k$ and $\lambda$ prime powers. *Designs, Codes, and Cryptography*, 89(6):1255–1260, June 2021. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00869-5.

**Falcone:2021:BHC**

[2678] Giovanni Falcone and Marco Pavone. Binary Hamming codes and Boolean designs. *Designs, Codes, and Cryptography*, 89(6):1261–1277, June 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00853-z.

**Renner:2021:LCB**

[2679] Julian Renner, Sven Puchinger, and Antonia Wachter-Zeh. LIGA: a cryptosystem based on the hardness of rank-metric list and interleaved decoding. *Designs, Codes, and Cryptography*, 89(6):1279–1319, June 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00861-z.

**Turner:2021:LPL**

[2680] Jonathan S. Turner, Ilias S. Kotsireas, and Andrew J. Geyer. A Legendre pair of length 77 using complementary binary matrices with fixed marginals. *Designs, Codes, and Cryptography*, 89(6):1321–1333, June 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00862-y.

**Chakraborty:2021:CEF**

[2681] Olive Chakraborty, Jean-Charles Faugère, and Ludovic Perret. Cryptanalysis of the extension field cancellation cryptosystem. *Designs, Codes, and Cryptography*, 89(6):1335–1364, June 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00873-9.

**Polujan:2021:CCB**

[2682] Alexandr A. Polujan and Alexander Pott. Correction to: Cubic bent functions outside the completed Maiorana–McFarland class. *Designs, Codes, and Cryptography*, 89(6):1365–1366, June 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00877-5. See [2602].

**Lopez:2021:DEC**

[2683] Hiram H. López, Ivan Soprunov, and Rafael H. Villarreal. The dual of an evaluation code. *Designs, Codes, and Cryptography*, 89(7):1367–1403, July 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00872-w.

**Shi:2021:BLC**

[2684] Tairong Shi, Wenling Wu, and Sengpeng Wang. Breaking LWC candidates: sESTATE and elephant in quantum setting. *Designs, Codes, and Cryptography*, 89(7):1405–1432, July 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00875-7.

**Sajadieh:2021:CTM**

[2685] Mahdi Sajadieh and Mohsen Mousavi. Construction of MDS matrices from generalized Feistel structures. *Designs, Codes, and Cryptography*, 89 (7):1433–1452, July 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00876-6.

**Yang:2021:CLI**

[2686] Yumeng Yang, Xiangyong Zeng, and Shi Wang. Construction of lightweight involutory MDS matrices. *Designs, Codes, and Cryptography*, 89(7):1453–1483, July 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00879-3.

**Zhang:2021:WMB**

[2687] Fengrong Zhang, Enes Pasalic, and Yongzhuang Wei. Wide minimal binary linear codes from the general Maiorana–McFarland class. *Designs, Codes, and Cryptography*, 89 (7):1485–1507, July 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00883-7.

**Abdukhalikov:2021:ECN**

[2688] Kanat Abdukhalikov. Equivalence classes of Niho bent functions. *Designs, Codes, and Cryptography*, 89 (7):1509–1534, July 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00885-5.

**Emura:2021:ASR**

[2689] Keita Emura, Atsushi Takayasu, and Yohei Watanabe. Adaptively secure revocable hierarchical IBE from $k$-linear assumption. *Designs, Codes, and Cryptography*, 89(7):1535–1574, July 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00880-w.

**Zhou:2021:NGC**

[2690] Yanwei Zhou, Bo Yang, and Yi Mu. Novel generic construction of leakage-resilient PKE scheme with CCA security. *Designs, Codes, and Cryptography*, 89(7):1575–1614, July 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-020-00831-x.

**Dougherty:2021:CMG**

[2691] Steven T. Dougherty, Joe Gildea, and Abidin Kaya. Composite matrices from group rings, composite $G$-codes and constructions of self-dual codes. *Designs, Codes, and Cryptography*, 89 (7):1615–1638, July 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00882-8.

**Chen:2021:GPO**

[2692] Ruikai Chen, Sihem Mesnager, and Chang-An Zhao. Good polynomials for optimal LRC of low locality. *Designs, Codes, and Cryptography*, 89 (7):1639–1660, July 2021. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00886-4.

**Etzion:2021:LSM**

[2693] Tuvi Etzion and Junling Zhou. Large sets with multiplicity. *Designs, Codes, and Cryptography*, 89(7):1661–1690, July 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00878-4.

**Liu:2021:PGC**

[2694] Huaning Liu and Xi Liu. On the properties of generalized cyclotomic binary sequences of period $2p^m$. *Designs, Codes, and Cryptography*, 89(7):1691–1712, July 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00887-3.

**Ding:2021:PGL**

[2695] Cunsheng Ding, Chunming Tang, and Vladimir D. Tonchev. The projective general linear group $\mathrm{PGL}(2, 2^{\mathrm{m}})$ and linear codes of length $2^m + 1$. *Designs, Codes, and Cryptography*, 89(7):1713–1734, July 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00888-2.

**Farras:2021:PPD**

[2696] Oriol Farràs, Jordi Ribes-González, and Sara Ricci. Privacy-preserving data splitting: a combinatorial approach. *Designs, Codes, and Cryptography*, 89(7):1735–1756, July 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00884-6.

**Gong:2021:SEF**

[2697] Junqing Gong and Haifeng Qian. Simple and efficient FE for quadratic functions. *Designs, Codes, and Cryptography*, 89(8):1757–1786, August 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00871-x.

**Chauhan:2021:HWD**

[2698] Varsha Chauhan, Anuradha Sharma, and Monika Yadav. Hamming weight distributions of multi-twisted codes over finite fields. *Designs, Codes, and Cryptography*, 89(8):1787–1837, August 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00889-1.

**Chisaki:2021:CCT**

[2699] Shoko Chisaki, Ryoh Fuji-Hara, and Nobuko Miyamoto. A construction for circulant type dropout designs. *Designs, Codes, and Cryptography*, 89(8):1839–1852, August 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00890-8.

**Zini:2021:SSR**

[2700] Giovanni Zini and Ferdinando Zullo. Scattered subspaces and related codes. *Designs, Codes, and Cryptography*, 89

(8):1853–1873, August 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00891-7.

**Song:2021:SAS**

[2701] Ling Song, Yi Tu, and Lei Hu. Security analysis of Subterranean 2.0. *Designs, Codes, and Cryptography*, 89 (8):1875–1905, August 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00892-6.

**Ghosh:2021:BTE**

[2702] Sebati Ghosh and Palash Sarkar. Breaking tweakable enciphering schemes using Simon's algorithm. *Designs, Codes, and Cryptography*, 89(8):1907–1926, August 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00893-5.

**Takayasu:2021:TBA**

[2703] Atsushi Takayasu. Tag-based ABE in prime-order groups via pair encoding. *Designs, Codes, and Cryptography*, 89 (8):1927–1963, August 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00894-4.

**Takayasu:2021:ASL**

[2704] Atsushi Takayasu. Adaptively secure lattice-based revocable IBE in the QROM: compact parameters, tight security, and anonymity. *Designs, Codes, and Cryptography*, 89(8):1965–1992, August 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00895-3.

**Heng:2021:FPT**

[2705] Ziling Heng, Dexiang Li, and Fuling Chen. A family of projective two-weight linear codes. *Designs, Codes, and Cryptography*, 89(8):1993–2007, August 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00896-2.

**Wang:2021:BLC**

[2706] Xiaoqiang Wang, Dabin Zheng, and Yan Zhang. Binary linear codes with few weights from Boolean functions. *Designs, Codes, and Cryptography*, 89 (8):2009–2030, August 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00898-0.

**Chen:2021:CGP**

[2707] Ruikai Chen, Sihem Mesnager, and Chang-An Zhao. Correction to: Good polynomials for optimal LRC of low locality. *Designs, Codes, and Cryptography*, 89(8):2031, August 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00909-0.

**Kharaghani:2021:BSO**

[2708] Hadi Kharaghani, Thomas Pender, and Sho Suda. Balancedly splittable orthogonal designs and equiangular tight frames. *Designs, Codes,*

*and Cryptography*, 89(9):2033–2050, September 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00897-1.

**Liu:2021:CMT**

[2709] Hongwei Liu and Shengwei Liu. Construction of MDS twisted Reed–Solomon codes and LCD–MDS codes. *Designs, Codes, and Cryptography*, 89(9):2051–2065, September 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00899-z.

**Ligeti:2021:GTS**

[2710] Peter Ligeti, Peter Sziklai, and Marcella Takáts. Generalized threshold secret sharing and finite geometry. *Designs, Codes, and Cryptography*, 89(9):2067–2078, September 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00900-9.

**Ghasemi:2021:IHS**

[2711] Fatemeh Ghasemi, Reza Kaboli, and Mohammad-Mahdi Rafiei. On ideal homomorphic secret sharing schemes and their decomposition. *Designs, Codes, and Cryptography*, 89(9):2079–2096, September 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00901-8.

**Aragon:2021:CCB**

[2712] Nicolas Aragon, Marco Baldi, and Paolo Santini. Cryptanalysis of a code-based full-time signature. *Designs, Codes, and Cryptography*, 89(9):2097–2112, September 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00902-7.

**Sadeghi:2021:PMB**

[2713] Sadegh Sadeghi, Vincent Rijmen, and Nasour Bagheri. Proposing an MILP-based method for the experimental verification of difference-based trails: application to SPECK, SIMECK. *Designs, Codes, and Cryptography*, 89(9):2113–2155, September 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00904-5.

**Ballico:2021:LRC**

[2714] E. Ballico. Locally recoverable codes correcting many erasures over small fields. *Designs, Codes, and Cryptography*, 89(9):2157–2162, September 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00905-4.

**Johnsen:2021:MCP**

[2715] Trygve Johnsen and Hugues Verdure. Möbius and coboundary polynomials for matroids. *Designs, Codes, and Cryptography*, 89(9):2163–2177, September 2021. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00906-3.

**Chen:2021:NFE**

[2716] Xiaojing Chen, Shixin Zhu, and Gaojun Luo. A new family of EAQMDS codes constructed from constacyclic codes. *Designs, Codes, and Cryptography*, 89(9):2179–2193, September 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00908-1.

**Huang:2021:MNS**

[2717] Daitao Huang, Qin Yue, and Xia Li. MDS or NMDS self-dual codes from twisted generalized Reed–Solomon codes. *Designs, Codes, and Cryptography*, 89(9):2195–2209, September 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00910-7.

**Davydov:2021:TCP**

[2718] Alexander A. Davydov, Stefano Marcugini, and Fernanda Pambianco. Twisted cubic and point-line incidence matrix in PG$(3, q)$. *Designs, Codes, and Cryptography*, 89(10):2211–2233, October 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00911-6.

**Alfarano:2021:CLC**

[2719] Gianira N. Alfarano, Julia Lieb, and Joachim Rosenthal. Construction of LDPC convolutional codes via difference triangle sets. *Designs, Codes, and Cryptography*, 89(10):2235–2254, October 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00912-5.

**Bhaumik:2021:IIS**

[2720] Ritam Bhaumik, Mridul Nandi, and Anik Raychaudhuri. Improved indifferentiability security proof for 3-round tweakable Luby–Rackoff. *Designs, Codes, and Cryptography*, 89(10):2255–2281, October 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00913-4.

**Abdukhalikov:2021:ECC**

[2721] Kanat Abdukhalikov and Duy Ho. Extended cyclic codes, maximal arcs and ovoids. *Designs, Codes, and Cryptography*, 89(10):2283–2294, October 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00915-2.

**Harada:2021:CBL**

[2722] Masaaki Harada. Construction of binary LCD codes, ternary LCD codes and quaternary Hermitian LCD codes. *Designs, Codes, and Cryptography*, 89(10):2295–2312, October 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00916-1.

**Cesmelioglu:2021:VBF**

[2723] Ayça Çesmelioglu, Wilfried Meidl, and Isabel Pirsic. Vectorial bent functions and partial difference sets. *Designs, Codes, and Cryptography*, 89(10):2313–2330, October 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00919-y`.

**Alonso-Gonzalez:2021:COF**

[2724] Clementa Alonso-González and Miguel Ángel Navarro-Pérez. Cyclic orbit flag codes. *Designs, Codes, and Cryptography*, 89(10):2331–2356, October 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00920-5`.

**Chen:2021:PKE**

[2725] Yu-Chi Chen, Xin Xie, and Raylin Tso. Public key encryption with filtered equality test revisited. *Designs, Codes, and Cryptography*, 89(10):2357–2372, October 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00924-1`.

**Colbourn:2021:EST**

[2726] Charles J. Colbourn. Egalitarian Steiner triple systems for data popularity. *Designs, Codes, and Cryptography*, 89(10):2373–2395, October 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00925-0`.

**Emura:2021:EIB**

[2727] Keita Emura, Atsushi Takayasu, and Yohei Watanabe. Efficient identity-based encryption with hierarchical key-insulation from HIBE. *Designs, Codes, and Cryptography*, 89(10):2397–2431, October 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00926-z`.

**Rozhkov:2021:SCA**

[2728] Michail I. Rozhkov and Alexander V. Sorokin. Some conditions for absence of affine functions in NFSR output stream. *Designs, Codes, and Cryptography*, 89(11):2433–2443, November 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00928-x`.

**Bouyuklieva:2021:OBL**

[2729] Stefka Bouyuklieva. Optimal binary LCD codes. *Designs, Codes, and Cryptography*, 89(11):2445–2461, November 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00929-w`.

**Bapic:2021:NMS**

[2730] A. Bapić and E. Pasalic. A new method for secondary constructions of vectorial bent functions. *Designs, Codes, and Cryptography*, 89(11):2463–2475, November 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https:`

//link.springer.com/article/10.1007/s10623-021-00930-3.

**Wang:2021:BLI**

[2731] Qian Wang and Chenhui Jin. Bounding the length of impossible differentials for SPN block ciphers. *Designs, Codes, and Cryptography*, 89(11):2477–2493, November 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00932-1.

**Hu:2021:LCP**

[2732] Peng Hu and Xiusheng Liu. Linear complementary pairs of codes over rings. *Designs, Codes, and Cryptography*, 89(11):2495–2509, November 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00933-0.

**Wang:2021:NPP**

[2733] Xiang Wang, Yuanjie Wang, and Fang-Wei Fu. Nonexistence of perfect permutation codes under the Kendall $\tau$ -metric. *Designs, Codes, and Cryptography*, 89(11):2511–2531, November 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00934-z.

**Chen:2021:CCS**

[2734] Xiaojing Chen, Shixin Zhu, and Wan Jiang. Cyclic codes and some new entanglement-assisted quantum MDS codes. *Designs, Codes, and Cryptography*, 89(11):2533–2551, November 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00935-y.

**Fickus:2021:GCP**

[2735] Matthew Fickus, Joseph W. Iverson, and Emily J. King. Grassmannian codes from paired difference sets. *Designs, Codes, and Cryptography*, 89(11):2553–2576, November 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00937-w.

**Tomida:2021:FCE**

[2736] Junichi Tomida, Yuto Kawahara, and Ryo Nishimaki. Fast, compact, and expressive attribute-based encryption. *Designs, Codes, and Cryptography*, 89(11):2577–2626, November 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00939-8.

**Hasan:2021:BUC**

[2737] Sartaj Ul Hasan, Mohit Pal, and Pantelimon Stănică. Boomerang uniformity of a class of power maps. *Designs, Codes, and Cryptography*, 89(11):2627–2636, November 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00944-x.

**Wu:2021:NPA**

[2738] Yanan Wu, Nian Li, and Xiangyong Zeng. New P$c$N and AP$c$N

functions over finite fields. *Designs, Codes, and Cryptography*, 89(11):2637–2651, November 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00946-9`.

**Monroe:2021:BSD**

[2739] Laura Monroe. Binary signed-digit integers and the Stern diatomic sequence. *Designs, Codes, and Cryptography*, 89(12):2653–2662, December 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00903-6`.

**Chai:2021:WSN**

[2740] Jinjin Chai, Zilong Wang, and Erzhong Xue. Walsh spectrum and nega spectrum of complementary arrays. *Designs, Codes, and Cryptography*, 89(12):2663–2677, December 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00938-9`.

**Pang:2021:FFN**

[2741] Binbin Pang, Shixin Zhu, and Xiaoshan Kai. Five families of the narrow-sense primitive BCH codes over finite fields. *Designs, Codes, and Cryptography*, 89(12):2679–2696, December 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00942-z`.

**Zhang:2021:TCB**

[2742] WeiGuo Zhang, YuJuan Sun, and Enes Pasalic. Three classes of balanced vectorial semi-bent functions. *Designs, Codes, and Cryptography*, 89(12):2697–2714, December 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00943-y`.

**Ahmadi:2021:NPC**

[2743] M. H. Ahmadi, N. Akhlaghinia, and S. Sadri. New partitionings of complete designs. *Designs, Codes, and Cryptography*, 89(12):2715–2723, December 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00950-z`.

**Bonvicini:2021:FFH**

[2744] Simona Bonvicini, Marco Buratti, and Tommaso Traetta. The first families of highly symmetric Kirkman Triple Systems whose orders fill a congruence class. *Designs, Codes, and Cryptography*, 89(12):2725–2757, December 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00952-x`.

**Kurz:2021:BFC**

[2745] Sascha Kurz. Bounds for flag codes. *Designs, Codes, and Cryptography*, 89(12):2759–2785, December 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/`

article/10.1007/s10623-021-00953-w.

**Ye:2021:IDE**

[2746] Chen-Dong Ye and Tian Tian. An improved degree evaluation method of NFSR-based cryptosystems. *Designs, Codes, and Cryptography*, 89(12):2787–2806, December 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00954-9.

**Li:2021:PFN**

[2747] Yiming Li, Shengli Liu, and Dawu Gu. Pseudorandom functions in NC class from the standard LWE assumption. *Designs, Codes, and Cryptography*, 89(12):2807–2839, December 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00955-8.

**Sharma:2021:EPN**

[2748] Hariom Sharma and R. K. Sharma. Existence of primitive normal pairs with one prescribed trace over finite fields. *Designs, Codes, and Cryptography*, 89(12):2841–2855, December 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00956-7.

**Esfahani:2021:SPA**

[2749] Navid Nasr Esfahani and Douglas R. Stinson. On security properties of all-or-nothing transforms. *Designs, Codes, and Cryptography*, 89(12):2857–2867, December 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00958-5.

**Tu:2021:BPF**

[2750] Ziran Tu, Xiangyong Zeng, and Yan Li. Binomial permutations over finite fields with even characteristic. *Designs, Codes, and Cryptography*, 89(12):2869–2888, December 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00959-4.

**Li:2022:NSC**

[2751] Nian Li, Zhao Hu, and Xiangyong Zeng. A note on "Cryptographically strong permutations from the butterfly structure". *Designs, Codes, and Cryptography*, 90(2):265–276, February 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00974-5. See [2654].

**Hara:2022:GTB**

[2752] Keisuke Hara, Takahiro Matsuda, and Keisuke Tanaka. Generic transformation from broadcast encryption to round-optimal deniable ring authentication. *Designs, Codes, and Cryptography*, 90(2):277–316, February 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00975-4.

**Gildea:2022:NBS**

[2753] Joe Gildea, Adrian Korban, and Adam Michael Roberts. New binary self-dual codes of lengths 80, 84 and 96 from composite matrices. *Designs, Codes, and Cryptography*, 90 (2):317–342, February 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00976-3.

**Biswas:2022:QCM**

[2754] Soumak Biswas and Maheshanand Bhaintwal. Quantum codes from $\mathbf{Z}_2\mathbf{Z}_2[u]/\langle u^4\rangle$-cyclic codes. *Designs, Codes, and Cryptography*, 90(2):343–366, February 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00978-1.

**Pan:2022:DMF**

[2755] Rong Pan, R. Julian R. Abel, and Xiaomiao Wang. Difference matrices with five rows over finite abelian groups. *Designs, Codes, and Cryptography*, 90 (2):367–386, February 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00981-6.

**Wang:2022:GMI**

[2756] Xiao-Juan Wang, Tian Tian, and Wen-Feng Qi. A generic method for investigating nonsingular Galois NFSRs. *Designs, Codes, and Cryptography*, 90 (2):387–408, February 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00982-5.

**Dougherty:2022:NGB**

[2757] Steven T. Dougherty. The neighbor graph of binary self-dual codes. *Designs, Codes, and Cryptography*, 90 (2):409–425, February 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00985-2.

**Fernandez:2022:SSP**

[2758] Marcel Fernandez and Jorge J. Urroz. A study of the separating property in Reed–Solomon codes by bounding the minimum distance. *Designs, Codes, and Cryptography*, 90 (2):427–442, February 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00988-z.

**Demirbas:2022:ICK**

[2759] Fatih Demirbas and Orhun Kara. Integral characteristics by keyspace partitioning. *Designs, Codes, and Cryptography*, 90(2):443–472, February 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00989-y.

**Dempwolff:2022:CCE**

[2760] Ulrich Dempwolff. Correction to: CCZ equivalence of power functions. *Designs, Codes, and Cryptography*, 90 (2):473–475, February 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https:

//link.springer.com/article/10.1007/s10623-021-00979-0. See [2211].

**Blokhuis:2022:CCL**

[2761] A. Blokhuis, M. De Boeck, and J. D'haeseleer. Correction to: Cameron–Liebler sets of $k$-spaces in PG$(n, q)$. *Designs, Codes, and Cryptography*, 90(2):477–487, February 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00983-4. See correction [2410].

**Dalai:2022:SBR**

[2762] Deepak Kumar Dalai, Santu Pal, and Santanu Sarkar. A state bit recovery algorithm with TMDTO attack on Lizard and Grain-128a. *Designs, Codes, and Cryptography*, 90 (3):489–521, March 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00984-3.

**Geil:2022:PDA**

[2763] Olav Geil. From primary to dual affine variety codes over the Klein quartic. *Designs, Codes, and Cryptography*, 90 (3):523–543, March 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00990-5.

**Xu:2022:RCP**

[2764] Xiaofang Xu, Xiangyong Zeng, and Shasha Zhang. Regular complete permutation polynomials over $\mathbf{F}_{2^n}$. *Designs, Codes, and Cryptography*, 90 (3):545–575, March 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00992-3.

**Liu:2022:EQH**

[2765] Jiang Liu, Qin Li, and Haozhen Situ. Efficient quantum homomorphic encryption scheme with flexible evaluators and its simulation. *Designs, Codes, and Cryptography*, 90 (3):577–591, March 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00993-2.

**Wiese:2022:MCD**

[2766] Moritz Wiese and Holger Boche. Mosaics of combinatorial designs for information-theoretic security. *Designs, Codes, and Cryptography*, 90 (3):593–632, March 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00994-1.

**DeBeule:2022:CLK**

[2767] Jan De Beule, Jonathan Mannaert, and Leo Storme. Cameron–Liebler $k$-sets in subspaces and non-existence conditions. *Designs, Codes, and Cryptography*, 90(3):633–651, March 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00995-0.

**Zhao:2022:TSC**

[2768] H. Zhao, Y. Wei, and N. Cepak. Two secondary constructions of bent func-

tions without initial conditions. *Designs, Codes, and Cryptography*, 90 (3):653–679, March 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00996-z`.

**Tan:2022:LCS**

[2769] Pan Tan, Cuiling Fan, and Wei Guo. Linear codes from support designs of ternary cyclic codes. *Designs, Codes, and Cryptography*, 90 (3):681–693, March 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-01001-3`.

**Lau:2022:DSL**

[2770] Terry Shue Chien Lau and Chik How Tan. On the design and security of Lee metric McEliece cryptosystems. *Designs, Codes, and Cryptography*, 90 (3):695–717, March 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-01002-2`.

**Yuan:2022:SRH**

[2771] Quan Yuan, Mehdi Tibouchi, and Masayuki Abe. On subset-resilient hash function families. *Designs, Codes, and Cryptography*, 90(3):719–758, March 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01008-4`.

**Rajput:2022:LQC**

[2772] Charul Rajput and Maheshanand Bhaintwal. On the locality of quasi-cyclic codes over finite fields. *Designs, Codes, and Cryptography*, 90 (3):759–777, March 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01009-3`.

**Jena:2022:GFL**

[2773] Dibyayoti Jena and Geertrui Van de Voorde. The geometric field of linearity of linear sets. *Designs, Codes, and Cryptography*, 90(3):779–799, March 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01011-9`.

**Koshelev:2022:IHO**

[2774] Dmitrii Koshelev. Indifferentiable hashing to ordinary elliptic $\mathbf{F}_q$-curves of $j = 0$ with the cost of one exponentiation in $\mathbf{F}_q$. *Designs, Codes, and Cryptography*, 90(3):801–812, March 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01012-8`.

**Zhao:2022:NOB**

[2775] Mengzhen Zhao, Cuiling Fan, and Zihong Tian. Nearly optimal balanced quaternary sequence pairs of prime period $N \equiv 5 \pmod 8$. *Designs, Codes, and Cryptography*, 90 (3):813–826, March 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01013-7`.

**Penttila:2022:UIP**

[2776] Tim Penttila. Uniqueness of the inversive plane of order sixty-four. *Designs, Codes, and Cryptography*, 90 (3):827–834, March 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01014-6`.

**Byrnes:2022:IML**

[2777] Kevin M. Byrnes. Isomorphism of maximum length circuit codes. *Designs, Codes, and Cryptography*, 90 (4):835–850, April 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-01005-z`.

**Lan:2022:COC**

[2778] Liantao Lan, Yanxun Chang, and Lidong Wang. The completion of optimal cyclic quaternary codes of weight 3 and distance 3. *Designs, Codes, and Cryptography*, 90 (4):851–862, April 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01006-6`.

**Zhao:2022:FTV**

[2779] Yanwei Zhao and Shenglin Zhou. Flag-transitive $2-(v,k,\lambda)$ designs with $r > \lambda(k-3)$. *Designs, Codes, and Cryptography*, 90(4):863–869, April 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01010-w`.

**Pawale:2022:NEQ**

[2780] Rajendra M. Pawale, Mohan S. Shrikhande, and Kusum S. Rajbhar. Non-existence of quasi-symmetric designs with restricted block graphs. *Designs, Codes, and Cryptography*, 90 (4):871–879, April 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01016-4`.

**Music:2022:DMS**

[2781] Luka Music, Céline Chevalier, and Elham Kashefi. Dispelling myths on superposition attacks: formal security model and attack analyses. *Designs, Codes, and Cryptography*, 90 (4):881–920, April 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01017-3`. See correction [2813].

**Zhao:2022:PAS**

[2782] Yi Zhao, Kaitai Liang, and Emmanouil Panaousis. Practical algorithm substitution attack on extractable signatures. *Designs, Codes, and Cryptography*, 90 (4):921–937, April 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01019-1`.

**Barg:2022:CMR**

[2783] Alexander Barg, Zitan Chen, and Itzhak Tamo. A construction of maximally recoverable codes. *Designs, Codes, and Cryptography*, 90 (4):939–945, April 2022. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01020-8.

**Kawabata:2022:NTL**

[2784] Daiki Kawabata and Tatsuya Maruta. On the nonexistence of ternary linear codes attaining the Griesmer bound. *Designs, Codes, and Cryptography*, 90 (4):947–956, April 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01021-7.

**Santonastaso:2022:LDR**

[2785] Paolo Santonastaso and Ferdinando Zullo. On the list decodability of rank-metric codes containing Gabidulin codes. *Designs, Codes, and Cryptography*, 90(4):957–982, April 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01022-6.

**Dunkelman:2022:PKR**

[2786] Orr Dunkelman, Maria Eichlseder, and Markus Schofnegger. Practical key recovery attacks on FlexAEAD. *Designs, Codes, and Cryptography*, 90 (4):983–1007, April 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01023-5.

**Beierle:2022:TEQ**

[2787] Christof Beierle, Gregor Leander, and Léo Perrin. Trims and extensions of quadratic APN functions. *Designs, Codes, and Cryptography*, 90 (4):1009–1036, April 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01024-4.

**Bhunia:2022:LCM**

[2788] Dipak K. Bhunia, Cristina Fernández-Córdoba, and Mercè Villanueva. On the linearity and classification of $\mathbf{Z}_{p^s}$-linear generalized Hadamard codes. *Designs, Codes, and Cryptography*, 90 (4):1037–1058, April 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01026-2.

**Alawatugoda:2022:SML**

[2789] Janaka Alawatugoda and Tatsuaki Okamoto. Standard model leakage-resilient authenticated key exchange using inner-product extractors. *Designs, Codes, and Cryptography*, 90 (4):1059–1079, April 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01028-0.

**Anbar:2022:BP**

[2790] Nurdagül Anbar and Wilfried Meidl. Bent partitions. *Designs, Codes, and Cryptography*, 90(4):1081–1101, April 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01029-z.

**Galindo:2022:GCQ**

[2791] Carlos Galindo and Fernando Hernando. On the generalization of the construction of quantum codes from

Hermitian self-orthogonal codes. *Designs, Codes, and Cryptography*, 90 (5):1103–1112, May 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01018-2`.

**Zhu:2022:CEB**

[2792] Hongwei Zhu, Minjia Shi, and Ferruh Özbudak. Complete $b$-symbol weight distribution of some irreducible cyclic codes. *Designs, Codes, and Cryptography*, 90(5):1113–1125, May 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01030-6`.

**Ong:2022:ECD**

[2793] Kai Lin Ong and Miin Huey Ang. On equivalence of cyclic and dihedral zero-divisor codes having nilpotents of nilpotency degree two as generators. *Designs, Codes, and Cryptography*, 90 (5):1127–1138, May 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01025-3`.

**Zhang:2022:POS**

[2794] WeiGuo Zhang, Enes Pasalic, and Liu-Piao Zhang. Phase orthogonal sequence sets for (QS)CDMA communications. *Designs, Codes, and Cryptography*, 90 (5):1139–1156, May 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01031-5`.

**Luo:2022:ABS**

[2795] Fucai Luo and Saif Al-Kuwari. Attribute-based signatures from lattices: unbounded attributes and semi-adaptive security. *Designs, Codes, and Cryptography*, 90(5):1157–1177, May 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01027-1`.

**Lu:2022:SBM**

[2796] Zhenyu Lu, Sihem Mesnager, and Meiqin Wang. An STP-based model toward designing S-boxes with good cryptographic properties. *Designs, Codes, and Cryptography*, 90(5):1179–1202, May 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01034-2`.

**Lazebnik:2022:PCH**

[2797] Felix Lazebnik and Lorinda Leshock. On Pappus configurations in Hall planes. *Designs, Codes, and Cryptography*, 90(5):1203–1219, May 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01036-0`.

**Zhang:2022:CTD**

[2798] Hui Zhang, Cuiling Fan, and Sihem Mesnager. Constructions of two-dimensional Z-complementary array pairs with large ZCZ ratio. *Designs, Codes, and Cryptography*, 90 (5):1221–1239, May 2022. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01035-1.

**Aydin:2022:PCA**

[2799] Nuh Aydin, Peihan Liu, and Bryan Yoshino. Polycyclic codes associated with trinomials: good codes and open questions. *Designs, Codes, and Cryptography*, 90(5):1241–1269, May 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01038-y.

**Luo:2022:AOE**

[2800] Gaojun Luo and San Ling. Application of optimal $p$-ary linear codes to alphabet-optimal locally repairable codes. *Designs, Codes, and Cryptography*, 90(5):1271–1287, May 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01040-4.

**Zhang:2022:MBL**

[2801] Fengrong Zhang, Enes Pasalic, and Yongzhuang Wei. Minimal binary linear codes: a general framework based on bent concatenation. *Designs, Codes, and Cryptography*, 90(5):1289–1318, May 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01037-z.

**Xiang:2022:IFA**

[2802] Can Xiang, Chunming Tang, and Qi Liu. An infinite family of antiprimitive cyclic codes supporting Steiner systems $S(3, 8, 7^m + 1)$. *Designs, Codes, and Cryptography*, 90(6):1319–1333, June 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01032-4.

**Kiermaier:2022:PAF**

[2803] Michael Kiermaier. On $\alpha$-points of $q$-analogs of the Fano plane. *Designs, Codes, and Cryptography*, 90(6):1335–1345, June 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01033-3.

**Dose:2022:HOE**

[2804] Valerio Dose, Pietro Mercuri, and Claudio Stirpe. High order elements in finite fields arising from recursive towers. *Designs, Codes, and Cryptography*, 90(6):1347–1368, June 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01041-3.

**Senel:2022:AGA**

[2805] Engin Senel and Figen Öke. On the automorphisms of generalized algebraic geometry codes. *Designs, Codes, and Cryptography*, 90(6):1369–1379, June 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01043-1.

**Bhattacharjee:2022:MCB**

[2806] Arghya Bhattacharjee, Avijit Dutta, and Mridul Nandi. CENCPP$^*$:

beyond-birthday-secure encryption from public permutations. *Designs, Codes, and Cryptography*, 90(6):1381–1425, June 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01045-z.

**Dukes:2022:OSG**

[2807] Austin Dukes, Andrea Ferraguti, and Giacomo Micheli. Optimal selection for good polynomials of degree up to five. *Designs, Codes, and Cryptography*, 90(6):1427–1436, June 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01046-y.

**Kim:2022:PQB**

[2808] Kwang Ho Kim, Sihem Mesnager, and Myong Chol Jo. On permutation quadrinomials with boomerang uniformity 4 and the best-known nonlinearity. *Designs, Codes, and Cryptography*, 90(6):1437–1461, June 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01047-x.

**Wen:2022:SBF**

[2809] Jinming Wen and Xiao-Wen Chang. Sharper bounds on four lattice constants. *Designs, Codes, and Cryptography*, 90(6):1463–1484, June 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01048-w.

**Miezaki:2022:NAM**

[2810] Tsuyoshi Miezaki and Hiroyuki Nakasora. A note on the Assmus–Mattson theorem for some binary codes. *Designs, Codes, and Cryptography*, 90(6):1485–1502, June 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01050-2.

**Aguglia:2022:SHF**

[2811] Angela Aguglia, Michela Ceria, and Luca Giuzzi. Some hypersurfaces over finite fields, minimal codes and secret sharing schemes. *Designs, Codes, and Cryptography*, 90(6):1503–1519, June 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01051-1.

**Crnkovic:2022:NTC**

[2812] Dean Crnković, Daniel R. Hawtin, and Andrea Svob. Neighbour-transitive codes and partial spreads in generalised quadrangles. *Designs, Codes, and Cryptography*, 90(6):1521–1533, June 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01053-z.

**Music:2022:CDM**

[2813] Luka Music, Céline Chevalier, and Elham Kashefi. Correction to: Dispelling myths on superposition attacks: formal security model and attack analyses. *Designs, Codes, and Cryptography*, 90(6):1535, June 2022. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01042-2. See [2781].

**Kim:2022:CWP**

[2814] Hyun Kwang Kim and Jieun Kwon. Classification of weighted posets and digraphs admitting the extended Hamming code to be a perfect code. *Designs, Codes, and Cryptography*, 90(10):2249–2269, October 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01066-8.

**Abe:2022:BKG**

[2815] Masayuki Abe and Miguel Ambrona. Blind key-generation attribute-based encryption for general predicates. *Designs, Codes, and Cryptography*, 90(10):2271–2299, October 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01069-5.

**Agrawal:2022:CBA**

[2816] Shweta Agrawal, Rajarshi Biswas, Ryo Nishimaki, Keita Xagawa, Xiang Xie, and Shota Yamada. Cryptanalysis of Boyen's attribute-based encryption scheme in TCC 2013. *Designs, Codes, and Cryptography*, 90(10):2301–2318, October 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01076-6.

**Alhakim:2022:DPF**

[2817] Abbas Alhakim. Designing preference functions for de Bruijn sequences with forbidden words. *Designs, Codes, and Cryptography*, 90(10):2319–2335, October 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01077-5.

**Ma:2022:CMS**

[2818] Junru Ma and Jinquan Luo. Constructions of MDS symbol-pair codes with minimum distance seven or eight. *Designs, Codes, and Cryptography*, 90(10):2337–2359, October 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01081-9.

**Eyvazi:2022:LCG**

[2819] Hamidreza Eyvazi, Karim Samei, and Batoul Savari. The linearity of Carlet's Gray image of linear codes over $\mathbf{Z}_8$. *Designs, Codes, and Cryptography*, 90(10):2361–2373, October 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01084-6.

**Horsley:2022:BAP**

[2820] Daniel Horsley and Padraig Ó Catháin. Block avoiding point sequencings of partial Steiner systems. *Designs, Codes, and Cryptography*, 90(10):2375–2383, October 2022. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01085-5.

**Yan:2022:DSP**

[2821] Haode Yan and Kun Zhang. On the $c$-differential spectrum of power functions over finite fields. *Designs, Codes, and Cryptography*, 90(10):2385–2405, October 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01086-4.

**Cakiroglu:2022:NIP**

[2822] Yagmur Çakiroglu, Oguz Yayla, and Emrah Sercan Yilmaz. The number of irreducible polynomials over finite fields with vanishing trace and reciprocal trace. *Designs, Codes, and Cryptography*, 90(10):2407–2417, October 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01088-2.

**Liu:2022:IKR**

[2823] Jun Liu, Dachao Wang, Yupu Hu, Jie Chen, and Baocang Wang. Improved key-recovery attacks on reduced-round WEM-8. *Designs, Codes, and Cryptography*, 90(10):2419–2448, October 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01089-1.

**Zhou:2022:EES**

[2824] Zhaocun Zhou, Dengguo Feng, and Bin Zhang. Efficient and extensive search for precise linear approximations with high correlations of full SNOW-V. *Designs, Codes, and Cryptography*, 90(10):2449–2479, October 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01090-8.

**Janusz:2022:CPP**

[2825] Gerald J. Janusz. Covering polynomials and projections of self-dual codes. *Designs, Codes, and Cryptography*, 90(10):2481–2489, October 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01091-7.

**Ji:2022:CCS**

[2826] Lijun Ji, Miao Liang, and Yanting Wang. Combinational constructions of splitting authentication codes with perfect secrecy. *Designs, Codes, and Cryptography*, 90(10):2491–2515, October 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01092-6.

**Huffman:2022:GEC**

[2827] W. Cary Huffman, Jon-Lark Kim, and Patrick Solé. Guest editorial: On coding theory and combinatorics — in memory of Vera Pless. *Designs, Codes, and Cryptography*, 90(11):2517–2527, November 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01126-z.

**Gao:2022:WDD**

[2828] Jian Gao, Xiangrui Meng, and Fang-Wei Fu. Weight distribution of double cyclic codes over Galois rings. *Designs, Codes, and Cryptography*, 90(11):2529–2549, November 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00914-3.

**Wu:2022:MZZ**

[2829] Rongsheng Wu and Minjia Shi. On $\mathbf{Z}_2\mathbf{Z}_4$-additive polycyclic codes and their Gray images. *Designs, Codes, and Cryptography*, 90(11):2551–2562, November 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00917-0.

**Martinez:2022:SFS**

[2830] Federico N. Martínez. Symmetric functions and spherical $t$-designs in $\pm\mathbf{R}^2$. *Designs, Codes, and Cryptography*, 90(11):2563–2581, November 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00922-3.

**Chakraborty:2022:VJP**

[2831] Himadri Shekhar Chakraborty and Tsuyoshi Miezaki. Variants of Jacobi polynomials in coding theory. *Designs, Codes, and Cryptography*, 90(11):2583–2597, November 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00923-2.

**Shi:2022:QRC**

[2832] Minjia Shi, Shukai Wang, Tor Helleseth, and Patrick Solé. Quadratic residue codes, rank three groups and PBIBDs. *Designs, Codes, and Cryptography*, 90(11):2599–2611, November 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00918-z.

**Qin:2022:CDP**

[2833] Rongcun Qin, Hengming Zhao, and Huangsheng Yu. Compatible difference packing set systems and their applications to multilength variable-weight OOCs. *Designs, Codes, and Cryptography*, 90(11):2613–2645, November 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00927-y.

**Borello:2022:CSQ**

[2834] Martino Borello, Cem Güneri, Elif Saçıkara, and Patrick Solé. The concatenated structure of quasi-abelian codes. *Designs, Codes, and Cryptography*, 90(11):2647–2661, November 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00921-4.

**Qian:2022:NMC**

[2835] Liqin Qian, Xiwang Cao, Wei Lu, and Patrick Solé. A new method for constructing linear codes with small hulls. *Designs, Codes, and Cryptography*, 90(11):2663–2682,

November 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00940-1.

**Dyshko:2022:MEP**

[2836] Serhii Dyshko and Jay A. Wood. MacWilliams extension property for arbitrary weights on linear codes over module alphabets. *Designs, Codes, and Cryptography*, 90(11):2683–2701, November 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00945-w.

**Fu:2022:GSO**

[2837] Yuqing Fu and Hongwei Liu. Galois self-orthogonal constacyclic codes over finite fields. *Designs, Codes, and Cryptography*, 90(11):2703–2733, November 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00957-6.

**Choi:2022:IUB**

[2838] Whan Hyuk Choi and Jon Lark Kim. An improved upper bound on self-dual codes over finite fields GF(11), GF(19), and GF(23). *Designs, Codes, and Cryptography*, 90(11):2735–2751, November 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00968-3.

**Tonchev:2022:PSC**

[2839] Vladimir D. Tonchev. On Pless symmetry codes, ternary QR codes, and related Hadamard matrices and designs. *Designs, Codes, and Cryptography*, 90(11):2753–2762, November 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00941-0.

**Patel:2022:TDT**

[2840] Shikha Patel and Om Prakash. $(\theta, \delta_\theta)$-cyclic codes over $\mathbf{F}_q[u,v]/\langle u^2 - u, v^2 - v, uv - vu\rangle$. *Designs, Codes, and Cryptography*, 90(11):2763–2781, November 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00964-7.

**Ballet:2022:CAC**

[2841] Stéphane Ballet, Nicolas Baudru, Alexis Bonnecaze, and Mila Tukumuli. Construction of asymmetric Chudnovsky-type algorithms for multiplication in finite fields. *Designs, Codes, and Cryptography*, 90(12):2783–2811, December 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00986-1.

**Wu:2022:FII**

[2842] Yansheng Wu, Yoonjin Lee, and Qiang Wang. Further improvement on index bounds. *Designs, Codes, and Cryptography*, 90(12):2813–2821, December 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-00987-0.

**Sok:2022:NCL**

[2843] Lin Sok. A new construction of linear codes with one-dimensional hull. *Designs, Codes, and Cryptography*, 90(12):2823–2839, December 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00991-4`.

**Jafari:2022:EPG**

[2844] Fatemeh Jafari, Alireza Abdollahi, Javad Bagherian, Maryam Khatami, and Reza Sobhani. Equidistant permutation group codes. *Designs, Codes, and Cryptography*, 90(12):2841–2859, December 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00997-y`.

**Ayebie:2022:NCB**

[2845] Edoukou Berenger Ayebie and El Mamoun Souidi. New code-based cryptographic accumulator and fully dynamic group signature. *Designs, Codes, and Cryptography*, 90(12):2861–2891, December 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01007-5`.

**Takahashi:2022:DAM**

[2846] Hokuto Takahashi and Manabu Hagiwara. Decoding algorithms of monotone codes and azinv codes and their unified view. *Designs, Codes, and Cryptography*, 90(12):2893–2922, December 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-01004-0`.

**Duursma:2022:JGC**

[2847] Iwan Duursma and Xiao Li. Johnson graph codes. *Designs, Codes, and Cryptography*, 90(12):2923–2941, December 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-01003-1`.

**Bariffi:2022:MDP**

[2848] Jessica Bariffi, Sam Mattheus, Alessandro Neri, and Joachim Rosenthal. Moderate-density parity-check codes from projective bundles. *Designs, Codes, and Cryptography*, 90(12):2943–2966, December 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01054-y`.

**Kim:2022:SPC**

[2849] Jon-Lark Kim and JunYong Park. Steganography from perfect codes on Cayley graphs over Gaussian integers, Eisenstein–Jacobi integers and Lipschitz integers. *Designs, Codes, and Cryptography*, 90(12):2967–2989, December 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01063-x`.

**He:2022:PSC**

[2850] Xianmang He, Yindong Chen, Zusheng Zhang, and Kunxiao Zhou. Parallel sub-code construction for constant-dimension codes. *Designs, Codes,*

*and Cryptography*, 90(12):2991–3001, December 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01065-9`.

**Alahmadi:2022:BCC**

[2851] Adel Alahmadi, Amani Alkathiry, Alaa Altassan, Alexis Bonnecaze, Hatoon Shoaib, and Patrick Solé. The build-up construction over a commutative non-unital ring. *Designs, Codes, and Cryptography*, 90(12):3003–3010, December 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01044-0`.

**Bettaieb:2022:GCB**

[2852] Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Yann Connan, and Philippe Gaborit. A gapless code-based hash proof system based on RQC and its applications. *Designs, Codes, and Cryptography*, 90(12):3011–3044, December 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01075-7`.

**Ozbudak:2022:CPP**

[2853] Ferruh Özbudak and Burcu Gülmez Temür. Classification of permutation polynomials of the form $x^3 g(x^{q-1})$ of $\mathbf{F}_{q^2}$ where $g(x) = x^3 + bx + c$ and $b, c \in \mathbf{F}_q^*$. *Designs, Codes, and Cryptography*, 90(7):1537–1556, July 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01052-0`.

**Ball:2022:ELC**

[2854] Simeon Ball and James Dixon. The equivalence of linear codes implies semi-linear equivalence. *Designs, Codes, and Cryptography*, 90(7):1557–1565, July 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01055-x`.

**vanTrung:2022:MCR**

[2855] Tran van Trung. A method of constructing 2-resolvable $t$-designs for $t = 3, 4$. *Designs, Codes, and Cryptography*, 90(7):1567–1583, July 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01056-w`.

**Crnkovic:2022:SD**

[2856] Dean Crnković and Andrea Svob. Switching for 2-designs. *Designs, Codes, and Cryptography*, 90(7):1585–1593, July 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01059-7`.

**Tonchev:2022:BRD**

[2857] Vladimir D. Tonchev. Book review: *Designs from Linear Codes*, second edition, by Cunsheng Ding and Chunming Tang, World Scientific, 2022. *Designs, Codes, and Cryptography*, 90(7):1595–1597, July 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01058-8`.

**Bao:2022:LSD**

[2858] Jingjun Bao and Lijun Ji. Large sets of $t$-designs over finite fields exist for all $t$. *Designs, Codes, and Cryptography*, 90(7):1599–1609, July 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01061-z`.

**Zhang:2022:ECE**

[2859] Menglong Zhang, Tao Feng, and Xiaomiao Wang. The existence of cyclic $(v, 4, 1)$-designs. *Designs, Codes, and Cryptography*, 90(7):1611–1628, July 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01057-9`.

**Li:2022:NBI**

[2860] Xia Li and Qin Yue. Non-binary irreducible quasi-cyclic parity-check subcodes of Goppa codes and extended Goppa codes. *Designs, Codes, and Cryptography*, 90(7):1629–1647, July 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01062-y`.

**Zhang:2022:CTG**

[2861] Jun Zhang, Zhengchun Zhou, and Chunming Tang. A class of twisted generalized Reed–Solomon codes. *Designs, Codes, and Cryptography*, 90(7):1649–1658, July 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01064-w`.

**Bereg:2022:UPR**

[2862] Sergey Bereg, Brian Malouf, Linda Morales, Thomas Stanley, and I. Hal Sudborough. Using permutation rational functions to obtain permutation arrays with large Hamming distance. *Designs, Codes, and Cryptography*, 90(7):1659–1677, July 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01039-x`.

**Korban:2022:RGC**

[2863] Adrian Korban, Serap Sahinkaya, and Deniz Ustun. Reversible $G^k$-codes with applications to DNA codes. *Designs, Codes, and Cryptography*, 90(7):1679–1694, July 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01067-7`.

**Wang:2022:LCM**

[2864] Yan Wang, Xilin Han, Weiqiong Wang, and Ziling Heng. Linear complexity over $\mathbf{F}_q$ and 2-adic complexity of a class of binary generalized cyclotomic sequences with good autocorrelation. *Designs, Codes, and Cryptography*, 90(8):1695–1712, August 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01068-6`.

**Romanov:2022:NEQ**

[2865] Alexander M. Romanov. On the number of $q$ -ary quasi-perfect codes with covering radius 2. *Designs, Codes, and Cryptography*, 90(8):1713–1719, August 2022. CODEN DC-

CREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01070-y.

**Bibak:2022:MSS**

[2866] Khodakhast Bibak and Behrouz Zolfaghari. The Modular Subset-Sum Problem and the size of deletion correcting codes. *Designs, Codes, and Cryptography*, 90(8):1721–1734, August 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01073-9.

**Cheon:2022:ACD**

[2867] Jung Hee Cheon, Wonhee Cho, Jeong Han Kim, and Jiseung Kim. Adventures in crypto dark matter: attacks, fixes and analysis for weak pseudorandom functions. *Designs, Codes, and Cryptography*, 90(8):1735–1760, August 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01071-x.

**Mashahdi:2022:NIP**

[2868] Samaneh Mashahdi, Bagher Bagherpour, and Ali Zaghian. A non-interactive $(t, n)$-publicly verifiable multi-secret sharing scheme. *Designs, Codes, and Cryptography*, 90(8):1761–1782, August 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01082-8.

**Kudin:2022:CCM**

[2869] Sadmir Kudin and Enes Pasalic. A complete characterization of $\mathcal{D}_\prime \cap \mathcal{M}^\#$ and a general framework for specifying bent functions in $\mathcal{C}$ outside $\mathcal{M}^\#$. *Designs, Codes, and Cryptography*, 90(8):1783–1796, August 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01079-3.

**Azimi:2022:BVD**

[2870] Seyyed Arash Azimi, Adrián Ranea, Mahmoud Salmasizadeh, Javad Mohajeri, Mohammad Reza Aref, and Vincent Rijmen. A bit-vector differential model for the modular addition by a constant and its applications to differential and impossible-differential cryptanalysis. *Designs, Codes, and Cryptography*, 90(8):1797–1855, August 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01074-8.

**Wang:2022:GOC**

[2871] Lidong Wang, Lulu Cai, Tao Feng, Zihong Tian, and Xiaomiao Wang. Geometric orthogonal codes and geometrical difference packings. *Designs, Codes, and Cryptography*, 90(8):1857–1879, August 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01078-4.

**Abreu:2022:SRC**

[2872] Marién Abreu, Martin Funk, Vedran Krčadinac, and Domenico Labbate.

Strongly regular configurations. *Designs, Codes, and Cryptography*, 90 (8):1881–1897, August 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01080-w`.

**Boudgoust:2022:VMR**

[2873] Katharina Boudgoust, Amin Sakzad, and Ron Steinfeld. Vandermonde meets Regev: public key encryption schemes based on partial Vandermonde problems. *Designs, Codes, and Cryptography*, 90(8):1899–1936, August 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01083-7`.

**Sui:2022:MNM**

[2874] Junzhen Sui, Xiaomeng Zhu, and Xueying Shi. MDS and near-MDS codes via twisted Reed–Solomon codes. *Designs, Codes, and Cryptography*, 90 (8):1937–1958, August 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01049-9`.

**Ball:2022:CAB**

[2875] Simeon Ball, Michel Lavrauw, and Tamás Szőnyi. Contributions by Aart Blokhuis to finite geometry, discrete mathematics, and combinatorics. *Designs, Codes, and Cryptography*, 90(9): 1959–1961, September 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01072-w`.

**DeBruyn:2022:CCC**

[2876] B. De Bruyn and M. Gao. A characterization of the Coxeter cap. *Designs, Codes, and Cryptography*, 90(9): 1963–1981, September 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00855-x`.

**Haemers:2022:SSC**

[2877] Willem H. Haemers and Leila Parsaei Majd. Spectral symmetry in conference matrices. *Designs, Codes, and Cryptography*, 90(9):1983–1990, September 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00858-8`.

**Janzer:2022:CLH**

[2878] Oliver Janzer and Zoltán Lóránt Nagy. Coloring linear hypergraphs: the Erdős–Faber–Lovász conjecture and the Combinatorial Nullstellensatz. *Designs, Codes, and Cryptography*, 90(9): 1991–2001, September 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00859-7`.

**Abiad:2022:NGF**

[2879] Aida Abiad, Bart De Bruyn, Jozefien D'haeseleer, and Jack H. Koolen. Neumaier graphs with few eigenvalues. *Designs, Codes, and Cryptography*, 90(9): 2003–2019, September 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00856-w`.

**Lavrauw:2022:CIN**

[2880] Michel Lavrauw, Tomasz Popiel, and John Sheekey. Combinatorial invariants for nets of conics in PG$(2, q)$. *Designs, Codes, and Cryptography*, 90(9): 2021–2067, September 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00881-9`.

**Bailey:2022:DGA**

[2881] R. A. Bailey, Peter J. Cameron, Michael Kinyon, and Cheryl E. Praeger. Diagonal groups and arcs over groups. *Designs, Codes, and Cryptography*, 90(9):2069–2080, September 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00907-2`.

**Longobardi:2022:SST**

[2882] Giovanni Longobardi, Leo Storme, and Rocco Trombetti. On sets of subspaces with two intersection dimensions and a geometrical junta bound. *Designs, Codes, and Cryptography*, 90(9): 2081–2099, September 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00931-2`.

**Blokhuis:2022:SBE**

[2883] A. Blokhuis, M. De Boeck, and J. D'haeseleer. On the sunflower bound for $k$-spaces, pairwise intersecting in a point. *Designs, Codes, and Cryptography*, 90(9):2101–2111, September 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00949-6`.

**Denaux:2022:CSS**

[2884] Lins Denaux. Constructing saturating sets in projective spaces using subgeometries. *Designs, Codes, and Cryptography*, 90(9):2113–2144, September 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00951-y`.

**Kantor:2022:ASD**

[2885] William M. Kantor. Automorphism subgroups for designs with $\lambda = 1$. *Designs, Codes, and Cryptography*, 90(9): 2145–2157, September 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00936-x`.

**Betten:2022:EPC**

[2886] Anton Betten and Fatma Karaoglu. The Eckardt point configuration of cubic surfaces revisited. *Designs, Codes, and Cryptography*, 90(9):2159–2180, September 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00999-w`.

**Tan:2022:AUD**

[2887] Xinyu Tan, Narayanan Rengaswamy, and Robert Calderbank. Approximate unitary 3-designs from transvection Markov chains. *Designs, Codes, and Cryptography*, 90(9):2181–2204, September 2022. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-021-01000-4.

**Amarra:2022:DDP**

[2888] Carmen Amarra, Alice Devillers, and Cheryl E. Praeger. Delandtsheer–Doyen parameters for block-transitive point-imprimitive 2-designs. *Designs, Codes, and Cryptography*, 90(9):2205–2221, September 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01015-5.

**Blokhuis:2022:ECL**

[2889] Aart Blokhuis, Ruud Pellikaan, and Tamás Szőnyi. The extended coset leader weight enumerator of a twisted cubic code. *Designs, Codes, and Cryptography*, 90(9):2223–2247, September 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01060-0.

**Kolsch:2023:ISP**

[2890] Lukas Kölsch, Björn Kriepke, and Gohar M. Kyureghyan. Image sets of perfectly nonlinear maps. *Designs, Codes, and Cryptography*, 91 (1):1–27, January 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01094-4.

**Zhang:2023:CLC**

[2891] He Zhang and Chunming Tang. Constructions of large cyclic constant dimension codes via Sidon spaces. *Designs, Codes, and Cryptography*, 91 (1):29–44, January 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01095-3.

**Kharaghani:2023:COC**

[2892] Hadi Kharaghani, Sho Suda, and Vlad Zaitsev. On a class of optimal constant weight ternary codes. *Designs, Codes, and Cryptography*, 91 (1):45–54, January 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01096-2.

**Khaefi:2023:SPC**

[2893] Yasamin Khaefi, Zeinab Akhlaghi, and Behrooz Khosravi. On the subgroup perfect codes in Cayley graphs. *Designs, Codes, and Cryptography*, 91 (1):55–61, January 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01098-0.

**Gadouleau:2023:BFP**

[2894] Maximilien Gadouleau, Luca Mariot, and Stjepan Picek. Bent functions in the partial spread class generated by linear recurring sequences. *Designs, Codes, and Cryptography*, 91 (1):63–82, January 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01097-1.

**Tan:2023:MLL**

[2895] Pan Tan, Cuiling Fan, Cunsheng Ding, Chunming Tang, and Zhengchun Zhou.

The minimum locality of linear codes. *Designs, Codes, and Cryptography*, 91 (1):83–114, January 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01099-z`.

**Aguirre:2023:APN**

[2896] Josimar J. R. Aguirre, Cícero Carvalho, and Victor G. L. Neumann. About $r$-primitive and $k$-normal elements in finite fields. *Designs, Codes, and Cryptography*, 91(1):115–126, January 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01101-8`.

**Wang:2023:NRV**

[2897] Jiaxin Wang and Fang-Wei Fu. New results on vectorial dual-bent functions and partial difference sets. *Designs, Codes, and Cryptography*, 91 (1):127–149, January 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01103-6`.

**Carlet:2023:SCB**

[2898] Claude Carlet, Rebeka Kiss, and Gábor P. Nagy. Simplicity conditions for binary orthogonal arrays. *Designs, Codes, and Cryptography*, 91 (1):151–163, January 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01105-4`.

**Venema:2023:SCP**

[2899] Marloes Venema, Greg Alpár, and Jaap-Henk Hoepman. Systematizing core properties of pairing-based attribute-based encryption to uncover remaining challenges in enforcing access control in practice. *Designs, Codes, and Cryptography*, 91(1):165–220, January 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01093-5`.

**Li:2023:PCC**

[2900] Ming Li, Yupeng Jiang, and Dongdai Lin. Properties of the cycles that contain all vectors of weight $\leq k$. *Designs, Codes, and Cryptography*, 91 (1):221–239, January 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01100-9`.

**Caruso:2023:DLR**

[2901] Xavier Caruso and Amaury Durand. Duals of linearized Reed–Solomon codes. *Designs, Codes, and Cryptography*, 91(1):241–271, January 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01102-7`.

**Shi:2023:ACD**

[2902] Minjia Shi, Na Liu, Jon-Lark Kim, and Patrick Solé. Additive complementary dual codes over $\mathbf{F}_4$. *Designs, Codes, and Cryptography*, 91 (1):273–284, January 2023. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01106-3.

**Jiang:2023:RBS**

[2903] Yupeng Jiang. A relation between sequences generated by Golomb's preference algorithm. *Designs, Codes, and Cryptography*, 91(1):285–291, January 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01108-1.

**Lavorante:2023:NHH**

[2904] Vincenzo Pallozzi Lavorante and Valentino Smaldore. New hemisystems of the Hermitian surface. *Designs, Codes, and Cryptography*, 91(1):293–307, January 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01107-2.

**Xie:2023:SCB**

[2905] Xi Xie, Nian Li, Xiangyong Zeng, Xiaohu Tang, and Yao Yao. Several classes of bent functions over finite fields. *Designs, Codes, and Cryptography*, 91(2):309–332, February 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01109-0.

**Armario:2023:BFP**

[2906] José Andrés Armario, Ivan Bailera, and Ronan Egan. Butson full propelinear codes. *Designs, Codes, and Cryptography*, 91(2):333–351, February 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01110-7.

**Shen:2023:NCZ**

[2907] Bingsheng Shen, Hua Meng, Yang Yang, and Zhengchun Zhou. New constructions of $Z$-complementary code sets and mutually orthogonal complementary sequence sets. *Designs, Codes, and Cryptography*, 91(2):353–371, February 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01112-5.

**Zhang:2023:DFA**

[2908] WeiGuo Zhang, Enes Pasalic, Yiran Liu, Liupiao Zhang, and Chunlei Xie. A design and flexible assignment of orthogonal binary sequence sets for (QS)-CDMA systems. *Designs, Codes, and Cryptography*, 91(2):373–389, February 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01113-4.

**Katsumata:2023:DCB**

[2909] Shuichi Katsumata, Toi Tomita, and Shota Yamada. Direct computation of branching programs and its applications to more efficient lattice-based cryptography. *Designs, Codes, and Cryptography*, 91(2):391–431, February 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01104-5.

**Beierle:2023:GFS**

[2910] Christof Beierle and Claude Carlet. Gold functions and switched cube functions are not 0-extendable in dimension $n > 5$. *Designs, Codes, and Cryptography*, 91(2):433–449, February 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01111-6`.

**Byrne:2023:CNM**

[2911] Eimear Byrne, Michela Ceria, Sorina Ionica, Relinde Jurrius, and Elif Saçıkara. Constructions of new matroids and designs over $\mathbf{F}_q$. *Designs, Codes, and Cryptography*, 91 (2):451–473, February 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01087-3`.

**Hong:2023:IGB**

[2912] Xiaoqin Hong and Xiwang Cao. Improved generalized block inserting construction of constant dimension codes. *Designs, Codes, and Cryptography*, 91 (2):475–495, February 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01117-0`.

**Bidoux:2023:CBS**

[2913] Loïc Bidoux, Philippe Gaborit, Mukul Kulkarni, and Victor Mateu. Code-based signatures from new proofs of knowledge for the syndrome decoding problem. *Designs, Codes, and Cryptography*, 91(2):497–544, February 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01114-3`.

**Anbar:2023:GSS**

[2914] Nurdagül Anbar, Tekgül Kalayci, and Wilfried Meidl. Generalized semifield spreads. *Designs, Codes, and Cryptography*, 91(2):545–562, February 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01115-2`.

**Feneuil:2023:SPS**

[2915] Thibauld Feneuil, Antoine Joux, and Matthieu Rivain. Shared permutation for syndrome decoding: new zero-knowledge protocol and code-based signature. *Designs, Codes, and Cryptography*, 91(2):563–608, February 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01116-1`.

**Doulgerakis:2023:IVL**

[2916] Emmanouil Doulgerakis, Thijs Laarhoven, and Benne de Weger. The irreducible vectors of a lattice: Some theory and applications. *Designs, Codes, and Cryptography*, 91(2):609–643, February 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01119-y`.

**Kiermaier:2023:SWR**

[2917] Michael Kiermaier, Sascha Kurz, Patrick Solé, Michael Stoll, and Alfred Wassermann. On strongly walk regular graphs, triple sum sets and their codes. *Designs, Codes, and Cryptography*, 91 (2):645–675, February 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01118-z`.

**Shi:2023:SOC**

[2918] Minjia Shi, Shukai Wang, Jon-Lark Kim, and Patrick Solé. Self-orthogonal codes over a non-unital ring and combinatorial matrices. *Designs, Codes, and Cryptography*, 91(2):677–689, February 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00948-7`. See correction [2919].

**Shi:2023:CSO**

[2919] Minjia Shi, Shukai Wang, Jon-Lark Kim, and Patrick Solé. Correction: Self-orthogonal codes over a non-unital ring and combinatorial matrices. *Designs, Codes, and Cryptography*, 91 (2):691, February 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01170-9`. See [2918].

**Shi:2023:RAM**

[2920] Minjia Shi, Shukai Wang, and Xiaoxiao Li. Retracted Article: $\mathbf{Z}_p\mathbf{Z}_{p^2}$-linear codes: rank and kernel. *Designs, Codes, and Cryptography*, 91 (2):693, February 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00947-8`.

**Liu:2023:LGC**

[2921] Xiusheng Liu and Hualu Liu. LCP of group codes over finite Frobenius rings. *Designs, Codes, and Cryptography*, 91 (3):695–708, March 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01120-5`.

**Shen:2023:FTD**

[2922] Jiaxin Shen, Jianfu Chen, and Shenglin Zhou. Flag-transitive 2-designs with prime square replication number and alternating groups. *Designs, Codes, and Cryptography*, 91 (3):709–717, March 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01121-4`.

**Mesnager:2023:FPB**

[2923] Sihem Mesnager, Liqin Qian, and Xiwang Cao. Further projective binary linear codes derived from two-to-one functions and their duals. *Designs, Codes, and Cryptography*, 91 (3):719–746, March 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01122-3`.

**Datta:2023:CSP**

[2924] Mrinmoy Datta and Trygve Johnsen. Codes from symmetric polynomials.

*Designs, Codes, and Cryptography*, 91 (3):747–761, March 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01123-2`.

**Akre:2023:GCC**

[2925] Dev Akre, Nuh Aydin, Matthew Harrington, and Saurav Pandey. A generalization of cyclic code equivalence algorithm to constacyclic codes. *Designs, Codes, and Cryptography*, 91 (3):763–777, March 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01124-1`.

**Correll:2023:DBS**

[2926] Bill Correll, Jr. and Christopher N. Swanson. Difference-based structural properties of Costas arrays. *Designs, Codes, and Cryptography*, 91 (3):779–794, March 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01125-0`.

**Araya:2023:HMR**

[2927] Makoto Araya, Masaaki Harada, and Koji Momihara. Hadamard matrices related to a certain series of ternary self-dual codes. *Designs, Codes, and Cryptography*, 91(3):795–805, March 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01127-y`.

**Meng:2023:WDQ**

[2928] Xiangrui Meng, Jian Gao, Fang-Wei Fu, and Fanghui Ma. Weight distributions of Q2DC codes over finite fields. *Designs, Codes, and Cryptography*, 91 (3):807–830, March 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01128-x`.

**Montanucci:2023:GWS**

[2929] M. Montanucci and G. Tizziotti. Generalized Weierstrass semigroups at several points on certain maximal curves which cannot be covered by the Hermitian curve. *Designs, Codes, and Cryptography*, 91 (3):831–851, March 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01130-3`.

**Kim:2023:PDG**

[2930] Hyoseung Kim, Olivier Sanders, Michel Abdalla, and Jong Hwan Park. Practical dynamic group signatures without knowledge extractors. *Designs, Codes, and Cryptography*, 91(3):853–893, March 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01129-w`.

**DeBoeck:2023:EAP**

[2931] Maarten De Boeck and Geertrui Van de Voorde. Embedded antipodal planes and the minimum weight of the dual code of points and lines in projective planes of order $p^2$. *Designs, Codes, and Cryptography*, 91

(3):895–920, March 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01131-2`.

**Tong:2023:ETS**

[2932] Yan Tong, Xiangyong Zeng, Shasha Zhang, Shiwei Xu, and Zhengwei Ren. The estimates of trigonometric sums and new bounds on a mean value, a sequence and a cryptographic function. *Designs, Codes, and Cryptography*, 91 (3):921–949, March 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01140-1`.

**Na:2023:GBS**

[2933] Jingzhou Na, Jonathan Jedwab, and Shuxing Li. A group-based structure for perfect sequence covering arrays. *Designs, Codes, and Cryptography*, 91 (3):951–970, March 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01132-1`.

**Guo:2023:SSM**

[2934] Fei Guo, Zilong Wang, and Guang Gong. Several secondary methods for constructing bent-negabent functions. *Designs, Codes, and Cryptography*, 91 (3):971–995, March 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01133-0`.

**Bouvier:2023:ADI**

[2935] Clémence Bouvier, Anne Canteaut, and Léo Perrin. On the algebraic degree of iterated power functions. *Designs, Codes, and Cryptography*, 91 (3):997–1033, March 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01136-x`.

**Zhang:2023:JTA**

[2936] Zhongliang Zhang, Zhen Qin, and Chun Guo. Just tweak! Asymptotically optimal security for the cascaded LRW1 tweakable blockcipher. *Designs, Codes, and Cryptography*, 91 (3):1035–1052, March 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01137-w`.

**Lee:2023:DMC**

[2937] Kwangsu Lee. Decentralized multi-client functional encryption for set intersection with improved efficiency. *Designs, Codes, and Cryptography*, 91 (3):1053–1093, March 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01139-8`.

**Ceria:2023:NMC**

[2938] Michela Ceria, Antonio Cossidente, Giuseppe Marino, and Francesco Pavese. On near-MDS codes and caps. *Designs, Codes, and Cryptography*, 91 (3):1095–1110, March 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01141-0`.

**Augot:2023:EML**

[2939] Daniel Augot, Sarah Bordage, and Jade Nardi. Efficient multivariate low-degree tests via interactive oracle proofs of proximity for polynomial codes. *Designs, Codes, and Cryptography*, 91(3):1111–1151, March 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01134-z`.

**Zhang:2023:ELP**

[2940] Wanbao Zhang and Shenglin Zhou. Extremely line-primitive automorphism groups of finite linear spaces. *Designs, Codes, and Cryptography*, 91(3):1153–1163, March 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01138-9`.

**Zheng:2023:IPP**

[2941] Yanbin Zheng, Yuyin Yu, Zhengbang Zha, and Xingchen Zhou. On inverses of permutation polynomials of the form $x\left(x^s - a\right)^{\left(q^m-1\right)/s}$ over $\mathbf{F}_{q^n}$. *Designs, Codes, and Cryptography*, 91(4):1165–1181, April 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01142-z`.

**Vorobyev:2023:CTM**

[2942] Ilya Vorobyev. Complete traceability multimedia fingerprinting codes resistant to averaging attack and adversarial noise with optimal rate. *Designs, Codes, and Cryptography*, 91(4):1183–1191, April 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01144-x`.

**Li:2023:CCD**

[2943] Yun Li and Hongwei Liu. Cyclic constant dimension subspace codes via the sum of Sidon spaces. *Designs, Codes, and Cryptography*, 91(4):1193–1207, April 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01146-9`.

**Fang:2023:PLO**

[2944] Weijun Fang, Bin Chen, Shu-Tao Xia, Fang-Wei Fu, and Xiangyu Chen. Perfect LRCs and $k$-optimal LRCs. *Designs, Codes, and Cryptography*, 91(4):1209–1232, April 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01148-7`.

**Huang:2023:RSO**

[2945] Zhengan Huang, Junzuo Lai, Gongxian Zeng, and Xin Mu. Receiver selective opening security for identity-based encryption in the multi-challenge setting. *Designs, Codes, and Cryptography*, 91(4):1233–1259, April 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01147-8`.

**Xu:2023:CCP**

[2946] Bangteng Xu. Characterizations and constructions of plateaued functions on finite abelian groups. *Designs,*

*Codes, and Cryptography*, 91(4):1261–1292, April 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01151-y.

**Gill:2023:PMO**

[2947] Michael J. Gill and Ian M. Wanless. Pairs of MOLS of order ten satisfying non-trivial relations. *Designs, Codes, and Cryptography*, 91(4):1293–1313, April 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01149-6.

**Satake:2023:CSG**

[2948] Shohei Satake and Yujie Gu. Cayley sum graphs and their applications to codebooks. *Designs, Codes, and Cryptography*, 91(4):1315–1333, April 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01152-x.

**Mo:2023:IHS**

[2949] Songbao Mo. Ideal hierarchical secret sharing and lattice path matroids. *Designs, Codes, and Cryptography*, 91(4):1335–1349, April 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01154-9.

**Mora:2023:DSS**

[2950] Rocco Mora and Jean-Pierre Tillich. On the dimension and structure of the square of the dual of a Goppa code. *Designs, Codes, and Cryptography*, 91(4):1351–1372, April 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01153-w.

**Zeng:2023:CSC**

[2951] Dan Zeng, Xiangyong Zeng, Lisha Li, and Yunge Xu. The cycle structure of a class of permutation polynomials. *Designs, Codes, and Cryptography*, 91(4):1373–1400, April 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01155-8.

**Sun:2023:ISP**

[2952] Shi-Feng Sun, Ron Steinfeld, and Amin Sakzad. Incremental symmetric puncturable encryption with support for unbounded number of punctures. *Designs, Codes, and Cryptography*, 91(4):1401–1426, April 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01143-y.

**Lavorante:2023:EPC**

[2953] Vincenzo Pallozzi Lavorante. External points to a conic from a Baer subplane. *Designs, Codes, and Cryptography*, 91(4):1427–1441, April 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01156-7.

**Elsholtz:2023:LSM**

[2954] Christian Elsholtz, Benjamin Klahn, and Gabriel F. Lipnik. Large subsets

of $\mathbf{Z}_m^n$ without arithmetic progressions. *Designs, Codes, and Cryptography*, 91 (4):1443–1452, April 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01145-w`.

**Shi:2023:SDB**

[2955] Minjia Shi, Yaya Li, Wei Cheng, Dean Crnković, Denis Krotov, and Patrick Solé. Self-dual bent sequences for complex Hadamard matrices. *Designs, Codes, and Cryptography*, 91 (4):1453–1474, April 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01157-6`.

**Monzillo:2023:EFP**

[2956] Giusy Monzillo, Tim Penttila, and Alessandro Siciliano. Eggs in finite projective spaces and unitals in translation planes. *Designs, Codes, and Cryptography*, 91(4):1475–1485, April 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01162-9`.

**Iurlano:2023:GPS**

[2957] Enrico Iurlano. Growth of the perfect sequence covering array number. *Designs, Codes, and Cryptography*, 91 (4):1487–1494, April 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01168-3`.

**Xu:2023:OQR**

[2958] Li Xu, Zhengchun Zhou, Jun Zhang, and Sihem Mesnager. Optimal quaternary $(r, \delta)$-locally recoverable codes: their structures and complete classification. *Designs, Codes, and Cryptography*, 91(4):1495–1526, April 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01165-6`.

**Sun:2023:OQH**

[2959] Zhonghua Sun, Sujuan Huang, and Shixin Zhu. Optimal quaternary Hermitian LCD codes and their related codes. *Designs, Codes, and Cryptography*, 91(4):1527–1558, April 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01166-5`.

**Su:2023:FSC**

[2960] Sihong Su and Xiaoqi Guo. A further study on the construction methods of bent functions and self-dual bent functions based on Rothaus's bent function. *Designs, Codes, and Cryptography*, 91 (4):1559–1580, April 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01169-2`.

**Barwick:2023:GDF**

[2961] S. G. Barwick, Alice M. W. Hui, and Wen-Ai Jackson. A geometric description of the Figueroa plane. *Designs, Codes, and Cryptography*, 91 (5):1581–1593, May 2023. CODEN

DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01158-5.

**Hollmann:2023:SBC**

[2962] Henk D. L. Hollmann, Karan Khathuria, Ago-Erik Riet, and Vitaly Skachek. On some batch code properties of the simplex code. *Designs, Codes, and Cryptography*, 91(5):1595–1605, May 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01173-6.

**Shaporenko:2023:DBF**

[2963] Alexander Shaporenko. Derivatives of bent functions in connection with the bent sum decomposition problem. *Designs, Codes, and Cryptography*, 91(5):1607–1625, May 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01167-4.

**Ducoat:2023:RWH**

[2964] Jérôme Ducoat and Frédérique Oggier. Rank weight hierarchy of some classes of polynomial codes. *Designs, Codes, and Cryptography*, 91(5):1627–1644, May 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01181-6.

**Attrapadung:2023:MCP**

[2965] Nuttapong Attrapadung, Goichiro Hanaoka, Ryo Hiromasa, Takahiro Matsuda, and Jacob C. N. Schuldt. Maliciously circuit-private multi-key FHE and MPC based on LWE. *Designs, Codes, and Cryptography*, 91(5):1645–1684, May 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01160-x.

**Ball:2023:GRC**

[2966] Simeon Ball. Grassl–Rötteler cyclic and consta-cyclic MDS codes are generalised Reed–Solomon codes. *Designs, Codes, and Cryptography*, 91(5):1685–1694, May 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01174-5.

**Hu:2023:DSB**

[2967] Zhao Hu, Nian Li, Linjie Xu, Xiangyong Zeng, and Xiaohu Tang. The differential spectrum and boomerang spectrum of a class of locally-APN functions. *Designs, Codes, and Cryptography*, 91(5):1695–1711, May 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01161-w.

**Yu:2023:IMP**

[2968] Han-Bing Yu, Qun-Xiong Zheng, Yi-Jian Liu, Jing-Guo Bi, Yu-Fei Duan, Jing-Wen Xue, You Wu, Yue Cao, Rong Cheng, Lin Wang, and Bai-Shun Sun. An improved method for predicting truncated multiple recursive generators with unknown parameters. *Designs, Codes, and Cryptography*, 91(5):1713–1736, May 2023. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01175-4.

**Tang:2023:GFP**

[2969] Hopein Christofen Tang and Djoko Suprijanto. A general family of Plotkin-optimal two-weight codes over $\mathbf{Z}_4$. *Designs, Codes, and Cryptography*, 91 (5):1737–1750, May 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01176-3.

**Eriguchi:2023:MVM**

[2970] Reo Eriguchi, Noboru Kunihiro, and Koji Nuida. Multiplicative and verifiably multiplicative secret sharing for multipartite adversary structures. *Designs, Codes, and Cryptography*, 91 (5):1751–1778, May 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01177-2.

**Wang:2023:PSN**

[2971] Jiabo Wang and Cong Ling. Polar sampler: A novel Bernoulli sampler using polar codes with application to integer Gaussian sampling. *Designs, Codes, and Cryptography*, 91 (5):1779–1811, May 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01164-7.

**Araya:2023:SRW**

[2972] Makoto Araya and Masaaki Harada. Some restrictions on the weight enumerators of near-extremal ternary self-dual codes and quaternary Hermitian self-dual codes. *Designs, Codes, and Cryptography*, 91(5):1813–1843, May 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01172-7.

**Datta:2023:SAB**

[2973] Pratish Datta, Ratna Dutta, and Sourav Mukhopadhyay. Short attribute-based signatures for arbitrary Turing machines from standard assumptions. *Designs, Codes, and Cryptography*, 91 (5):1845–1872, May 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01163-8.

**Li:2023:CCL**

[2974] Fengwei Li. Cyclic codes of length $5p$ with MDS symbol-pair. *Designs, Codes, and Cryptography*, 91 (5):1873–1888, May 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01184-x.

**Wang:2023:DNC**

[2975] Zhongxiao Wang, Xiaoxin Zhao, Qunxiong Zheng, Xiutao Feng, and Zehao Sun. The decomposition of an NFSR into the cascade connection of two smaller NFSRs revisited. *Designs, Codes, and Cryptography*, 91 (5):1889–1910, May 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01182-z.

**Durante:2023:DVS**

[2976] N. Durante, G. Longobardi, and V. Pepe. $(d, \sigma)$-Veronese variety and some applications. *Designs, Codes, and Cryptography*, 91(5):1911–1921, May 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01186-9`.

**Han:2023:CMP**

[2977] Hui Han, Jianjun Mu, Xiaopeng Jiao, Yu-Cheng He, and Zhanzhan Zhao. Constructions of multi-permutation codes correcting a single burst of deletions. *Designs, Codes, and Cryptography*, 91(5):1923–1934, May 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01190-z`.

**Lavrauw:2023:SDS**

[2978] Michel Lavrauw and John Sheekey. Symplectic 4-dimensional semifields of order $8^4$ and $9^4$. *Designs, Codes, and Cryptography*, 91(5):1935–1949, May 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01183-y`.

**Gyarmati:2023:SSR**

[2979] Máté Gyarmati. Secret sharing on regular bipartite access structures. *Designs, Codes, and Cryptography*, 91(5):1951–1971, May 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01187-8`.

**Yadav:2023:RMC**

[2980] Monika Yadav and Anuradha Sharma. A recursive method for the construction and enumeration of self-orthogonal and self-dual codes over the quasi-Galois ring $\mathbf{F}_{2^r}[u]/\langle u^e \rangle$. *Designs, Codes, and Cryptography*, 91(5):1973–2003, May 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01185-w`.

**Gorla:2023:QOA**

[2981] Elisa Gorla and Cristina Landolina. Quasi optimal anticodes: structure and invariants. *Designs, Codes, and Cryptography*, 91(5):2005–2020, May 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01188-7`.

**Jiao:2023:GDA**

[2982] Lin Jiao, Yonglin Hao, and Yongqiang Li. Guess-and-determine attacks on SNOW–VI stream cipher. *Designs, Codes, and Cryptography*, 91(5):2021–2055, May 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01150-z`.

**Qiao:2023:NCL**

[2983] Wenxiao Qiao, Hailun Yan, Siwei Sun, Lei Hu, and Jiwu Jing. New cryptanalysis of LowMC with algebraic techniques. *Designs,*

*Codes, and Cryptography*, 91(5):2057–2075, May 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01178-1`.

**Chara:2023:MDP**

[2984] María Chara, Sam Kottler, Beth Malmskog, Bianca Thompson, and Mckenzie West. Minimum distance and parameter ranges of locally recoverable codes with availability from fiber products of curves. *Designs, Codes, and Cryptography*, 91(5):2077–2105, May 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01189-6`.

**Gordon:2023:SDS**

[2985] Daniel M. Gordon. Signed difference sets. *Designs, Codes, and Cryptography*, 91(5):2107–2115, May 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01171-8`.

**Li:2023:UOD**

[2986] Rupert Li. Unique optima of the Delsarte linear program. *Designs, Codes, and Cryptography*, 91(6):2117–2140, June 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01191-y`.

**Beullens:2023:GSM**

[2987] Ward Beullens, Samuel Dobson, Shuichi Katsumata, Yi-Fu Lai, and Federico Pintore. Group signatures and more from isogenies and lattices: generic, simple, and efficient. *Designs, Codes, and Cryptography*, 91(6):2141–2200, June 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01192-x`.

**Ryabko:2023:USS**

[2988] Boris Ryabko. Unconditionally secure short key ciphers based on data compression and randomization. *Designs, Codes, and Cryptography*, 91(6):2201–2212, June 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01195-8`.

**Vega:2023:SWD**

[2989] Gerardo Vega. The $b$-symbol weight distributions of all semiprimitive irreducible cyclic codes. *Designs, Codes, and Cryptography*, 91(6):2213–2221, June 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01193-w`.

**Chakraborty:2023:HTP**

[2990] Himadri Shekhar Chakraborty, Tsuyoshi Miezaki, and Manabu Oura. Harmonic Tutte polynomials of matroids. *Designs, Codes, and Cryptography*, 91(6):2223–2236, June 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01196-7`.

**Jho:2023:PMG**

[2991] Nam-Su Jho and Jooyoung Lee. Partition and mix: generalizing the swap-or-not shuffle. *Designs, Codes, and Cryptography*, 91(6):2237–2254, June 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01199-4.

**Zhang:2023:NMS**

[2992] Zihan Zhang. A new metric on symmetric groups and applications to block permutation codes. *Designs, Codes, and Cryptography*, 91(6):2255–2271, June 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01197-6.

**Du:2023:SCN**

[2993] Xiaoni Du, Wengang Jin, and Sihem Mesnager. Several classes of new weakly regular bent functions outside $\mathcal{RF}$, their duals and some related (minimal) codes with few weights. *Designs, Codes, and Cryptography*, 91(6):2273–2307, June 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01198-5.

**Hammer:2023:DCF**

[2994] James Hammer and John Lorch. Diagonal cellular factor pair Latin squares. *Designs, Codes, and Cryptography*, 91(6):2309–2322, June 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01200-0.

**Lemos:2023:APF**

[2995] Abílio Lemos, Victor G. L. Neumann, and Sávio Ribas. On arithmetic progressions in finite fields. *Designs, Codes, and Cryptography*, 91(6):2323–2346, June 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01201-z.

**Feng:2023:FGQ**

[2996] Tao Feng and Jianbing Lu. On finite generalized quadrangles with $\mathrm{PSL}(2, q)$ as an automorphism group. *Designs, Codes, and Cryptography*, 91(6):2347–2364, June 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01203-x.

**Pasalic:2023:EIF**

[2997] Enes Pasalic, Amar Bapić, Fengrong Zhang, and Yongzhuang Wei. Explicit infinite families of bent functions outside the completed Maiorana–McFarland class. *Designs, Codes, and Cryptography*, 91(7):2365–2393, July 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01204-w.

**Wang:2023:TFN**

[2998] Xiaoqiang Wang, Zhonghua Sun, and Cunsheng Ding. Two families of negacyclic BCH codes. *Designs, Codes, and Cryptography*, 91

(7):2395–2420, July 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01208-6.

**Ding:2023:FTC**

[2999] Jian Ding, Changlu Lin, Fuchun Lin, and Huaxiong Wang. Full threshold change range of threshold changeable secret sharing. *Designs, Codes, and Cryptography*, 91 (7):2421–2447, July 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01205-9.

**Stanojkovski:2023:SCS**

[3000] Mima Stanojkovski. Submodule codes as spherical codes in buildings. *Designs, Codes, and Cryptography*, 91 (7):2449–2472, July 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01207-7.

**Shparlinski:2023:FPS**

[3001] Igor E. Shparlinski. Fixed points of the subset sum pseudorandom number generators. *Designs, Codes, and Cryptography*, 91(7):2473–2479, July 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01209-5.

**Delgado:2023:SNT**

[3002] Moises Delgado, Heeralal Janwa, and Carlos Agrinsoni. Some new techniques and progress towards the resolution of the conjecture of exceptional APN functions and absolutely irreducibility of a class of polynomials. *Designs, Codes, and Cryptography*, 91(7):2481–2495, July 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01202-y.

**vanTrung:2023:PME**

[3003] Tran van Trung. Point-missing $s$-resolvable $t$-designs: infinite series of 4-designs with constant index. *Designs, Codes, and Cryptography*, 91 (7):2497–2508, July 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01206-8.

**Bannai:2023:NAM**

[3004] Eiichi Bannai, Tsuyoshi Miezaki, and Hiroyuki Nakasora. A note on the Assmus–Mattson theorem for some binary codes II. *Designs, Codes, and Cryptography*, 91(7):2509–2522, July 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01212-w.

**Kobayashi:2023:TLB**

[3005] Hirokazu Kobayashi, Yohei Watanabe, Kazuhiko Minematsu, and Junji Shikata. Tight lower bounds and optimal constructions of anonymous broadcast encryption and authentication. *Designs, Codes, and Cryptography*, 91 (7):2523–2562, July 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01211-x.

**Li:2023:IMC**

[3006] Shitao Li, Minjia Shi, and Juan Wang. An improved method for constructing formally self-dual codes with small hulls. *Designs, Codes, and Cryptography*, 91(7):2563–2583, July 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01210-y`.

**Pavone:2023:SSB**

[3007] Marco Pavone. Subset sums and block designs in a finite vector space. *Designs, Codes, and Cryptography*, 91 (7):2585–2603, July 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01213-9`.

**Chen:2023:CNO**

[3008] Guangzhou Chen and Xiaodong Niu. Constructions for new orthogonal arrays based on large sets of orthogonal arrays. *Designs, Codes, and Cryptography*, 91(7):2605–2625, July 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01217-5`.

**Lu:2023:GCR**

[3009] Wei Lu, Xia Wu, Yufei Wang, and Xiwang Cao. A general construction of regular complete permutation polynomials. *Designs, Codes, and Cryptography*, 91(8):2627–2647, August 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01224-6`.

**Byrne:2023:IMD**

[3010] Isabel Byrne, Natalie Dodson, Ryan Lynch, Eric Pabón-Cancel, and Fernando Piñero-González. Improving the minimum distance bound of Trace Goppa codes. *Designs, Codes, and Cryptography*, 91(8):2649–2663, August 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01216-6`.

**Chen:2023:NME**

[3011] Hao Chen. New MDS entanglement-assisted quantum codes from MDS Hermitian self-orthogonal codes. *Designs, Codes, and Cryptography*, 91 (8):2665–2676, August 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01232-6`.

**Liu:2023:MRL**

[3012] Yan Liu and Jianguo Lei. More results on large sets of Kirkman triple systems. *Designs, Codes, and Cryptography*, 91 (8):2677–2686, August 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01221-9`.

**Zhang:2023:PQS**

[3013] Zhongya Zhang, Wenling Wu, Han Sui, and Bolin Wang. Post-quantum security on the Lai–Massey scheme. *Designs, Codes, and Cryptography*, 91

(8):2687–2704, August 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01225-5.

**Hoepman:2023:TFB**

[3014] Jaap-Henk Hoepman. Two faces of blindness. *Designs, Codes, and Cryptography*, 91(8):2705–2721, August 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01228-2.

**Bagherpour:2023:BPB**

[3015] Bagher Bagherpour. A bivariate polynomial-based cryptographic hard problem and its applications. *Designs, Codes, and Cryptography*, 91 (8):2723–2735, August 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01229-1.

**Zhu:2023:OEG**

[3016] Yan Zhu. Optimal and extremal graphical designs on regular graphs associated with classical parameters. *Designs, Codes, and Cryptography*, 91 (8):2737–2754, August 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01231-7.

**Tan:2023:DSC**

[3017] Xiantong Tan and Haode Yan. Differential spectrum of a class of APN power functions. *Designs, Codes, and Cryptography*, 91(8):2755–2768, August 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01218-4.

**Xue:2023:AGA**

[3018] Erzhong Xue and Zilong Wang. The $q$-ary Golay arrays of size $2 \times 2 \times \cdots \times 2$ are standard. *Designs, Codes, and Cryptography*, 91(8):2769–2778, August 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01230-8.

**Kim:2023:PTA**

[3019] Jiseung Kim and Changmin Lee. A polynomial time algorithm for breaking NTRU encryption with multiple keys. *Designs, Codes, and Cryptography*, 91 (8):2779–2789, August 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01233-5.

**Lan:2023:BTD**

[3020] Ting Lan, Weijun Liu, and Fu-Gang Yin. Block-transitive 3-$(v, k, 1)$ designs associated with alternating groups. *Designs, Codes, and Cryptography*, 91 (8):2791–2807, August 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01215-7.

**Feng:2023:OPZ**

[3021] Rongquan Feng. Obituary of Professor Zhexian Wan. *Designs, Codes, and Cryptography*, 91(9):2809–2810, September 2023. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01273-x.

**Zhang:2023:CSP**

[3022] Junyang Zhang. Characterizing subgroup perfect codes by 2-subgroups. *Designs, Codes, and Cryptography*, 91(9):2811–2819, September 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01240-6.

**Sun:2023:SFI**

[3023] Zhonghua Sun, Xiaoqiang Wang, and Cunsheng Ding. Several families of irreducible constacyclic and cyclic codes. *Designs, Codes, and Cryptography*, 91(9):2821–2843, September 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01242-4.

**Zhang:2023:MMA**

[3024] Kai Zhang, Xuejia Lai, Lei Wang, Jie Guan, Bin Hu, Senpeng Wang, and Tairong Shi. Meet-in-the-middle attack with splice-and-cut technique and a general automatic framework. *Designs, Codes, and Cryptography*, 91(9):2845–2878, September 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01226-4.

**Glasby:2023:PND**

[3025] S. P. Glasby, Ferdinand Ihringer, and Sam Mattheus. The proportion of non-degenerate complementary subspaces in classical spaces. *Designs, Codes, and Cryptography*, 91(9):2879–2891, September 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01235-3.

**Zhan:2023:HIS**

[3026] Yu Zhan, Ziqian Zhang, Qian Liu, and Baocang Wang. Hiding the input-size in multi-party private set intersection. *Designs, Codes, and Cryptography*, 91(9):2893–2915, September 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01238-0.

**Datta:2023:CAS**

[3027] Pratish Datta and Tapas Pal. (Compact) adaptively secure FE for attribute-weighted sums from $k$–Lin. *Designs, Codes, and Cryptography*, 91(9):2917–3034, September 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01219-3.

**Dupin:2023:AIR**

[3028] Aurélien Dupin, Pierrick Méaux, and Mélissa Rossi. On the algebraic immunity-resiliency trade-off, implications for Goldreich's pseudorandom generator. *Designs, Codes, and Cryptography*, 91(9):3035–3079, September 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https:

//link.springer.com/article/10.1007/s10623-023-01220-w.

**Lee:2023:SFE**

[3029] Hyung Tae Lee and Jae Hong Seo. On the security of functional encryption in the generic group model. *Designs, Codes, and Cryptography*, 91(9):3081–3114, September 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01237-1.

**Liu:2023:NSN**

[3030] Kaiqiang Liu, Zhengchun Zhou, Avik Ranjan Adhikary, and Rong Luo. New sets of non-orthogonal spreading sequences with low correlation and low PAPR using extended Boolean functions. *Designs, Codes, and Cryptography*, 91(10):3115–3139, October 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01247-z.

**Dai:2023:FSM**

[3031] Yu Dai, Kaizhan Lin, Chang-An Zhao, and Zijian Zhou. Fast subgroup membership testings for $\mathbf{G}_1$, $\mathbf{G}_2$ and $\mathbf{G}_T$ on pairing-friendly curves. *Designs, Codes, and Cryptography*, 91(10):3141–3166, October 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01223-7.

**Bartoli:2023:ERA**

[3032] Daniele Bartoli, Giuliana Fatabbi, and Francesco Ghiandoni. On the exceptionality of rational APN functions. *Designs, Codes, and Cryptography*, 91(10):3167–3186, October 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01246-0.

**Zhang:2023:WRP**

[3033] Kai Zhang, Xuejia Lai, Jie Guan, and Bin Hu. Weak rotational property and its application. *Designs, Codes, and Cryptography*, 91(10):3187–3214, October 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01241-5.

**Crnkovic:2023:LSC**

[3034] Dean Crnković and Andrea Svob. LCD subspace codes. *Designs, Codes, and Cryptography*, 91(10):3215–3226, October 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01251-3.

**Lee:2023:EPG**

[3035] Melissa Lee and Gabriel Verret. Extremely primitive groups and linear spaces. *Designs, Codes, and Cryptography*, 91(10):3227–3240, October 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01244-2.

**Tseng:2023:SPB**

[3036] Pin-Chieh Tseng, Ching-Yi Lai, and Wei-Hsuan Yu. Semidefinite program-

ming bounds for binary codes from a split Terwilliger algebra. *Designs, Codes, and Cryptography*, 91(10):3241–3262, October 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01250-4.

**Ma:2023:BCP**

[3037] Wen Ma and Jinquan Luo. Block codes in pomset metric over $\mathbf{Z}_m$. *Designs, Codes, and Cryptography*, 91(10):3263–3284, October 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01249-x.

**Reis:2023:ADK**

[3038] Lucas Reis. The average density of $K$-normal elements over finite fields. *Designs, Codes, and Cryptography*, 91(10):3285–3292, October 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01257-x.

**Krotov:2023:PTF**

[3039] Denis S. Krotov. Projective tilings and full-rank perfect codes. *Designs, Codes, and Cryptography*, 91(10):3293–3303, October 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01256-y.

**Betti:2023:LRQ**

[3040] Livia Betti, Jim Brown, Fernando Gaitan, Aiyana Spear, and Japheth Varlack. Lattices in real quadratic fields and associated theta series arising from codes over $\mathbf{F}_4$ and $\mathbf{F}_2 \times \mathbf{F}_2$. *Designs, Codes, and Cryptography*, 91(10):3305–3319, October 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01258-w.

**Xu:2023:TPP**

[3041] Jie Xu, Zhiyong Zheng, Kun Tian, and Man Chen. Two properties of prefix codes and uniquely decodable codes. *Designs, Codes, and Cryptography*, 91(10):3321–3330, October 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01253-1.

**Galbraith:2023:GES**

[3042] Steven Galbraith, Rosario Gennaro, Carla Ràfols, and Ron Steinfeld. Guest editorial: Special issue on mathematics of zero-knowledge. *Designs, Codes, and Cryptography*, 91(11):3331–3332, November 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01260-2.

**Aranha:2023:SEC**

[3043] Diego F. Aranha, Youssef El Housni, and Aurore Guillevic. A survey of elliptic curves for proof systems. *Designs, Codes, and Cryptography*, 91(11):3333–3378, November 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-022-01135-y.

**Ames:2023:LLS**

[3044] Scott Ames, Carmit Hazay, Yuval Ishai, and Muthuramakrishnan Venkitasubramaniam. Ligero: lightweight sublinear arguments without a trusted setup. *Designs, Codes, and Cryptography*, 91(11):3379–3424, November 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01222-8.

**Beullens:2023:PKI**

[3045] Ward Beullens, Luca De Feo, Steven D. Galbraith, and Christophe Petit. Proving knowledge of isogenies: a survey. *Designs, Codes, and Cryptography*, 91(11):3425–3456, November 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01243-3.

**Benarroch:2023:ZKP**

[3046] Daniel Benarroch, Matteo Campanelli, Dario Fiore, Kobi Gurkan, and Dimitris Kolonelos. Zero-knowledge proofs for set membership: efficient, succinct, modular. *Designs, Codes, and Cryptography*, 91(11):3457–3525, November 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01245-1.

**Baum:2023:SVO**

[3047] Carsten Baum, Samuel Dittmer, Peter Scholl, and Xiao Wang. Sok: vector OLE-based zero-knowledge protocols. *Designs, Codes, and Cryptography*, 91(11):3527–3561, November 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01292-8.

**Castoldi:2023:CSS**

[3048] André Guerino Castoldi, Anderson Novaes Martinhão, Emerson L. Monte Carmelo, and Otávio J. N. T. N. dos Santos. Covering schemes of strength $t$. *Designs, Codes, and Cryptography*, 91(11):3563–3580, November 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01252-2.

**Wei:2023:IAA**

[3049] Congming Wei, Bingyou Dong, Jialiang Hua, Xiaoyang Dong, and Guoyan Zhang. Improved attacks against reduced-round Whirlwind. *Designs, Codes, and Cryptography*, 91(11):3581–3602, November 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01254-0.

**Wang:2023:NMC**

[3050] Senpeng Wang, Dengguo Feng, Bin Hu, Jie Guan, Kai Zhang, and Tairong Shi. New method for combining Matsui's bounding conditions with sequential encoding method. *Designs, Codes, and Cryptography*, 91(11):3603–3642, November 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01259-9.

**Asgarli:2023:PCG**

[3051] Shamil Asgarli, Dragos Ghioca, and Chi Hoi Yip. Plane curves giving rise to blocking sets over finite fields. *Designs, Codes, and Cryptography*, 91(11):3643–3669, November 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01264-y.

**Bardet:2023:RAA**

[3052] Magali Bardet, Pierre Briaud, Maxime Bros, Philippe Gaborit, and Jean-Pierre Tillich. Revisiting algebraic attacks on MinRank and on the rank decoding problem. *Designs, Codes, and Cryptography*, 91(11):3671–3707, November 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01265-x.

**Tian:2023:FSB**

[3053] Shizhu Tian, Yitong Liu, and Xiangyong Zeng. A further study on bridge structures and constructing bijective S-boxes for low-latency masking. *Designs, Codes, and Cryptography*, 91(11):3709–3739, November 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01266-w.

**Bao:2023:CCO**

[3054] Jingjun Bao. Constructions of column-orthogonal strong orthogonal arrays via matchings of bipartite graphs. *Designs, Codes, and Cryptography*, 91(11):3741–3755, November 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01267-9.

**Zhou:2023:LRI**

[3055] Yanwei Zhou, Bo Yang, Zirui Qiao, Zhe Xia, Mingwu Zhang, and Yi Mu. Leakage-resilient identity-based cryptography from minimal assumptions. *Designs, Codes, and Cryptography*, 91(11):3757–3801, November 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01268-8.

**Cao:2023:GAE**

[3056] Jinzheng Cao, Jian Weng, Yanbin Pan, and Qingfeng Cheng. Generalized attack on ECDSA: known bits in arbitrary positions. *Designs, Codes, and Cryptography*, 91(11):3803–3823, November 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01269-7.

**Pang:2023:BTV**

[3057] Xuan Pang and Xiaoqin Zhan. Block-transitive 3-$(v, 4, \lambda)$ designs with sporadic or alternating socle. *Designs, Codes, and Cryptography*, 91(12):3825–3835, December 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01275-9.

**Samajder:2023:ALK**

[3058] Subhabrata Samajder and Palash Sarkar. Another look at key ran-

domisation hypotheses. *Designs, Codes, and Cryptography*, 91(12):3837–3855, December 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01272-y`.

**Golalizadeh:2023:FWG**

[3059] Somayyeh Golalizadeh and Nasrin Soltankhah. On the fourth weight of generalized Reed–Muller codes. *Designs, Codes, and Cryptography*, 91(12):3857–3879, December 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01276-8`.

**Xie:2023:SEA**

[3060] Xiaofeng Xie and Tian Tian. Structural evaluation of AES-like ciphers against mixture differential cryptanalysis. *Designs, Codes, and Cryptography*, 91(12):3881–3899, December 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01277-7`.

**Huang:2023:CSC**

[3061] Hexiang Huang and Qing Xiang. Construction of storage codes of rate approaching one on triangle-free graphs. *Designs, Codes, and Cryptography*, 91(12):3901–3913, December 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01278-6`.

**Shinagawa:2023:PSM**

[3062] Kazumasa Shinagawa, Reo Eriguchi, Shohei Satake, and Koji Nuida. Private simultaneous messages based on quadratic residues. *Designs, Codes, and Cryptography*, 91(12):3915–3932, December 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01279-5`.

**Pang:2023:BCL**

[3063] Binbin Pang, Shixin Zhu, Tian Yang, and Jun Gao. BCH codes with larger dimensional hull. *Designs, Codes, and Cryptography*, 91(12):3933–3951, December 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01281-x`.

**Heng:2023:TSO**

[3064] Ziling Heng, Dexiang Li, and Fenjin Liu. Ternary self-orthogonal codes from weakly regular bent functions and their application in LCD codes. *Designs, Codes, and Cryptography*, 91(12):3953–3976, December 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01287-5`.

**Liu:2023:OFD**

[3065] Shuangqing Liu. Optimal Ferrers diagram rank-metric codes from MRD codes. *Designs, Codes, and Cryptography*, 91(12):3977–3993, December 2023. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01284-8.

**Gomez-Torrecillas:2023:SDG**

[3066] José Gómez-Torrecillas, F. J. Lobillo, and Gabriel Navarro. Skew differential Goppa codes and their application to Mceliece cryptosystem. *Designs, Codes, and Cryptography*, 91(12):3995–4017, December 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01286-6.

**Kim:2023:CBP**

[3067] Haider Al Kim, Sven Puchinger, Ludo Tolhuizen, and Antonia Wachter-Zeh. Coding and bounds for partially defective memory cells. *Designs, Codes, and Cryptography*, 91(12):4019–4058, December 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01270-0.

**Aswad:2023:IDL**

[3068] Haetham Al Aswad and Cécile Pierrot. Individual discrete logarithm with sublattice reduction. *Designs, Codes, and Cryptography*, 91(12):4059–4091, December 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01282-w.

**Chee:2023:SRC**

[3069] Yeow Meng Chee, Alan Chi Hung Ling, Van Khu Vu, and Hui Zhang. Scheduling to reduce close contacts: resolvable grid graph decomposition and packing. *Designs, Codes, and Cryptography*, 91(12):4093–4106, December 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01291-9.

**Li:2023:PAS**

[3070] Qiang Li, Qun xiong Zheng, and Wen feng Qi. Practical attacks on small private exponent RSA: new records and new insights. *Designs, Codes, and Cryptography*, 91(12):4107–4142, December 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01295-5.

**Liu:2023:CCC**

[3071] Hongwei Liu and Shengwei Liu. A class of constacyclic codes are generalized Reed–Solomon codes. *Designs, Codes, and Cryptography*, 91(12):4143–4151, December 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01294-6.

**Liu:2024:PSF**

[3072] Hai Liu, Chengju Li, and Haifeng Qian. Parameters of several families of binary duadic codes and their related codes. *Designs, Codes, and Cryptography*, 92(1):1–12, January 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01285-7.

**Bhattacharjee:2024:BSR**

[3073] Arghya Bhattacharjee, Ritam Bhaumik, Avijit Dutta, Mridul Nandi, and Anik Raychaudhuri. BBB security for 5-round even-Mansour-based key-alternating Feistel ciphers. *Designs, Codes, and Cryptography*, 92 (1):13–49, January 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01288-4.

**Pan:2024:GCM**

[3074] Jiaxin Pan, Chen Qian, and Benedikt Wagner. Generic constructions of master-key KDM secure attribute-based encryption. *Designs, Codes, and Cryptography*, 92(1):51–92, January 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01296-4.

**Coolsaet:2024:NHN**

[3075] Kris Coolsaet. Nonsingular hypercubes and nonintersecting hyperboloids. *Designs, Codes, and Cryptography*, 92 (1):93–112, January 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01297-3.

**Kutsenko:2024:DSD**

[3076] Aleksandr Kutsenko. Decomposing self-dual bent functions. *Designs, Codes, and Cryptography*, 92(1):113–144, January 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01298-2.

**Sagar:2024:MOB**

[3077] Vidya Sagar and Ritumoni Sarma. Minimal and optimal binary codes obtained using $C_D$-construction over the non-unital ring I. *Designs, Codes, and Cryptography*, 92(1):145–157, January 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01299-1.

**Dunkelman:2024:QTM**

[3078] Orr Dunkelman, Nathan Keller, Eyal Ronen, and Adi Shamir. Quantum time/memory/data tradeoff attacks. *Designs, Codes, and Cryptography*, 92 (1):159–177, January 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01300-x.

**Ceria:2024:TGF**

[3079] Michela Ceria and Teo Mora. Towards a Gröbner-free approach to coding. *Designs, Codes, and Cryptography*, 92 (1):179–204, January 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01302-9.

**Gavrilyuk:2024:UAS**

[3080] Alexander L. Gavrilyuk and Sho Suda. Uniqueness of an association scheme related to the Witt design on 11 points. *Designs, Codes, and Cryptography*, 92 (1):205–209, January 2024. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01303-8.

**He:2024:PEC**

[3081] Boyi He and Qunying Liao. The properties and the error-correcting pair for lengthened GRS codes. *Designs, Codes, and Cryptography*, 92 (1):211–225, January 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01304-7.

**Hodzic:2024:QCF**

[3082] S. Hodzić, A. Roy, and E. Andreeva. Quantum cryptanalysis of Farfalle and (generalised) key-alternating Feistel networks. *Designs, Codes, and Cryptography*, 92 (2):227–257, February 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01305-6.

**Lu:2024:FTS**

[3083] Ziwei Lu and Shenglin Zhou. Flag-transitive symmetric 2-designs of prime order. *Designs, Codes, and Cryptography*, 92(2):259–266, February 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01307-4.

**Wu:2024:PPT**

[3084] Danyao Wu and Pingzhi Yuan. Permutation polynomials and their compositional inverses over finite fields by a local method. *Designs, Codes, and Cryptography*, 92(2):267–276, February 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01308-3.

**Takahashi:2024:CCS**

[3085] Kota Takahashi, Keitaro Hashimoto, and Wakaha Ogata. Chosen-ciphertext secure code-based threshold public key encryptions with short ciphertext. *Designs, Codes, and Cryptography*, 92 (2):277–301, February 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01309-2.

**Yadav:2024:CES**

[3086] Monika Yadav and Anuradha Sharma. Construction and enumeration of self-orthogonal and self-dual codes over Galois rings of even characteristic. *Designs, Codes, and Cryptography*, 92 (2):303–339, February 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01310-9.

**Ma:2024:CRW**

[3087] Wen Ma and Jinquan Luo. Codes with respect to weighted poset block metric. *Designs, Codes, and Cryptography*, 92 (2):341–363, February 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01311-8.

**Su:2024:DSO**

[3088] Xiaowei Su, Zihong Tian, and Guohui Hao. Determination of the sizes

of optimal geometric orthogonal codes with parameters $(n \times m, k, \lambda, k-1)$. *Designs, Codes, and Cryptography*, 92 (2):365–395, February 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01312-7`.

**Fan:2024:NCN**

[3089] Cuiling Fan, An Wang, and Li Xu. New classes of NMDS codes with dimension 3. *Designs, Codes, and Cryptography*, 92(2):397–418, February 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01313-6`.

**Donovan:2024:MPL**

[3090] Diane M. Donovan, Mike J. Grannell, and Emine Sule Yazici. On maximal partial Latin hypercubes. *Designs, Codes, and Cryptography*, 92 (2):419–433, February 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01314-5`.

**Bartz:2024:FKN**

[3091] Hannes Bartz, Thomas Jerkovits, and Johan Rosenkilde. Fast Kötter–Nielsen–Høholdt interpolation over skew polynomial rings and its application in coding theory. *Designs, Codes, and Cryptography*, 92(2):435–465, February 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01315-4`.

**Kolomeec:2024:IAS**

[3092] Nikolay Kolomeec and Denis Bykov. On the image of an affine subspace under the inverse function within a finite field. *Designs, Codes, and Cryptography*, 92(2):467–476, February 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01316-3`.

**Can:2024:DCH**

[3093] Mahir Bilen Can, Roy Joshua, and G. V. Ravindra. Defects of codes from higher dimensional algebraic varieties. *Designs, Codes, and Cryptography*, 92 (2):477–494, February 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01317-2`.

**Bamberg:2024:CPH**

[3094] John Bamberg. On the 430-cap of PG$(6, 4)$ having two intersection sizes with respect to hyperplanes. *Designs, Codes, and Cryptography*, 92 (2):495–503, February 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01318-1`.

**Anonymous:2024:ENC**

[3095] Anonymous. Editorial note: Coding and Cryptography 2022. *Designs, Codes, and Cryptography*, 92 (3):505, March 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01365-2`.

**Timpanella:2024:FLM**

[3096] Marco Timpanella and Giovanni Zini. On a family of linear MRD codes with parameters $[8 \times 8, 16, 7]_q$. *Designs, Codes, and Cryptography*, 92 (3):507–530, March 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01179-0`.

**Bapic:2024:VBF**

[3097] Amar Bapić, Enes Pasalic, Alexandr Polujan, and Alexander Pott. Vectorial Boolean functions with the maximum number of bent components beyond the Nyberg's bound. *Designs, Codes, and Cryptography*, 92 (3):531–552, March 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01180-7`.

**Hormann:2024:IBD**

[3098] Felicitas Hörmann and Hannes Bartz. Interpolation-based decoding of folded variants of linearized and skew Reed–Solomon codes. *Designs, Codes, and Cryptography*, 92(3):553–586, March 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01214-8`.

**Cheriere:2024:ERC**

[3099] Agathe Cheriere, Lina Mortajine, Tania Richmond, and Nadia El Mrabet. Exploiting ROLLO's constant-time implementations with a single-trace analysis. *Designs, Codes, and Cryptography*, 92(3):587–608, March 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01227-3`.

**Gruica:2024:DCV**

[3100] Anina Gruica, Anna-Lena Horlemann, Alberto Ravagnani, and Nadja Willenborg. Densities of codes of various linearity degrees in translation-invariant metric spaces. *Designs, Codes, and Cryptography*, 92(3):609–637, March 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01236-2`.

**Potapov:2024:ALB**

[3101] V. N. Potapov, A. A. Taranenko, and Yu. V. Tarannikov. An asymptotic lower bound on the number of bent functions. *Designs, Codes, and Cryptography*, 92(3):639–651, March 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01239-z`.

**Kavut:2024:MPW**

[3102] Selçuk Kavut. Modified Patterson–Wiedemann construction. *Designs, Codes, and Cryptography*, 92(3):653–666, March 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01248-y`.

**Guneri:2024:SSO**

[3103] Cem Güneri, Ferruh Özbudak, and Selcen Sayici. On subfield subcodes ob-

tained from restricted evaluation codes. *Designs, Codes, and Cryptography*, 92 (3):667–680, March 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01261-1`.

**Gologlu:2024:CNN**

[3104] Faruk Göloglu and Lukas Kölsch. Counting the number of non-isotopic Taniguchi semifields. *Designs, Codes, and Cryptography*, 92(3):681–694, March 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01262-0`.

**Graner:2024:CIP**

[3105] Anna-Maurin Graner and Gohar M. Kyureghyan. Constructing irreducible polynomials recursively with a reverse composition method. *Designs, Codes, and Cryptography*, 92(3):695–708, March 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01271-z`.

**Arce:2024:ACM**

[3106] Rafael Arce, Carlos Hernández, José Ortiz, Ivelisse Rubio, and Jaziel Torres. Analysis and computation of multidimensional linear complexity of periodic arrays. *Designs, Codes, and Cryptography*, 92(3):709–722, March 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01274-w`.

**David:2024:QID**

[3107] Nicolas David, María Naya-Plasencia, and André Schrottenloher. Quantum impossible differential attacks: applications to AES and SKINNY. *Designs, Codes, and Cryptography*, 92 (3):723–751, March 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01280-y`.

**Pratihar:2024:ATW**

[3108] Rakhi Pratihar and Tovohery Hajatiana Randrianarisoa. Antipodal two-weight rank metric codes. *Designs, Codes, and Cryptography*, 92 (3):753–769, March 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01283-9`.

**Munemasa:2024:CET**

[3109] Akihiro Munemasa and Rowena Alma L. Betty. Classification of extremal type II $\mathbf{Z}_4$-codes of length 24. *Designs, Codes, and Cryptography*, 92 (3):771–785, March 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01293-7`.

**Dastbasteh:2024:NQC**

[3110] Reza Dastbasteh and Petr Lisonek. New quantum codes from self-dual codes over $\mathbf{F}_4$. *Designs, Codes, and Cryptography*, 92(3):787–801, March 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https:`

//link.springer.com/article/10.1007/s10623-023-01306-5.

**Chailloux:2024:SOS**

[3111] André Chailloux and Simona Etinski. On the (in)security of optimized Stern-like signature schemes. *Designs, Codes, and Cryptography*, 92 (3):803–832, March 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01329-y.

**Reijnders:2024:HEC**

[3112] Krijn Reijnders, Simona Samardjiska, and Monika Trimoska. Hardness estimates of the code equivalence problem in the rank metric. *Designs, Codes, and Cryptography*, 92(3):833–862, March 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01338-x.

**Dutta:2024:INF**

[3113] Suman Dutta and Subhamoy Maitra. Introducing nega-Forrelation: quantum algorithms in analyzing nega-Hadamard and nega-crosscorrelation spectra. *Designs, Codes, and Cryptography*, 92(3):863–883, March 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01346-x.

**Yan:2024:MDS**

[3114] Qianqian Yan and Junling Zhou. Mutually disjoint Steiner systems from BCH codes. *Designs, Codes, and Cryptography*, 92(4):885–907, April 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01319-0.

**Ducas:2024:PLR**

[3115] Léo Ducas. Provable lattice reduction of $\mathbf{Z}^n$ with blocksize $n/2$. *Designs, Codes, and Cryptography*, 92 (4):909–916, April 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01320-7.

**Lyu:2024:LCL**

[3116] Shanxiang Lyu, Ling Liu, Cong Ling, Junzuo Lai, and Hao Chen. Lattice codes for lattice-based PKE. *Designs, Codes, and Cryptography*, 92 (4):917–939, April 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01321-6.

**Veitch:2024:USN**

[3117] Shannon Veitch and Douglas R. Stinson. Unconditionally secure non-malleable secret sharing and circular external difference families. *Designs, Codes, and Cryptography*, 92 (4):941–956, April 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01322-5.

**Lu:2024:IMM**

[3118] Jiqiang Lu and Wenchang Zhou. Improved meet-in-the-middle attack on 10 rounds of the AES-256 block cipher.

*Designs, Codes, and Cryptography*, 92 (4):957–973, April 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01323-4`.

**Wiese:2024:VAC**

[3119] Moritz Wiese and Holger Boche. $\varepsilon$-almost collision-flat universal hash functions and mosaics of designs. *Designs, Codes, and Cryptography*, 92 (4):975–998, April 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01324-3`.

**Bhunia:2024:EMZ**

[3120] Dipak K. Bhunia, Cristina Fernández-Córdoba, Carlos Vela, and Mercè Villanueva. On the equivalence of $\mathbf{Z}_{p^s}$-linear generalized Hadamard codes. *Designs, Codes, and Cryptography*, 92 (4):999–1022, April 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01325-2`.

**Bereg:2024:IBP**

[3121] Sergey Bereg, Mohammadreza Haghpanah, Brian Malouf, and I. Hal Sudborough. Improved bounds for permutation arrays under Chebyshev distance. *Designs, Codes, and Cryptography*, 92(4):1023–1039, April 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01326-1`.

**Miezaki:2024:JPH**

[3122] Tsuyoshi Miezaki and Akihiro Munemasa. Jacobi polynomials and harmonic weight enumerators of the first-order Reed–Muller codes and the extended Hamming codes. *Designs, Codes, and Cryptography*, 92(4):1041–1049, April 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01327-0`.

**Xu:2024:JSG**

[3123] Deng-Ming Xu, Gang Wang, Sihem Mesnager, You Gao, and Fang-Wei Fu. Jacobi sums over Galois rings of arbitrary characters and their applications in constructing asymptotically optimal codebooks. *Designs, Codes, and Cryptography*, 92(4):1051–1073, April 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01328-z`.

**Aragon:2024:LNR**

[3124] Nicolas Aragon, Victor Dyseryn, Philippe Gaborit, Pierre Loidreau, Julian Renner, and Antonia Wachter-Zeh. LowMS: a new rank metric code-based KEM without ideal structure. *Designs, Codes, and Cryptography*, 92 (4):1075–1093, April 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01330-5`.

**Xu:2024:HLC**

[3125] Guangkui Xu, Gaojun Luo, Xiwang Cao, and Heqian Xu. Hulls of lin-

ear codes from simplex codes. *Designs, Codes, and Cryptography*, 92 (4):1095–1112, April 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01331-4`.

**AlvesOliveira:2024:DPM**

[3126] José Alves Oliveira and F. E. Brochero Martínez. Dynamics of polynomial maps over finite fields. *Designs, Codes, and Cryptography*, 92 (5):1113–1125, May 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01332-3`.

**Kirshanova:2024:CDL**

[3127] Elena Kirshanova and Ekaterina Malygina. Construction-D lattice from Garcia–Stichtenoth tower code. *Designs, Codes, and Cryptography*, 92 (5):1127–1142, May 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01333-2`.

**Carvalho:2024:DNT**

[3128] Cícero Carvalho, Hiram H. López, and Gretchen L. Matthews. Decreasing norm-trace codes. *Designs, Codes, and Cryptography*, 92(5):1143–1161, May 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01334-1`.

**Chen:2024:NEA**

[3129] Xiaojing Chen, Xingbo Lu, Shixin Zhu, Wan Jiang, and Xindi Wang. New entanglement-assisted quantum error-correcting codes from negacyclic codes. *Designs, Codes, and Cryptography*, 92 (5):1163–1174, May 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01335-0`.

**Zhang:2024:OBN**

[3130] Lei Zhang. Observations on the branch number and differential analysis of SPEEDY. *Designs, Codes, and Cryptography*, 92(5):1175–1199, May 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01336-z`.

**Sahin:2024:CSW**

[3131] Mesut Sahin and Oguz Yayla. Codes on subgroups of weighted projective tori. *Designs, Codes, and Cryptography*, 92 (5):1201–1218, May 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01337-y`.

**Castellanos:2024:WSP**

[3132] Alonso S. Castellanos, Erik A. R. Mendoza, and Luciane Quoos. Weierstrass semigroups, pure gaps and codes on function fields. *Designs, Codes, and Cryptography*, 92(5):1219–1242, May 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01339-w`.

**Ban:2024:CSO**

[3133] Sara Ban and Sanja Rukavina. Construction of self-orthogonal $\mathbf{Z}_{2^k}$-codes. *Designs, Codes, and Cryptography*, 92 (5):1243–1250, May 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01340-3`.

**Zhang:2024:OBT**

[3134] Wenqin Zhang, Yuan Luo, and Lele Wang. Optimal binary and ternary locally repairable codes with minimum distance 6. *Designs, Codes, and Cryptography*, 92(5):1251–1265, May 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01341-2`.

**Yasunaga:2024:IBC**

[3135] Kenji Yasunaga. Improved bounds for codes correcting insertions and deletions. *Designs, Codes, and Cryptography*, 92(5):1267–1278, May 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01342-1`.

**Britz:2024:HTP**

[3136] Thomas Britz, Himadri Shekhar Chakraborty, Reina Ishikawa, Tsuyoshi Miezaki, and Hopein Christofen Tang. Harmonic Tutte polynomials of matroids II. *Designs, Codes, and Cryptography*, 92(5):1279–1297, May 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01343-0`.

**Stanovnik:2024:SMN**

[3137] Lidija Stanovnik, Miha Moskon, and Miha Mraz. In search of maximum non-overlapping codes. *Designs, Codes, and Cryptography*, 92 (5):1299–1326, May 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01344-z`.

**Chen:2024:CPR**

[3138] Ruikai Chen and Sihem Mesnager. On a class of permutation rational functions involving trace maps. *Designs, Codes, and Cryptography*, 92 (5):1327–1339, May 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01345-y`.

**Einsele:2024:ACE**

[3139] Semira Einsele and Kenneth Paterson. Average case error estimates of the strong Lucas test. *Designs, Codes, and Cryptography*, 92 (5):1341–1378, May 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01347-w`.

**Gavrilyuk:2024:SRG**

[3140] Alexander L. Gavrilyuk and Vladislav V. Kabanov. Strongly regular graphs decomposable into a divisible design graph and a Hoffman coclique. *Designs, Codes, and Cryptography*, 92

(5):1379–1391, May 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01348-9.

**Schoone:2024:SDC**

[3141] Jan Schoone and Joan Daemen. The state diagram of $\chi$. *Designs, Codes, and Cryptography*, 92(5):1393–1421, May 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01349-8.

**Li:2024:NCC**

[3142] Yun Li, Hongwei Liu, and Sihem Mesnager. New constructions of constant dimension subspace codes with large sizes. *Designs, Codes, and Cryptography*, 92(5):1423–1437, May 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01350-1.

**Kreitzer:2024:UAB**

[3143] Matthew Kreitzer, Mihai Nica, and Rajesh Pereira. Using alternating de Bruijn sequences to construct de Bruijn tori. *Designs, Codes, and Cryptography*, 92(5):1439–1454, May 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01351-0.

**Du:2024:IFM**

[3144] Xiaoni Du, René Rodríguez, and Hao Wu. Infinite families of minimal binary codes via Krawtchouk polynomials. *Designs, Codes, and Cryptography*, 92(6):1455–1475, June 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01353-y.

**Tseng:2024:PES**

[3145] Yi-Fan Tseng, Zi-Yuan Liu, and Raylin Tso. Predicate encryption with selective-opening security for receivers: formal definition, generic construction, and concrete instantiations for several primitives. *Designs, Codes, and Cryptography*, 92(6):1477–1500, June 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01354-x.

**Monroe:2024:OBS**

[3146] Laura Monroe. Optimal binary signed-digit representations of integers and the Stern polynomial. *Designs, Codes, and Cryptography*, 92(6):1501–1516, June 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-023-01355-w.

**Meng:2024:RCD**

[3147] Zhaoping Meng, Qingling Gao, and Zhanggui Wu. A recursive construction of doubly resolvable Steiner quadruple systems. *Designs, Codes, and Cryptography*, 92(6):1517–1531, June 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01356-3.

**Yan:2024:PEP**

[3148] Haode Yan and Yanan Yin. On the parameters of extended primitive cyclic codes and the related designs. *Designs, Codes, and Cryptography*, 92 (6):1533–1540, June 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01357-2.

**Lai:2024:LRI**

[3149] Qiqi Lai, Feng-Hao Liu, and Zhedong Wang. Leakage-resilient IBE/ABE with optimal leakage rates from lattices. *Designs, Codes, and Cryptography*, 92 (6):1541–1597, June 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01358-1.

**Roberts:2024:SDC**

[3150] Adam Michael Roberts. Self-dual codes from a block matrix construction characterised by group rings. *Designs, Codes, and Cryptography*, 92 (6):1599–1617, June 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01359-0.

**Singh:2024:LCA**

[3151] Kanchan Singh, Ritesh Kumar Pathak, and Sheo Kumar Singh. Linear codes associated to determinantal varieties in the space of Hermitian matrices. *Designs, Codes, and Cryptography*, 92 (6):1619–1635, June 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01360-7.

**Guo:2024:SIL**

[3152] Chun Guo, Yiyuan Luo, and Chenyu Xiao. On the sequential indifferentiability of the Lai–Massey construction. *Designs, Codes, and Cryptography*, 92 (6):1637–1661, June 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01361-6.

**Gong:2024:CMM**

[3153] Xinxin Gong, Yonglin Hao, and Qingju Wang. Combining MILP modeling with algebraic bias evaluation for linear mask search: improved fast correlation attacks on SNOW. *Designs, Codes, and Cryptography*, 92 (6):1663–1728, June 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01362-5.

**Chen:2024:CSG**

[3154] Yu-Chi Chen. A conceptually simple and generic construction of plaintext checkable encryption in the standard model. *Designs, Codes, and Cryptography*, 92(6):1729–1746, June 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01363-4.

**Romanov:2024:PMC**

[3155] Alexander M. Romanov. Perfect mixed codes from generalized Reed–Muller codes. *Designs,*

*Codes, and Cryptography*, 92(6):1747–1759, June 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01364-3`.

**Kunzweiler:2024:ECI**

[3156] S. Kunzweiler. Efficient computation of $(2^n, 2^n)$-isogenies. *Designs, Codes, and Cryptography*, 92(6):1761–1802, June 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01366-1`.

**Behajaina:2024:TSG**

[3157] Angelot Behajaina, Martino Borello, Javier de la Cruz, and Wolfgang Willems. Twisted skew $G$-codes. *Designs, Codes, and Cryptography*, 92(6):1803–1821, June 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01367-0`.

**Lin:2024:CMS**

[3158] Kaizhan Lin, Jianming Lin, Shiping Cai, Weize Wang, and Chang-An Zhao. Compressed M-SIDH: an instance of compressed SIDH-like schemes with isogenies of highly composite degrees. *Designs, Codes, and Cryptography*, 92(6):1823–1843, June 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01368-z`.

**Chen:2024:LHH**

[3159] Hao Chen. Large Hermitian hull GRS codes of any given length. *Designs, Codes, and Cryptography*, 92(7):1845–1853, July 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01369-y`.

**Yang:2024:ERG**

[3160] Hongna Yang, Yiwei Wang, and Yiwei Zhang. Extremal regular graphs and hypergraphs related to fractional repetition codes. *Designs, Codes, and Cryptography*, 92(7):1855–1878, July 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01370-5`.

**Qian:2024:MCG**

[3161] Liqin Qian, Xiwang Cao, Xia Wu, and Wei Lu. MDS codes with $l$-Galois hulls of arbitrary dimensions. *Designs, Codes, and Cryptography*, 92(7):1879–1902, July 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01371-4`.

**Boucher:2024:SCE**

[3162] Delphine Boucher and Kayodé Epiphane Nouetowa. Some constructions and existence conditions for Hermitian self-dual skew codes. *Designs, Codes, and Cryptography*, 92(7):1903–1924, July 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01372-3`.

**Phuong:2024:AAB**

[3163] Tran Viet Xuan Phuong. Anonymous attribute-based broadcast encryption with hidden multiple access structures. *Designs, Codes, and Cryptography*, 92 (7):1925–1945, July 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01373-2.

**Adiguzel-Goktas:2024:SRC**

[3164] Ebru Adiguzel-Goktas and Enver Ozdemir. Square root computation in finite fields. *Designs, Codes, and Cryptography*, 92(7):1947–1959, July 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01374-1.

**DAlconzo:2024:MIT**

[3165] Giuseppe D'Alconzo. Monomial isomorphism for tensors and applications to code equivalence problems. *Designs, Codes, and Cryptography*, 92 (7):1961–1982, July 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01375-0.

**Fuller:2024:IEI**

[3166] Benjamin Fuller. Impossibility of efficient information-theoretic fuzzy extraction. *Designs, Codes, and Cryptography*, 92(7):1983–2009, July 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01376-z.

**Wu:2024:BRC**

[3167] Rongsheng Wu and Xiande Zhang. Balanced reconstruction codes for single edits. *Designs, Codes, and Cryptography*, 92(7):2011–2029, July 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01377-y.

**Gan:2024:BDC**

[3168] Chunyu Gan, Chengju Li, Haifeng Qian, and Xueying Shi. On Bose distance of a class of BCH codes with two types of designed distances. *Designs, Codes, and Cryptography*, 92 (7):2031–2053, July 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01378-x.

**Tong:2024:ESM**

[3169] Yuxin Tong, Xiang Xie, Kang Yang, Rui Zhang, and Rui Xue. Efficient secure multi-party computation for proof of custody in Ethereum sharding. *Designs, Codes, and Cryptography*, 92 (7):2055–2083, July 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01379-w.

**Sun:2024:NBC**

[3170] Zhonghua Sun, Xinyue Liu, Shixin Zhu, and Yongsheng Tang. Negacyclic BCH codes of length $\frac{q^{2m}-1}{q+1}$ and their duals. *Designs, Codes, and Cryptography*, 92(7):2085–2101, July 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

URL https://link.springer.com/article/10.1007/s10623-024-01380-3.

**Guo:2024:CSC**

[3171] Chun Guo and Ling Song. CCA security for contracting (quasi-)Feistel constructions with tight round complexity. *Designs, Codes, and Cryptography*, 92 (8):2103–2129, August 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01394-x.

**Bettaieb:2024:PCS**

[3172] Slim Bettaieb, Loïc Bidoux, Victor Dyseryn, Andre Esser, Philippe Gaborit, Mukul Kulkarni, and Marco Palumbi. PERK: compact signature scheme based on a new variant of the permuted kernel problem. *Designs, Codes, and Cryptography*, 92 (8):2131–2157, August 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01381-2.

**Leung:2024:CSR**

[3173] Ka Hin Leung, Bernhard Schmidt, and Tao Zhang. Classification of semiregular relative difference sets with $\gcd(\lambda, n) = 1$ attaining Turyn's bound. *Designs, Codes, and Cryptography*, 92 (8):2159–2182, August 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01384-z.

**Monzillo:2024:CPO**

[3174] Giusy Monzillo, Tim Penttila, and Alessandro Siciliano. Classifying pseudo-ovals, translation generalized quadrangles, and elation Laguerre planes of small order. *Designs, Codes, and Cryptography*, 92(8):2183–2196, August 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01385-y.

**Baek:2024:PAR**

[3175] Seungjun Baek, Giyoon Kim, and Jongsung Kim. Preimage attacks on reduced-round Ascon–Xof. *Designs, Codes, and Cryptography*, 92 (8):2197–2217, August 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01383-0.

**Yu:2024:CQC**

[3176] Cong Yu, Shixin Zhu, and Fuyin Tian. Construction of quantum codes from multivariate polynomial rings. *Designs, Codes, and Cryptography*, 92 (8):2219–2234, August 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01387-w.

**Liu:2024:CCO**

[3177] Shuangqing Liu and Lijun Ji. Combinatorial constructions of optimal low-power error-correcting cooling codes. *Designs, Codes, and Cryptography*, 92 (8):2235–2252, August 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01391-0.

**Wang:2024:SDF**

[3178] Geyang Wang and Qi Wang. On the size distribution of the fixed-length Levenshtein balls with radius one. *Designs, Codes, and Cryptography*, 92 (8):2253–2265, August 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01382-1.

**Xu:2024:SOS**

[3179] Juanjuan Xu and Lijun Ji. Special overlarge sets of Kirkman triple systems. *Designs, Codes, and Cryptography*, 92(8):2267–2285, August 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01386-x.

**Bartoli:2024:OLD**

[3180] Daniele Bartoli, Nicola Durante, and Giovanni Giuseppe Grimaldi. Ovoids of $Q(6, q)$ of low degree. *Designs, Codes, and Cryptography*, 92(8):2287–2306, August 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01388-9.

**Yamaguchi:2024:JPF**

[3181] Ryosuke Yamaguchi. Jacobi polynomials for the first-order generalized Reed–Muller codes. *Designs, Codes, and Cryptography*, 92(8):2307–2321, August 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01392-z.

**He:2024:NCS**

[3182] Zhiwen He, Tingting Chen, and Gennian Ge. New constructions of signed difference sets. *Designs, Codes, and Cryptography*, 92(8):2323–2340, August 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01389-8.

**Schoone:2024:APM**

[3183] Jan Schoone and Joan Daemen. Algebraic properties of the maps $\chi_n$. *Designs, Codes, and Cryptography*, 92 (8):2341–2365, August 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01395-w.

**Kurz:2024:LDC**

[3184] Sascha Kurz. Lengths of divisible codes: the missing cases. *Designs, Codes, and Cryptography*, 92 (8):2367–2378, August 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01398-7.

**Bartz:2024:FDL**

[3185] Hannes Bartz and Sven Puchinger. Fast decoding of lifted interleaved linearized Reed–Solomon codes for multishot network coding. *Designs, Codes, and Cryptography*, 92(8):2379–2421, August 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01393-y.

**Dong:2024:MMA**

[3186] Xiaoli Dong, Jun Liu, Yongzhuang Wei, Wen Gao, and Jie Chen. Meet-in-the-middle attacks on AES with value constraints. *Designs, Codes, and Cryptography*, 92(9):2423–2449, September 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01396-9`.

**Adriaensen:2024:SWC**

[3187] Sam Adriaensen and Lins Denaux. Small weight codewords of projective geometric codes II. *Designs, Codes, and Cryptography*, 92(9):2451–2472, September 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01397-8`.

**Yang:2024:SAC**

[3188] Bo Yang, Kangkang He, Xiangyong Zeng, and Zibi Xiao. Symmetric 2-adic complexity of Tang–Gong interleaved sequences from generalized GMW sequence pair. *Designs, Codes, and Cryptography*, 92(9):2473–2489, September 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01399-6`.

**Amarra:2024:CIF**

[3189] Carmen Amarra, Alice Devillers, and Cheryl E. Praeger. Chain-imprimitive, flag-transitive 2-designs. *Designs, Codes, and Cryptography*, 92(9):2491–2510, September 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01400-2`.

**Acevedo:2024:NFQ**

[3190] Santiago Barrera Acevedo, Heiko Dietrich, and Corey Lionis. New families of quaternionic Hadamard matrices. *Designs, Codes, and Cryptography*, 92(9):2511–2525, September 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01401-1`.

**Davydov:2024:FRC**

[3191] Alexander A. Davydov, Stefano Marcugini, and Fernanda Pambianco. Further results on covering codes with radius $R$ and codimension $tR + 1$. *Designs, Codes, and Cryptography*, 92(9):2527–2548, September 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01402-0`.

**Galindo:2024:ORD**

[3192] C. Galindo, F. Hernando, and H. Martín-Cruz. Optimal $(r, \delta)$-LRCs from monomial-Cartesian codes and their subfield-subcodes. *Designs, Codes, and Cryptography*, 92(9):2549–2586, September 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01403-z`.

**Kiss:2024:SDF**

[3193] Gergely Kiss and Gábor Somlai. Special directions on the finite affine plane. *Designs, Codes,*

*and Cryptography*, 92(9):2587–2597, September 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01404-y`.

**Wang:2024:STP**

[3194] Xiaomeng Wang, Lina Wei, Shou-Jun Xu, and Sanming Zhou. Subgroup total perfect codes in Cayley sum graphs. *Designs, Codes, and Cryptography*, 92(9):2599–2613, September 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01405-x`.

**Muzychuk:2024:CLS**

[3195] Mikhail Muzychuk and Grigory Ryabov. Constructing linked systems of relative difference sets via Schur rings. *Designs, Codes, and Cryptography*, 92(9):2615–2637, September 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01406-w`.

**Pasalic:2024:UPP**

[3196] Enes Pasalic, Amar Bapić, Fengrong Zhang, and Yongzhuang Wei. Using $P_\tau$ property for designing bent functions provably outside the completed Maiorana–McFarland class. *Designs, Codes, and Cryptography*, 92(9):2639–2654, September 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01407-9`.

**Dong:2024:YAR**

[3197] Le Dong, Danxun Zhang, Wenya Li, and Wenling Wu. Yoyo attack on 4-round Lai–Massey scheme with secret round functions. *Designs, Codes, and Cryptography*, 92(9):2655–2684, September 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01408-8`.

**Hao:2024:OTL**

[3198] Jie Hao, Shu-Tao Xia, Kenneth W. Shum, Bin Chen, Fang-Wei Fu, and Yixian Yang. Optimal ternary locally repairable codes. *Designs, Codes, and Cryptography*, 92(9):2685–2704, September 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01409-7`.

**Xiao:2024:PDL**

[3199] Ang Xiao and Yue Zhou. On the packing density of Lee spheres. *Designs, Codes, and Cryptography*, 92(10):2705–2729, October 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01410-0`.

**Hyun:2024:CWR**

[3200] Jong Yoon Hyun, Jungyun Lee, and Yoonjin Lee. Characterization of weakly regular $p$-ary bent functions of $\ell$-form. *Designs, Codes, and Cryptography*, 92(10):2731–2741, October 2024. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01411-z.

**Chara:2024:LID**

[3201] María Chara, Ricardo Podestá, Luciane Quoos, and Ricardo Toledano. Lifting iso-dual algebraic geometry codes. *Designs, Codes, and Cryptography*, 92(10):2743–2767, October 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01412-y.

**Tian:2024:CGS**

[3202] Song Tian. Computing gluing and splitting $(\ell, \ell)$-isogenies. *Designs, Codes, and Cryptography*, 92(10):2769–2789, October 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01413-x.

**Kharaghani:2024:OCW**

[3203] Hadi Kharaghani, Thomas Pender, and Vladimir Tonchev. On optimal constant weight codes derived from $\omega$-circulant balanced generalized weighing matrices. *Designs, Codes, and Cryptography*, 92(10):2791–2799, October 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01414-w.

**Berardini:2024:SCC**

[3204] Elena Berardini, Alessio Caminata, and Alberto Ravagnani. Structure of CSS and CSS-T quantum codes. *Designs, Codes, and Cryptography*, 92(10):2801–2823, October 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01415-9.

**Imran:2024:EQA**

[3205] Muhammad Imran and Gábor Ivanyos. Efficient quantum algorithms for some instances of the semidirect discrete logarithm problem. *Designs, Codes, and Cryptography*, 92(10):2825–2843, October 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01416-8.

**Yu:2024:DFC**

[3206] Wenjun Yu and Moshe Schwartz. On duplication-free codes for disjoint or equal-length errors. *Designs, Codes, and Cryptography*, 92(10):2845–2861, October 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01417-7.

**Hall:2024:BDL**

[3207] Joanne Hall, Daniel Horsley, and Douglas R. Stinson. Bounds on data limits for all-to-all comparison from combinatorial designs. *Designs, Codes, and Cryptography*, 92(10):2863–2879, October 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01418-6.

**Rajpurohit:2024:LMR**

[3208] Rajendra Prasad Rajpurohit, Maheshanand Bhaintwal, and Charul Rajput. Locally maximal recoverable codes and LMR–LCD codes. *Designs, Codes, and Cryptography*, 92(10):2881–2899, October 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01419-5`.

**Wang:2024:LCA**

[3209] Xinran Wang, Ziling Heng, Fengwei Li, and Qin Yue. LCD codes and almost optimally extendable codes from self-orthogonal codes. *Designs, Codes, and Cryptography*, 92(10):2901–2926, October 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01420-y`.

**Harada:2024:MCQ**

[3210] Masaaki Harada. A method for constructing quaternary Hermitian self-dual codes and an application to quantum codes. *Designs, Codes, and Cryptography*, 92(10):2927–2948, October 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01421-x`.

**Jiang:2024:CSM**

[3211] Jing Jiang, Fenggui Pei, Cailin Wen, Minquan Cheng, and Henk D. L. Hollmann. Constructions of $t$-strongly multimedia IPP codes with length $t + 1$. *Designs, Codes, and Cryptography*, 92(10):2949–2970, October 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01422-w`.

**Qiu:2024:SNC**

[3212] Jing Qiu and Fang-Wei Fu. Some new constructions of optimal linear codes and alphabet-optimal $(r, \delta)$-locally repairable codes. *Designs, Codes, and Cryptography*, 92(10):2971–2991, October 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01423-9`.

**Liu:2024:LCS**

[3213] Hongwei Liu and Zihao Yu. Linear codes from simplicial complexes over $\mathbf{F}_{2^n}$. *Designs, Codes, and Cryptography*, 92(10):2993–3016, October 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01424-8`.

**Jiang:2024:POS**

[3214] Yupeng Jiang, Ming Li, Ying Gao, and Dongdai Lin. On prefer-one sequences. *Designs, Codes, and Cryptography*, 92(10):3017–3032, October 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01425-7`.

**Navarro:2024:BRR**

[3215] Horacio Navarro. Bases for Riemann–Roch spaces of linearized function fields

with applications to generalized algebraic geometry codes. *Designs, Codes, and Cryptography*, 92(10):3033–3048, October 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01426-6.

**Araya:2024:CSH**

[3216] Makoto Araya, Masaaki Harada, Hadi Kharaghani, Ali Mohammadian, and Behruz Tayfeh-Rezaie. On the classification of skew Hadamard matrices of order **36** and related structures. *Designs, Codes, and Cryptography*, 92(10):3049–3062, October 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01427-5.

**Quan:2024:HCC**

[3217] Xiaoshan Quan, Qin Yue, and Fuqing Sun. Hulls of cyclic codes with respect to the regular permutation inner product. *Designs, Codes, and Cryptography*, 92(10):3063–3083, October 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01428-4.

**Schage:2024:TPK**

[3218] Sven Schäge. TOPAS 2-pass key exchange with full perfect forward secrecy and optimal communication complexity. *Designs, Codes, and Cryptography*, 92(10):3085–3124, October 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01429-3.

**Steinerberger:2024:NAH**

[3219] Stefan Steinerberger. A note on approximate Hadamard matrices. *Designs, Codes, and Cryptography*, 92(10):3125–3131, October 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01430-w.

**Martinez:2024:NRP**

[3220] F. E. Brochero Martínez and Daniela Oliveira. On the number of rational points of Artin–Schreier's curves and hypersurfaces. *Designs, Codes, and Cryptography*, 92(10):3133–3154, October 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01431-9.

**Datta:2024:CFU**

[3221] Pratish Datta, Tapas Pal, and Katsuyuki Takashima. Compact FE for unbounded attribute-weighted sums for logspace from SXDH. *Designs, Codes, and Cryptography*, 92(10):3155–3235, October 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01432-8.

**Li:2024:SCB**

[3222] Jin Li, Huilian Zhu, and Shan Huang. Some constacyclic BCH codes with good parameters. *Designs,*

*Codes, and Cryptography*, 92(10):3237–3259, October 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01433-7`.

**Choi:2024:ZFO**

[3223] Wonseok Choi, Seongha Hwang, Byeonghak Lee, and Jooyoung Lee. ZLR: a fast online authenticated encryption scheme achieving full security. *Designs, Codes, and Cryptography*, 92(10):3261–3316, October 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01434-6`.

**Gonzalez-Sarabia:2024:IFN**

[3224] Manuel González-Sarabia, Humberto Muñoz-George, Jorge A. Ordaz, Eduardo Sáenz de Cabezón, and Rafael H. Villarreal. Indicator functions, $v$-numbers and Gorenstein rings in the theory of projective Reed–Muller-type codes. *Designs, Codes, and Cryptography*, 92(11):3317–3353, November 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01437-3`.

**Kschischang:2024:ECM**

[3225] F. R. Kschischang, F. Manganiello, A. Ravagnani, and K. Savary. External codes for multiple unicast networks via interference alignment. *Designs, Codes, and Cryptography*, 92(11):3355–3369, November 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01439-1`.

**Bierbrauer:2024:APQ**

[3226] Jürgen Bierbrauer, Stefano Marcugini, and Fernanda Pambianco. An asymptotic property of quaternary additive codes. *Designs, Codes, and Cryptography*, 92(11):3371–3375, November 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01438-2`.

**Wu:2024:CED**

[3227] Huawei Wu, Jing Yang, and Keqin Feng. Circular external difference families: construction and non-existence. *Designs, Codes, and Cryptography*, 92(11):3377–3390, November 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01443-5`.

**Canales-Martinez:2024:MCA**

[3228] Isaac A. Canales-Martínez and Igor Semaev. Multivariate correlation attacks and the cryptanalysis of LFSR-based stream ciphers. *Designs, Codes, and Cryptography*, 92(11):3391–3427, November 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01444-4`.

**Ming:2024:EMZ**

[3229] Xinyue Ming, Tao Feng, Guojing Jia, and Xiaomiao Wang. The

existence of $(\mathbf{Z}_v, 4, 1)$-disjoint difference families. *Designs, Codes, and Cryptography*, 92(11):3429–3446, November 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01442-6`.

**Arpin:2024:FOS**

[3230] Sarah Arpin, James Clements, Pierrick Dartois, Jonathan Komada Eriksen, Péter Kutas, and Benjamin Wesolowski. Finding orientations of supersingular elliptic curves and quaternion orders. *Designs, Codes, and Cryptography*, 92(11):3447–3493, November 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01435-5`.

**Gupta:2024:AVS**

[3231] Somi Gupta and Francesco Pavese. Affine vector space partitions and spreads of quadrics. *Designs, Codes, and Cryptography*, 92(11):3495–3502, November 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01447-1`.

**vanTrung:2024:CDR**

[3232] Tran van Trung. Constructions for $t$-designs and $s$-resolvable $t$-designs. *Designs, Codes, and Cryptography*, 92(11):3503–3514, November 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01448-0`. See retraction notice [3289].

**Chung:2024:SAI**

[3233] Woohyuk Chung, Hwigyeom Kim, Jooyoung Lee, and Yeongmin Lee. Security analysis of the ISO standard OFB–DRBG. *Designs, Codes, and Cryptography*, 92(11):3515–3532, November 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01449-z`.

**Pan:2024:SSD**

[3234] Xu Pan, Hao Chen, and Hongwei Liu. Some self-dual codes and isodual codes constructed by matrix product codes. *Designs, Codes, and Cryptography*, 92(11):3533–3559, November 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01453-3`.

**Buratti:2024:ASS**

[3235] Marco Buratti and Anamari Nakić. Additivity of symmetric and subspace 2-designs. *Designs, Codes, and Cryptography*, 92(11):3561–3572, November 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01452-4`.

**Han:2024:ECN**

[3236] Dongchun Han and Hanbin Zhang. Explicit constructions of NMDS self-dual codes. *Designs, Codes, and Cryptography*, 92(11):3573–3585, November 2024. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01450-6.

**Katsumata:2024:COI**

[3237] Shuichi Katsumata, Yi-Fu Lai, Jason T. LeGrow, and Ling Qin. CSI-Otter: isogeny-based (partially) blind signatures from the class group action with a twist. *Designs, Codes, and Cryptography*, 92(11):3587–3643, November 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01441-7.

**Matthews:2024:CLC**

[3238] Gretchen L. Matthews, Travis Morrison, and Aidan W. Murphy. Curve-lifted codes for local recovery using lines. *Designs, Codes, and Cryptography*, 92(11):3645–3664, November 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01456-0.

**Goryainov:2024:NCM**

[3239] Sergey Goryainov and Elena V. Konstantinova. Non-canonical maximum cliques without a design structure in the block graphs of 2-designs. *Designs, Codes, and Cryptography*, 92(11):3665–3675, November 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01459-x.

**Masip-Ardevol:2024:EES**

[3240] Héctor Masip-Ardevol, Jordi Baylina-Melé, Marc Guzmán-Albiol, and Jose Luis Muñoz-Tapia. eSTARK: extending STARKs with arguments. *Designs, Codes, and Cryptography*, 92(11):3677–3721, November 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01457-z.

**Li:2024:NIF**

[3241] Yang Li, Shitao Li, and Shixin Zhu. New and improved formally self-dual codes with small hulls from polynomial four Toeplitz codes. *Designs, Codes, and Cryptography*, 92(11):3723–3751, November 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01460-4.

**Wang:2024:SAP**

[3242] Bolin Wang and Wenling Wu. Security analysis of P-SPN schemes against invariant subspace attack with inactive S-boxes. *Designs, Codes, and Cryptography*, 92(11):3753–3782, November 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01465-z.

**Li:2024:MAC**

[3243] Lei Li, Xinchun Yu, Chenhao Ying, Liang Chen, Yuanyuan Dong, and Yuan Luo. MDS array codes with efficient repair and small sub-packetization level. *Designs, Codes, and Cryptography*, 92(11):3783–3798, November 2024. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01440-8.

**Yu:2024:TNC**

[3244] Shuhui Yu and Lijun Ji. Two new constructions of cyclic subspace codes via Sidon spaces. *Designs, Codes, and Cryptography*, 92(11):3799–3811, November 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01466-y.

**Lv:2024:UFL**

[3245] Yin Lv, Danping Shi, Lei Hu, and Yi Guo. Utilizing FWT in linear cryptanalysis of block ciphers with various structures. *Designs, Codes, and Cryptography*, 92(11):3813–3842, November 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01458-y.

**Huang:2024:CKE**

[3246] Huawei Huang, Changgen Peng, and Lunzhi Deng. Cryptanalysis of a key exchange protocol based on a modified tropical structure. *Designs, Codes, and Cryptography*, 92(11):3843–3858, November 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01469-9.

**Li:2024:TCP**

[3247] Yi Li, Xiutao Feng, and Qiang Wang. Towards a classification of permutation binomials of the form $x^i + ax$ over $\mathbf{F}_{2^n}$. *Designs, Codes, and Cryptography*, 92(12):3859–3875, December 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01462-2.

**Guan:2024:RBT**

[3248] Haiyan Guan and Shenglin Zhou. Reduction for block-transitive $t$–$(k^2, k, \lambda)$ designs. *Designs, Codes, and Cryptography*, 92(12):3877–3894, December 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01477-9.

**Bai:2024:AAB**

[3249] Shi Bai, Hansraj Jangir, Tran Ngo, and William Youmans. An algebraic algorithm for breaking NTRU with multiple keys. *Designs, Codes, and Cryptography*, 92(12):3895–3918, December 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01473-z.

**Sha:2024:FCA**

[3250] Jinrui Sha, Shengli Liu, and Shuai Han. Functional commitments for arbitrary circuits of bounded sizes. *Designs, Codes, and Cryptography*, 92(12):3919–3953, December 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01468-w.

**Gao:2024:OLR**

[3251] Yuan Gao, Weijun Fang, Jingke Xu, Dong Wang, and Sihuang Hu. Optimal $(2, \delta)$ locally repairable codes via punctured simplex codes. *Designs, Codes, and Cryptography*, 92(12):3955–3979, December 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01470-2`.

**Ozbudak:2024:NDB**

[3252] Ferruh Özbudak and Buket Özkaya. New distance bounds for quasi-cyclic codes. *Designs, Codes, and Cryptography*, 92(12):3981–4009, December 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01464-0`.

**Agrawal:2024:BFD**

[3253] Deepak Agrawal, Srinivasan Krishnaswamy, and Smarajit Das. On Boolean functions derived from linear maps over $\mathbf{Z}_4$ and their application to secret sharing. *Designs, Codes, and Cryptography*, 92(12):4011–4033, December 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01478-8`.

**Aranov:2024:MSU**

[3254] Noy Soffer Aranov and Angelot Behajaina. On the maximum size of ultrametric orthogonal sets over discrete valued fields. *Designs, Codes, and Cryptography*, 92(12):4035–4055, December 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01480-0`.

**Subroto:2024:AAC**

[3255] Robert Christian Subroto. An algebraic approach to circulant column parity mixers. *Designs, Codes, and Cryptography*, 92(12):4057–4083, December 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01476-w`.

**Cil:2024:CCO**

[3256] Melek Çil and Baris Bülent Kirlar. On the construction of certain odd degree irreducible polynomials over finite fields. *Designs, Codes, and Cryptography*, 92(12):4085–4097, December 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01479-7`.

**Zhao:2024:TBA**

[3257] Feixiang Zhao, Jian Weng, Wenli Xie, Lin Hou, and Ming Li. Time-based attribute-based proxy re-encryption with decryption key update. *Designs, Codes, and Cryptography*, 92(12):4099–4129, December 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01467-x`.

**Masson:2024:BFE**

[3258] Simon Masson, Antonio Sanso, and Zhenfei Zhang. Bandersnatch: a

fast elliptic curve built over the BLS12-381 scalar field. *Designs, Codes, and Cryptography*, 92(12):4131–4143, December 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01472-0`.

**Barg:2024:SCR**

[3259] Alexander Barg, Ohad Elishco, Ryan Gabrys, Geyang Wang, and Eitan Yaakobi. Storage codes and recoverable systems on lines and grids. *Designs, Codes, and Cryptography*, 92(12):4145–4168, December 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01481-z`.

**Gao:2024:UBC**

[3260] Yiwen Gao, Yuan Li, and Haibin Kan. On the uniqueness of balanced complex orthogonal design. *Designs, Codes, and Cryptography*, 92(12):4169–4187, December 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01483-x`.

**Furedi:2024:MAP**

[3261] Zoltán Füredi, Alexandr Kostochka, and Mohit Kumbhat. Minimal abundant packings and choosability with separation. *Designs, Codes, and Cryptography*, 92(12):4189–4194, December 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01484-w`.

**Durante:2024:NLM**

[3262] Nicola Durante, Giovanni Giuseppe Grimaldi, and Giovanni Longobardi. Non-linear MRD codes from cones over exterior sets. *Designs, Codes, and Cryptography*, 92(12):4195–4211, December 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01492-w`.

**Shen:2024:AOA**

[3263] Bingsheng Shen, Tao Yu, Zhengchun Zhou, and Yang Yang. Asymptotically optimal aperiodic quasi-complementary sequence sets based on extended Boolean functions. *Designs, Codes, and Cryptography*, 92(12):4213–4230, December 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01501-y`. See correction [3316].

**Gunasekara:2024:TPD**

[3264] Ajani De Vas Gunasekara and Alice Devillers. Transitive path decompositions of Cartesian products of complete graphs. *Designs, Codes, and Cryptography*, 92(12):4231–4245, December 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01493-9`.

**Sasidharan:2024:BCG**

[3265] Birenjith Sasidharan, Emanuele Viterbo, and Son Hoang Dau. Binary cyclic-gap constant weight codes with low-complexity encoding and decoding.

*Designs, Codes, and Cryptography*, 92(12):4247–4277, December 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01494-8`.

**Ding:2024:TCE**

[3266] Zhiguo Ding and Michael E. Zieve. Two classes of exceptional $m$-to-1 rational functions. *Designs, Codes, and Cryptography*, 92(12):4279–4285, December 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01499-3`.

**Pan:2024:GCJ**

[3267] Yingyin Pan, Jianghua Zhong, and Dongdai Lin. Generalized cycle joining method and its application to the construction of long-period Galois NFSRs. *Designs, Codes, and Cryptography*, 92(12):4287–4311, December 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01500-z`.

**Matszangosz:2024:CCH**

[3268] Ákos K. Matszangosz and Ferenc Szöllősi. A characterization of complex Hadamard matrices appearing in families of MUB triplets. *Designs, Codes, and Cryptography*, 92(12):4313–4333, December 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01503-w`.

**Luo:2024:AOD**

[3269] Rong Luo, Mingliang Yan, Sihem Mesnager, and Dongchun Han. On Abelian one-dimensional hull codes in group algebras. *Designs, Codes, and Cryptography*, 92(12):4335–4352, December 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01504-9`.

**Wei:2024:ASA**

[3270] Yadi Wei, Jiaxin Wang, and Fang-Wei Fu. Association schemes arising from non-weakly regular bent functions. *Designs, Codes, and Cryptography*, 92(12):4353–4422, December 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01495-7`.

**Minematsu:2024:IAM**

[3271] Kazuhiko Minematsu, Shingo Sato, and Junji Shikata. Interactive aggregate message authentication equipped with detecting functionality from adaptive group testing. *Designs, Codes, and Cryptography*, 92(12):4423–4451, December 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01498-4`.

**Mao:2024:QSP**

[3272] Shuping Mao, Tingting Guo, Peng Wang, Ruozhou Xu, Yuchao Chen, and Lei Hu. A quantum-secure partial parallel MAC QPCBC. *Designs,*

*Codes, and Cryptography*, 92(12):4453–4486, December 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01506-7`.

**Xu:2024:IFD**

[3273] Guangkui Xu, Xiwang Cao, Gaojun Luo, and Huawei Wu. Infinite families of 3-designs from special symmetric polynomials. *Designs, Codes, and Cryptography*, 92(12):4487–4509, December 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01508-5`.

**Aguilar-Melchor:2024:EEC**

[3274] Carlos Aguilar-Melchor, Nicolas Aragon, Jean-Christophe Deneuville, Philippe Gaborit, Jérôme Lacan, and Gilles Zémor. Efficient error-correcting codes for the HQC post-quantum cryptosystem. *Designs, Codes, and Cryptography*, 92(12):4511–4530, December 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01507-6`.

**Luo:2024:CPC**

[3275] Shuyu Luo, Weiqiong Wang, Qi Zhang, and Zhenjie Song. Constructions of plateaued correctors with high correction order and good nonlinearity via Walsh spectral neutralization technique. *Designs, Codes, and Cryptography*, 92(12):4531–4548, December 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01497-5`.

**Ahmadian:2024:TDC**

[3276] Zahra Ahmadian, Akram Khalesi, Dounia M'foukh, Hossein Moghimi, and María Naya-Plasencia. Truncated differential cryptanalysis: new insights and application to QARMAv1-$n$ and QARMAv2-64. *Designs, Codes, and Cryptography*, 92(12):4549–4591, December 2024. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01486-8`.

**Mavron:2025:DCT**

[3277] Vassili C. Mavron and Harold N. Ward. Designer of codes: a tribute to Jennifer Key. *Designs, Codes, and Cryptography*, 93(1):1–10, January 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01517-4`.

**Wang:2025:SRP**

[3278] Xiang Wang, Fang-Wei Fu, and Elena V. Konstantinova. The sequence reconstruction of permutations with Hamming metric. *Designs, Codes, and Cryptography*, 93(1):11–37, January 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01509-4`.

**Beierle:2025:RPF**

[3279] Christof Beierle. Revisiting products of the form $X$ times a lin-

earized polynomial $L(X)$. *Designs, Codes, and Cryptography*, 93(1):39–50, January 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01511-w.

**Chan:2025:DEP**

[3280] Chin Hei Chan, Fang-Wei Fu, and Maosheng Xiong. Decoding error probability of random parity-check matrix ensemble over the erasure channel. *Designs, Codes, and Cryptography*, 93(1):51–77, January 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01516-5.

**Dastbasteh:2025:ECC**

[3281] Reza Dastbasteh, Farzad Padashnick, Pedro M. Crespo, Markus Grassl, and Javad Sharafi. Equivalence of constacyclic codes with shift constants of different orders. *Designs, Codes, and Cryptography*, 93(1):79–93, January 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01512-9.

**Alvarez-Garcia:2025:DCG**

[3282] Cain Álvarez-García, Carlos Alberto Castillo-Guillén, Mohamed Badaoui, and Andriy Kryvko. DNA codes over groups. *Designs, Codes, and Cryptography*, 93(1):95–110, January 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01515-6.

**Haymaker:2025:AHL**

[3283] Kathryn Haymaker, Beth Malmskog, and Gretchen Matthews. Algebraic hierarchical locally recoverable codes with nested affine subspace recovery. *Designs, Codes, and Cryptography*, 93(1):111–132, January 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01510-x.

**Suryawanshi:2025:SVV**

[3284] Sahiba Suryawanshi, Shibam Ghosh, Dhiman Saha, and Prathamesh Ram. Simple vs. vectorial: exploiting structural symmetry to beat the ZeroSum distinguisher. *Designs, Codes, and Cryptography*, 93(1):133–174, January 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01502-x.

**Ball:2025:GTB**

[3285] Simeon Ball, Michel Lavrauw, and Tabriz Popatia. Griesmer type bounds for additive codes over finite fields, integral and fractional MDS codes. *Designs, Codes, and Cryptography*, 93(1):175–196, January 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01519-2. See correction [3462].

**Hong:2025:GBM**

[3286] Xiaoqin Hong, Xiwang Cao, and Gaojun Luo. Generalized bilateral multilevel construction for constant dimension codes. *Designs,*

*Codes, and Cryptography*, 93(1):197–225, January 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01513-8`.

**He:2025:PCC**

[3287] Xianmang He, Zusheng Zhang, Si Tian, Jingli Wang, and Yindong Chen. Parallel construction for constant dimension codes from mixed dimension construction. *Designs, Codes, and Cryptography*, 93(1):227–241, January 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01518-3`.

**Dey:2025:IKR**

[3288] Sabyasachi Dey, Gregor Leander, and Nitin Kumar Sharma. Improved key recovery attacks on reduced-round Salsa20. *Designs, Codes, and Cryptography*, 93(1):243–262, January 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01522-7`.

**vanTrung:2025:RNC**

[3289] Tran van Trung. Retraction note: Constructions for $t$-designs and $s$-resolvable $t$-designs. *Designs, Codes, and Cryptography*, 93(1):263, January 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01521-8`. See [3232].

**Cardinali:2025:FG**

[3290] Ilaria Cardinali, Michel Lavrauw, Klaus Metsch, and Alexander Pott. Finite geometries. *Designs, Codes, and Cryptography*, 93(2):265–266, February 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01530-7`.

**Alnajjarine:2025:CPI**

[3291] Nour Alnajjarine and Michel Lavrauw. A classification of planes intersecting the Veronese surface over finite fields of even order. *Designs, Codes, and Cryptography*, 93(2):267–296, February 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01194-9`.

**Faulkner:2025:ESF**

[3292] Jake Faulkner and Geertrui Van de Voorde. On the equivalence, stabilisers, and feet of Buekenhout–Tits unitals. *Designs, Codes, and Cryptography*, 93(2):297–307, February 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01234-4`.

**Abdukhalikov:2025:LCA**

[3293] Kanat Abdukhalikov and Duy Ho. Linear codes from arcs and quadrics. *Designs, Codes, and Cryptography*, 93(2):309–329, February 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01255-z`.

**Bamberg:2025:AVS**

[3294] John Bamberg, Yuval Filmus, Ferdinand Ihringer, and Sascha Kurz. Affine vector space partitions. *Designs, Codes, and Cryptography*, 93 (2):331–357, February 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01263-z`.

**Kurz:2025:GA**

[3295] Sascha Kurz, Ivan Landjev, Francesco Pavese, and Assia Rousseva. The geometry of $(t \bmod q)$-arcs. *Designs, Codes, and Cryptography*, 93(2):359–372, February 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01290-w`.

**Landjev:2025:STN**

[3296] Ivan Landjev and Emiliyan Rogachev. Sperner's theorem for non-free modules over finite chain rings. *Designs, Codes, and Cryptography*, 93 (2):373–390, February 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01352-z`.

**Bruyn:2025:FQS**

[3297] Bart De Bruyn. Families of quadratic sets on the Klein quadric. *Designs, Codes, and Cryptography*, 93 (2):391–407, February 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01390-1`.

**Kurz:2025:CIF**

[3298] Sascha Kurz. Capacity of an infinite family of networks related to the diamond network for fixed alphabet sizes. *Designs, Codes, and Cryptography*, 93 (2):409–421, February 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01485-9`.

**Gyarmati:2025:CHS**

[3299] Máté Gyarmati, Péter Ligeti, Peter Sziklai, and Marcella Takáts. Conjunctive hierarchical secret sharing by finite geometry. *Designs, Codes, and Cryptography*, 93(2):423–428, February 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01496-6`.

**Allen:2025:THS**

[3300] Kevin Allen and John Sheekey. On translation hyperovals in semifield planes. *Designs, Codes, and Cryptography*, 93(2):429–442, February 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01533-4`.

**Su:2025:NMC**

[3301] Sihong Su and Xiaoyan Chen. A new method of constructing $(k+s)$-variable bent functions based on a family of $s$-plateaued functions on $k$ variables. *Designs, Codes, and Cryptography*, 93 (3):443–465, March 2025. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01520-9.

**Giusto:2025:BPT**

[3302] Andrea Di Giusto and Chiara Marcolla. Breaking the power-of-two barrier: noise estimation for BGV in NTT-friendly rings. *Designs, Codes, and Cryptography*, 93(3):467–502, March 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01524-5.

**Wang:2025:ATS**

[3303] Zhedong Wang, Qiqi Lai, and Feng-Hao Liu. Almost tight security in lattices with polynomial moduli-PRF, IBE, all-but-many LTF, and more. *Designs, Codes, and Cryptography*, 93(3):503–551, March 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01523-6.

**Xu:2025:QRA**

[3304] Yin-Song Xu, Yi-Bo Luo, Zheng Yuan, Xuan Zhou, Qi di You, Fei Gao, and Xiao-Yang Dong. Quantum rectangle attack and its application on Deoxys–BC. *Designs, Codes, and Cryptography*, 93(3):553–590, March 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01526-3.

**Kolsch:2025:FIC**

[3305] Lukas Kölsch, Lucas Krompholz, and Gohar Kyureghyan. Factorization and irreducibility of composed products. *Designs, Codes, and Cryptography*, 93(3):591–614, March 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01529-0.

**Xu:2025:DDC**

[3306] Li Xu, Cuiling Fan, Chunming Tang, and Zhengchun Zhou. Derivative descendants of cyclic codes and constacyclic codes. *Designs, Codes, and Cryptography*, 93(3):615–632, March 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01536-1.

**Freed:2025:CTS**

[3307] Josline Freed. Codes over $\mathbf{F}_4$ and $\mathbf{F}_2 \times \mathbf{F}_2$ and theta series of the corresponding lattices in quadratic fields. *Designs, Codes, and Cryptography*, 93(3):633–644, March 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01537-0.

**Yu:2025:POO**

[3308] Shikang Yu, Tao Feng, and Menglong Zhang. A pair of orthogonal orthomorphisms of finite nilpotent groups. *Designs, Codes, and Cryptography*, 93(3):645–665, March 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01540-5.

**Wei:2025:SSS**

[3309] Xin Wei, Xiande Zhang, and Gennian Ge. On set systems with strongly restricted intersections. *Designs, Codes, and Cryptography*, 93 (3):667–682, March 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01535-2.

**Kaplan:2025:HPR**

[3310] Nathan Kaplan and Jon-Lark Kim. Hulls of projective Reed–Muller codes. *Designs, Codes, and Cryptography*, 93 (3):683–699, March 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01543-2.

**Bennett:2025:RCE**

[3311] Huck Bennett and Kaung Myat Htay Win. Relating code equivalence to other isomorphism problems. *Designs, Codes, and Cryptography*, 93 (3):701–723, March 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01542-3.

**Zheng:2025:OCN**

[3312] Xingyu Zheng, Shukai Wang, and Cuiling Fan. Optimal combinatorial neural codes via symmetric designs. *Designs, Codes, and Cryptography*, 93 (3):725–736, March 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01534-3.

**Xu:2025:QST**

[3313] Ying Xu, Xiaoni Du, and Jian Zou. Quantum security of Trojan message attacks on Merkle–Damgård hash construction. *Designs, Codes, and Cryptography*, 93 (3):737–768, March 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01538-z.

**Wu:2025:SNC**

[3314] Gaofei Wu, Zhuohui You, Zhengbang Zha, and Yuqing Zhang. Several new classes of optimal ternary cyclic codes with two or three zeros. *Designs, Codes, and Cryptography*, 93 (3):769–786, March 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01541-4.

**Canale:2025:GLB**

[3315] Federico Canale and María Naya-Plasencia. Guessing less and better: improved attacks on GIFT-64. *Designs, Codes, and Cryptography*, 93 (3):787–822, March 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01527-2.

**Shen:2025:CAO**

[3316] Bingsheng Shen, Tao Yu, Zhengchun Zhou, and Yang Yang. Correction: Asymptotically optimal aperiodic quasi-complementary sequence sets based on extended Boolean functions. *Designs, Codes, and Cryptography*, 93(3):823, March 2025. CODEN

DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01578-z. See [3263].

**Jedwab:2025:SCB**

[3317] Jonathan Jedwab, Alexander Pott, and Yue Zhou. Sequences, codes, and Boolean functions: in memory of Kai-Uwe Schmidt. *Designs, Codes, and Cryptography*, 93(4):825–829, April 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01612-0.

**Wang:2025:SCI**

[3318] Qiang Wang. A survey of compositional inverses of permutation polynomials over finite fields. *Designs, Codes, and Cryptography*, 93(4):831–870, April 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01436-4.

**Wang:2025:MSV**

[3319] Geyang Wang and Qi Wang. On the maximum size of variable-length non-overlapping codes. *Designs, Codes, and Cryptography*, 93(4):871–878, April 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01445-3.

**Davis:2025:NSD**

[3320] James A. Davis, John Polhill, Ken Smith, Eric Swartz, and Jordan Webster. New Spence difference sets. *Designs, Codes, and Cryptography*, 93(4):879–888, April 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01446-2.

**delaCruz:2025:ALG**

[3321] Javier de la Cruz and Wolfgang Willems. Around LCD group codes. *Designs, Codes, and Cryptography*, 93(4):889–897, April 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01451-5.

**Anbar:2025:VNC**

[3322] Nurdagül Anbar, Sadmir Kudin, Wilfried Meidl, Enes Pasalic, and Alexandr Polujan. Vectorial negabent concepts: similarities, differences, and generalizations. *Designs, Codes, and Cryptography*, 93(4):899–921, April 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01454-2.

**Coulter:2025:CFT**

[3323] Robert S. Coulter and Bradley Fain. A class of functions and their application in constructing semisymmetric designs. *Designs, Codes, and Cryptography*, 93(4):923–935, April 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01455-1.

**Helleseth:2025:IPL**

[3324] Tor Helleseth, Chunlei Li, and Yongbo Xia. Investigation of the permutation and linear codes from the Welch APN function. *Designs, Codes, and Cryptography*, 93(4):937–959, April 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01461-3`.

**Kolsch:2025:CMB**

[3325] Lukas Kölsch and Gohar Kyureghyan. The classifications of $o$-monomials and of 2-to-1 binomials are equivalent. *Designs, Codes, and Cryptography*, 93(4):961–970, April 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01463-1`. See correction [3412].

**Weiss:2025:NDP**

[3326] Charlene Weiß. Nontrivial $t$-designs in polar spaces exist for all $t$. *Designs, Codes, and Cryptography*, 93(4):971–981, April 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01471-1`.

**Chen:2025:IFA**

[3327] Ruikai Chen and Sihem Mesnager. Involutions of finite abelian groups with explicit constructions on finite fields. *Designs, Codes, and Cryptography*, 93(4):983–995, April 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01474-y`.

**Abubaker:2025:FDS**

[3328] Radi Abubaker and Guang Gong. Frequency distance sequences for packet detection in physical-layer security. *Designs, Codes, and Cryptography*, 93(4):997–1020, April 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01475-x`.

**Katz:2025:MAD**

[3329] Daniel J. Katz and Miriam E. Ramirez. Moments of autocorrelation demerit factors of binary sequences. *Designs, Codes, and Cryptography*, 93(4):1021–1065, April 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01482-y`.

**Budaghyan:2025:AOA**

[3330] Lilya Budaghyan and Mohit Pal. Arithmetization-oriented APN permutations. *Designs, Codes, and Cryptography*, 93(4):1067–1088, April 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01487-7`.

**Li:2025:IDD**

[3331] Shuxing Li and Maosheng Xiong. Intersection distribution of degree four polynomials over finite fields. *Designs, Codes, and Cryptography*, 93(4):1089–1111, April 2025. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01488-6.

**Dhaeseleer:2025:CGH**

[3332] Jozefien D'haeseleer, Ferdinand Ihringer, and Kai-Uwe Schmidt. A common generalization of hypercube partitions and ovoids in polar spaces. *Designs, Codes, and Cryptography*, 93 (4):1113–1126, April 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01489-5.

**Bamberg:2025:TDF**

[3333] John Bamberg, Michael Giudici, Jesse Lansdown, and Gordon F. Royle. Tactical decompositions in finite polar spaces and non-spreading classical group actions. *Designs, Codes, and Cryptography*, 93(4):1127–1141, April 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01490-y.

**Kiermaier:2025:DFC**

[3334] Michael Kiermaier, Kai-Uwe Schmidt, and Alfred Wassermann. Designs in finite classical polar spaces. *Designs, Codes, and Cryptography*, 93 (4):1143–1162, April 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01491-x.

**DeBeule:2025:TNE**

[3335] Jan De Beule, Jonathan Mannaert, and Leo Storme. On two non-existence results for Cameron–Liebler $k$-sets in $\mathrm{PG}(n, q)$. *Designs, Codes, and Cryptography*, 93 (4):1163–1177, April 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01505-8.

**Adriaensen:2025:ASO**

[3336] Sam Adriaensen and Maarten De Boeck. Association schemes and orthogonality graphs on anisotropic points of polar spaces. *Designs, Codes, and Cryptography*, 93(4):1179–1216, April 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01514-7.

**Bartoli:2025:DMC**

[3337] Daniele Bartoli and Francesco Ghiandoni. On 3-dimensional MRD codes of type $\langle X^{q^t}, X + \delta X^{q^{2t}}, G(X)\rangle$. *Designs, Codes, and Cryptography*, 93 (4):1217–1236, April 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01528-1.

**Carlet:2025:VSW**

[3338] Claude Carlet. On the vector subspaces of $\mathbf{F}_{2^n}$ over which the multiplicative inverse function sums to zero. *Designs, Codes, and Cryptography*, 93 (4):1237–1254, April 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01531-6.

**TerraBastos:2025:COQ**

[3339] Gustavo Terra Bastos, Angelynn Álvarez, Zachary Flores, and Adriana Salerno. A construction of optimal quasi-cyclic locally recoverable codes using constituent codes. *Designs, Codes, and Cryptography*, 93 (5):1255–1270, May 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01532-5`.

**Ma:2025:AGB**

[3340] Jicheng Ma and Guiying Yan. On automorphism groups of binary cyclic codes. *Designs, Codes, and Cryptography*, 93(5):1271–1282, May 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01539-y`.

**Gupta:2025:CPD**

[3341] Prachi Gupta, P. R. Mishra, and Atul Gaur. A class of permutations on $\mathbf{Z}_p$ with differential uniformity at most 3. *Designs, Codes, and Cryptography*, 93 (5):1283–1293, May 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01548-x`.

**Coelho:2025:LWC**

[3342] J. G. Coelho and F. E. Brochero Martínez. Low-weight codewords in cyclic codes. *Designs, Codes, and Cryptography*, 93(5):1295–1310, May 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01547-y`.

**Sun:2025:SFN**

[3343] Zhonghua Sun and Xinyue Liu. Several families of negacyclic BCH codes and their duals. *Designs, Codes, and Cryptography*, 93(5):1311–1336, May 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01551-2`.

**Lu:2025:WHT**

[3344] Wei Lu, Qingyao Wang, Xiaoqiang Wang, and Dabin Zheng. The weight hierarchies of three classes of linear codes. *Designs, Codes, and Cryptography*, 93(5):1337–1355, May 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01553-0`.

**Zhao:2025:FAM**

[3345] Chunzhi Zhao, Jinzheng Cao, Junqi Zhang, and Qingfeng Cheng. Fault attacks on multi-prime RSA signatures. *Designs, Codes, and Cryptography*, 93 (5):1357–1374, May 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01554-z`.

**Castellanos:2025:SPG**

[3346] Alonso S. Castellanos, Erik A. R. Mendoza, and Guilherme Tizziotti. The set of pure gaps at several rational places in function fields. *Designs, Codes, and Cryptography*, 93

(5):1375–1400, May 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01556-x.

**DeBruyn:2025:DDG**

[3347] Bart De Bruyn, Sergey Goryainov, Willem H. Haemers, and Leonid Shalaginov. Divisible design graphs from the symplectic graph. *Designs, Codes, and Cryptography*, 93 (5):1401–1424, May 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01557-w.

**Jia:2025:FSO**

[3348] Dingding Jia, Haiyang Xue, and Bao Li. Fully selective opening secure IBE from LWE. *Designs, Codes, and Cryptography*, 93(5):1425–1449, May 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01560-1.

**Bidoux:2025:RDS**

[3349] Loïc Bidoux, Jesús-Javier Chi-Domínguez, Thibauld Feneuil, Philippe Gaborit, Antoine Joux, Matthieu Rivain, and Adrien Vinçotte. RYDE: a digital signature scheme based on rank syndrome decoding problem with MPC-in-the-Head paradigm. *Designs, Codes, and Cryptography*, 93 (5):1451–1486, May 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01544-1.

**ElBadry:2025:LSG**

[3350] Mohammed El Badry, Abdelfattah Haily, and Ayoub Mounir. On LCD skew group codes. *Designs, Codes, and Cryptography*, 93(5):1487–1499, May 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01561-0.

**Li:2025:EIT**

[3351] Junru Li, Pengzhen Ke, and Liang Feng Zhang. Efficient information-theoretic distributed point functions with general output groups. *Designs, Codes, and Cryptography*, 93(5):1501–1530, May 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01562-z.

**Chen:2025:MMA**

[3352] Siwei Chen, Kai Hu, Guozhen Liu, Zhongfeng Niu, Quan Quan Tan, and Shichang Wang. Meet-in-the-middle attack on round-reduced SCARF under single pair-of-tweaks setting. *Designs, Codes, and Cryptography*, 93 (5):1531–1547, May 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01596-x.

**Xia:2025:FID**

[3353] Yongbo Xia, Chunlei Li, and Tor Helleseth. Further investigation on differential properties of the generalized Ness–Helleseth function. *Designs, Codes, and Cryptography*, 93

(6):??, June 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01525-4.

**Ding:2025:SDS**

[3354] Cunsheng Ding, Zhonghua Sun, and Qianqian Yan. The support designs of several families of lifted linear codes. *Designs, Codes, and Cryptography*, 93 (6):1549–1573, June 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01549-w.

**Micheli:2025:CIP**

[3355] Giacomo Micheli, Vincenzo Pallozzi Lavorante, and Phillip Waitkevich. Codes from $A_m$ -invariant polynomials. *Designs, Codes, and Cryptography*, 93(6):1575–1595, June 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01550-3.

**Engelberts:2025:QSC**

[3356] Lynn Engelberts, Simona Etinski, and Johanna Loyer. Quantum sieving for code-based cryptanalysis and its limitations for ISD. *Designs, Codes, and Cryptography*, 93(6):1597–1609, June 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01545-0.

**Aguilar-Melchor:2025:SHE**

[3357] Carlos Aguilar-Melchor, Victor Dyseryn, and Philippe Gaborit. Somewhat homomorphic encryption based on random codes. *Designs, Codes, and Cryptography*, 93(6):1611–1644, June 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01555-y.

**Shi:2025:TIC**

[3358] Minjia Shi, Ruowen Liu, and Andrea Svob. Ternary isodual codes and 3-designs. *Designs, Codes, and Cryptography*, 93(6):1645–1669, June 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01558-9.

**Dastbasteh:2025:ATC**

[3359] Reza Dastbasteh and Petr Lisonek. Additive twisted codes: new distance bounds and infinite families of quantum codes. *Designs, Codes, and Cryptography*, 93(6):1671–1685, June 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01552-1.

**Wang:2025:RIM**

[3360] Xiang Wang and Fang-Wei Fu. Rate-improved multi-permutation codes for correcting a single burst of stable deletions. *Designs, Codes, and Cryptography*, 93(6):1687–1724, June 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01564-5.

**Bruyn:2025:BSS**

[3361] Bart De Bruyn, Puspendu Pradhan, and Binod Kumar Sahoo. Blocking sets of secant and tangent lines with respect to a quadric of $\mathrm{PG}(n, q)$. *Designs, Codes, and Cryptography*, 93 (6):1725–1737, June 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-024-01559-8`.

**Pankov:2025:SDT**

[3362] Mark Pankov, Krzysztof Petelczyc, and Mariusz Zynel. Symmetric $(15, 8, 4)$-designs in terms of the geometry of binary simplex codes of dimension 4. *Designs, Codes, and Cryptography*, 93 (6):1739–1760, June 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01570-7`.

**Zajac:2025:PRS**

[3363] Pavol Zajac. Polynomial reduction from syndrome decoding problem to regular decoding problem. *Designs, Codes, and Cryptography*, 93 (6):1761–1775, June 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01567-2`.

**Martinez:2025:PFF**

[3364] Fabio Enrique Brochero Martínez, Lucas Reis, and Sávio Ribas. On polynomials over finite fields that are free of binomials. *Designs, Codes, and Cryptography*, 93(6):1777–1793, June 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01573-4`.

**Min:2025:PKE**

[3365] Rudong Min, Jiale Han, and Yi Yang. A public key encryption algorithm based on multi-dimensional general Chebyshev polynomial. *Designs, Codes, and Cryptography*, 93(6):1795–1807, June 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01574-3`.

**Sima:2025:PRS**

[3366] Jin Sima, Chao Pan, and Olgica Milenkovic. Perturbation-resilient sets for dynamic service balancing. *Designs, Codes, and Cryptography*, 93 (6):1809–1836, June 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01565-4`.

**Lobillo:2025:LCP**

[3367] F. J. Lobillo and José Manuel Muñoz. Linear complementary pairs of skew constacyclic codes. *Designs, Codes, and Cryptography*, 93 (6):1837–1861, June 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01568-1`.

**Xie:2025:VFM**

[3368] Xianhong Xie, Yi Ouyang, and Honggang Hu. On vectorial functions with maximal number of bent components. *Designs, Codes, and Cryptography*, 93

(6):1863–1888, June 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01569-0`.

**Sahoo:2025:ISC**

[3369] Soumya Sahoo, Raghavendra Patil, and Chester Rebeiro. Improved side channel attacks on TRIVIUM, GRAIN-128-AEAD, ACORN-128 v3 and ASCON-128a. *Designs, Codes, and Cryptography*, 93 (6):1889–1910, June 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01579-y`.

**Chang:2025:EGO**

[3370] Zuling Chang and Qiang Wang. Efficient generation of odd order de Bruijn sequence with the same complement and reverse sequences. (French) []. *Designs, Codes, and Cryptography*, 93 (6):1911–1933, June 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01580-5`.

**Garg:2025:RBC**

[3371] Kirpa Garg, Sartaj Ul Hasan, and Pantelimon Stanica. The revised boomerang connectivity tables and their connection to the difference distribution table. *Designs, Codes, and Cryptography*, 93(6):1935–1949, June 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01582-3`.

**Huczynska:2025:NRN**

[3372] Sophie Huczynska and Sophie Hume. New results on non-disjoint and classical strong external difference families. *Designs, Codes, and Cryptography*, 93 (6):1951–1984, June 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01566-3`.

**Zhang:2025:NAF**

[3373] Yuhan Zhang, Lei Zhang, and Wenling Wu. A new automatic framework for searching rotational-XOR differential characteristics in ARX ciphers. *Designs, Codes, and Cryptography*, 93 (6):1985–2012, June 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01571-6`.

**Degre:2025:NMC**

[3374] Mathieu Degré, Patrick Derbez, and André Schrottenloher. New models for the cryptanalysis of ASCON. *Designs, Codes, and Cryptography*, 93 (6):2013–2054, June 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01572-5`.

**Baek:2025:CWB**

[3375] Chunghun Baek and Taechan Kim. Can we beat three halves lower bound? (im)possibility of reducing communication cost for garbled circuits. *Designs, Codes, and Cryptography*, 93 (6):2055–2072, June 2025. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01577-0.

**Ming:2025:AEB**

[3376] Xinyue Ming, Tao Feng, and Menglong Zhang. The asymptotic existence of BIBDs having a nesting. *Designs, Codes, and Cryptography*, 93 (6):2073–2105, June 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01583-2.

**Liu:2025:COF**

[3377] Shuangqing Liu, Shuhui Yu, and Lijun Ji. Construction of optimal flag codes by MRD codes. *Designs, Codes, and Cryptography*, 93 (6):2107–2118, June 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01584-1.

**Baisse:2025:SSK**

[3378] Chloé Baïsse, Antoine Moran, and Antoine Loiseau. Secret and shared keys recovery on Hamming quasi-cyclic with SASCA. *Designs, Codes, and Cryptography*, 93(6):2119–2136, June 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01575-2.

**Mahak:2025:ESO**

[3379] Mahak and Maheshanand Bhaintwal. On equidistant single-orbit cyclic and quasi-cyclic subspace codes. *Designs, Codes, and Cryptography*, 93 (6):2137–2157, June 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01586-z.

**Gavrilyuk:2025:SRG**

[3380] Alexander L. Gavrilyuk and Vladislav V. Kabanov. Strongly regular graphs decomposable into a divisible design graph and a Delsarte clique. *Designs, Codes, and Cryptography*, 93 (6):2159–2175, June 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-024-01563-y.

**Chen:2025:PRA**

[3381] Zhixiong Chen and Arne Winterhof. Probabilistic results on the 2-adic complexity. *Designs, Codes, and Cryptography*, 93(6):2177–2189, June 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01592-1.

**Li:2025:CCP**

[3382] Kangquan Li. Constructions of complete permutations in multiplication. *Designs, Codes, and Cryptography*, 93 (6):2191–2203, June 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01593-0.

**Qin:2025:GCV**

[3383] Chunyan Qin and Gaojun Luo. A generalized construction of variable-length non-overlapping codes. *Designs, Codes, and Cryptography*, 93

(6):2205–2228, June 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01585-0.

**Steiner:2025:NWS**

[3384] Matthias Johann Steiner. A note on the Walsh spectrum of the flystel. *Designs, Codes, and Cryptography*, 93 (6):2229–2243, June 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01589-w.

**Zhao:2025:OTD**

[3385] Hengming Zhao, Rongcun Qin, and Dianhua Wu. Optimal two-dimensional multilength optical orthogonal codes via compatible mixed difference packing set systems. *Designs, Codes, and Cryptography*, 93(6):2245–2262, June 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01587-y.

**Zhao:2025:BCO**

[3386] Mengzhen Zhao and Yanxun Chang. Bounds and constructions of optimal symbol-pair codes with constant pair-weight. *Designs, Codes, and Cryptography*, 93(6):2263–2296, June 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01598-9.

**Pacifico:2025:ILS**

[3387] Bastien Pacifico. Introducing locality in some generalized AG codes. *Designs, Codes, and Cryptography*, 93(7):??, July 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01597-w.

**Dinh:2025:NFA**

[3388] Hai Q. Dinh, Hieu V. Ha, and Thieu N. Vo. A new family of AMDS symbol-pair constacyclic codes of length **4p** and symbol-pair distance **9**. *Designs, Codes, and Cryptography*, 93 (7):2317–2332, July 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01600-4.

**Gabric:2025:CKA**

[3389] Daniel Gabrić and Joe Sawada. Constructing k -ary orientable sequences with asymptotically optimal length. *Designs, Codes, and Cryptography*, 93 (7):2333–2347, July 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01581-4.

**Meena:2025:CTT**

[3390] Kapish Chand Meena, Piyush Pachauri, and Maheshanand Bhaintwal. A class of triple-twisted GRS codes. *Designs, Codes, and Cryptography*, 93 (7):2349–2367, July 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01595-y.

**Cheng:2025:CTC**

[3391] Kaimin Cheng. A class of ternary codes with few weights. *Designs,*

*Codes, and Cryptography*, 93(7):2369–2393, July 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01605-z`.

**Chou:2025:LEC**

[3392] Tung Chou, Edoardo Persichetti, and Paolo Santini. On linear equivalence, canonical forms, and digital signatures. *Designs, Codes, and Cryptography*, 93(7):2395–2414, July 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01576-1`.

**Li:2025:FCI**

[3393] Wenya Li, Kai Zhang, and Bin Hu. A framework for constructing impossible differential distinguishers and its applications. *Designs, Codes, and Cryptography*, 93(7):2415–2457, July 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01588-x`.

**Markov:2025:WDF**

[3394] Miroslav Markov and Yuri Borissov. The weight distribution of the fourth-order Reed–Muller code of length 512. *Designs, Codes, and Cryptography*, 93(7):2459–2486, July 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01602-2`.

**Bitzer:2025:HLS**

[3395] Sebastian Bitzer, Jeroen Delvaux, and Antonia Wachter-Zeh. How to lose some weight: a practical template syndrome decoding attack. *Designs, Codes, and Cryptography*, 93(7):2487–2502, July 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01603-1`.

**Couvee:2025:BSS**

[3396] Hugo Sauerbier Couvée, Thomas Jerkovits, and Jessica Bariffi. Bounds on sphere sizes in the sum-rank metric and coordinate-additive metrics. *Designs, Codes, and Cryptography*, 93(7):2503–2519, July 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01604-0`.

**Lv:2025:NGB**

[3397] Chang Lv and Yuqing Zhu. Nonexistence of generalized bent functions and the quadratic norm form equations. *Designs, Codes, and Cryptography*, 93(7):2521–2542, July 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01606-y`.

**Baena:2025:APC**

[3398] John Baena, Daniel Cabarcas, and Luis Villota. Admissible parameters for the Crossbred algorithm and semi-regular sequences over finite fields. *Designs, Codes, and Cryptography*, 93(7):2543–2559, July 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01610-2`.

**Agrinsoni:2025:REA**

[3399] Carlos Agrinsoni, Heeralal Janwa, and Moises Delgado. Resolution of the exceptional APN conjecture in the Gold degree case. *Designs, Codes, and Cryptography*, 93(7):2561–2589, July 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01607-x`.

**Song:2025:GID**

[3400] Ling Song, Qinggan Fu, and Lei Hu. Generalized impossible differential attacks on block ciphers: application to SKINNY and ForkSKINNY. *Designs, Codes, and Cryptography*, 93(7):2591–2610, July 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01611-1`.

**Dionigi:2025:GSH**

[3401] Arianna Dionigi and Barbara Gatti. Galois subcovers of the Hermitian curve in characteristic p with respect to subgroups of order dp with $d \neq p$ prime. *Designs, Codes, and Cryptography*, 93(7):2611–2655, July 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01613-z`.

**Zheng:2025:NFF**

[3402] Xiaopeng Zheng, Hongbo Li, and Dingkang Wang. A new framework for fast homomorphic matrix multiplication. *Designs, Codes, and Cryptography*, 93(7):2657–2670, July 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01614-y`.

**Zhang:2025:APA**

[3403] Chi Zhang. An attack on p -adic lattice public-key encryption cryptosystems and signature schemes. *Designs, Codes, and Cryptography*, 93(7):2671–2693, July 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01618-8`.

**Buratti:2025:ACD**

[3404] Marco Buratti, Francesca Merola, and Anamari Nakić. Additive combinatorial designs. *Designs, Codes, and Cryptography*, 93(7):2695–2716, July 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01594-z`.

**Boroojeni:2025:BSE**

[3405] Javad Ebrahimi Boroojeni and Mehri Oghbaei Bonab. Binary stretch embedding of weighted graphs. *Designs, Codes, and Cryptography*, 93(7):2717–2740, July 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01608-w`.

**Pathegama:2025:LDL**

[3406] Madhura Pathegama and Alexander Barg. Limitations of the decoding-to-LPN reduction via code smoothing.

*Designs, Codes, and Cryptography*, 93 (7):2741–2760, July 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01617-9.

**Zhu:2025:CWE**

[3407] Canze Zhu. The complete weight enumerator of the square of one-weight irreducible cyclic codes. *Designs, Codes, and Cryptography*, 93 (7):2761–2778, July 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01620-0.

**Carey:2025:UPT**

[3408] William D. Carey, Matthew David Kearney, and Stefan Popescu. Universal partial tori. *Designs, Codes, and Cryptography*, 93(7):2779–2802, July 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01609-9.

**Xiong:2025:SIN**

[3409] Jingtao Xiong, Jianghua Zhong, and Dongdai Lin. Studying the isomorphism of NFSRs via a general framework of bijections. *Designs, Codes, and Cryptography*, 93(7):2803–2822, July 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01622-y.

**Wang:2025:CSC**

[3410] Xiao juan Wang, Tian Tian, and Wen feng Qi. On the cycle structure of a class of Galois NFSRs: component sequences possessing identical periods. *Designs, Codes, and Cryptography*, 93 (7):2823–2853, July 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01616-w.

**Camps-Moreno:2025:WHD**

[3411] Eduardo Camps-Moreno, Hiram H. López, and Rodrigo San-José. The weight hierarchy of decreasing norm-trace codes. *Designs, Codes, and Cryptography*, 93(7):2855–2871, July 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01619-7.

**Kolsch:2025:CCM**

[3412] Lukas Kölsch and Gohar Kyureghyan. Correction: The classifications of $o$-monomials and of 2-to-1 binomials are equivalent. *Designs, Codes, and Cryptography*, 93(7):2873–2894, July 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01645-5. See [3325].

**Lieb:2025:NME**

[3413] Julia Lieb, Raquel Pinto, and Carlos Vela. A new method for erasure decoding of convolutional codes. *Designs, Codes, and Cryptography*, 93 (8):2897–2918, August 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01623-x.

**Kubischta:2025:QCI**

[3414] Eric Kubischta and Ian Teixeira. Quantum codes and irreducible products of characters. *Designs, Codes, and Cryptography*, 93(8):2919–2930, August 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01599-8.

**Micheli:2025:CLR**

[3415] Giacomo Micheli, Vincenzo Pallozzi Lavorante, and Noah Smith. Constructions of locally recoverable codes with large availability. *Designs, Codes, and Cryptography*, 93(8):2931–2945, August 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01624-w.

**Ahola:2025:FMP**

[3416] Joonas Ahola, Iván Blanco-Chacón, and Rodrigo M. Sánchez-Ledesma. Fast multiplication and the PLWE-RLWE equivalence for an infinite family of maximal real subfields of cyclotomic fields. *Designs, Codes, and Cryptography*, 93(8):2947–2969, August 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01601-3.

**Liu:2025:CBC**

[3417] Hai Liu, Chunyu Gan, and Xueying Shi. Constructions of binary cyclic codes with minimum weights exceeding the square-root lower bound. *Designs, Codes, and Cryptography*, 93(8):2971–2992, August 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01621-z.

**Bonini:2025:GCC**

[3418] Matteo Bonini, Martino Borello, and Eimear Byrne. The geometry of covering codes in the sum-rank metric. *Designs, Codes, and Cryptography*, 93(8):2993–3009, August 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01628-6.

**Zhu:2025:UTS**

[3419] Yuqing Zhu, Chang Lv, and Jiqiang Liu. Utilizing two subfields to accelerate individual logarithm computation in extended tower number field sieve. *Designs, Codes, and Cryptography*, 93(8):3011–3027, August 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01590-3.

**Kilic:2025:KTE**

[3420] Altan B. Kiliç, Anne Nijsten, and Alberto Ravagnani. Knot theory and error-correcting codes. *Designs, Codes, and Cryptography*, 93(8):3029–3068, August 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01615-x.

**Sun:2025:NUB**

[3421] Chengyu Sun and Xin Wang. New upper bounds for wide-sense frameproof

codes. *Designs, Codes, and Cryptography*, 93(8):3069–3082, August 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01631-x.

**Lemoine:2025:UND**

[3422] Axel Lemoine, Rocco Mora, and Jean-Pierre Tillich. Understanding the new distinguisher of alternant codes at degree 2. *Designs, Codes, and Cryptography*, 93(8):3083–3105, August 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01626-8.

**Jia:2025:CPA**

[3423] Xue Jia, Qin Yue, and Huan Sun. Coding properties and automorphism groups of two classes of twisted generalized Reed–Solomon codes. *Designs, Codes, and Cryptography*, 93(8):3107–3133, August 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01630-y.

**Cooper:2025:PMN**

[3424] Joshua Cooper and Jack Hyatt. Permutations minimizing the number of collinear triples. *Designs, Codes, and Cryptography*, 93(8):3135–3142, August 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01632-w.

**Schulz:2025:RTF**

[3425] Max Schulz. Rational transformations over finite fields that are never irreducible. *Designs, Codes, and Cryptography*, 93(8):3143–3157, August 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01591-2.

**Burgess:2025:WCK**

[3426] Andrea C. Burgess, Nicholas J. Cavenagh, and David A. Pike. Weak colourings of Kirkman triple systems. *Designs, Codes, and Cryptography*, 93(8):3159–3179, August 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01635-7.

**Liu:2025:LCC**

[3427] Shuiyin Liu and Amin Sakzad. Lattice codes for CRYSTALS-Kyber. *Designs, Codes, and Cryptography*, 93(8):3181–3205, August 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01640-w.

**TchoffoSaah:2025:ATS**

[3428] Gustave Tchoffo Saah, Tako Boris Fouotsa, and Célestin Nkuimi-Jugnia. Avoiding trusted setup in isogeny-based commitments. *Designs, Codes, and Cryptography*, 93(8):3207–3225, August 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01633-9.

**Xiao:2025:TRF**

[3429] Zibi Xiao, Yaya Ye, and Xiangyong Zeng. Trace representation of a family of generalized cyclotomic binary sequences with period $p^n$. *Designs, Codes, and Cryptography*, 93 (8):3227–3241, August 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01638-4`.

**Baudrin:2025:CCG**

[3430] Jules Baudrin, Christof Beierle, and Lukas Stennes. Commutative cryptanalysis as a generalization of differential cryptanalysis. *Designs, Codes, and Cryptography*, 93(8):3243–3281, August 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01625-9`.

**Yohananov:2025:CCR**

[3431] Lev Yohananov and Moshe Schwartz. On the coding capacity of reverse-complement and palindromic duplication-correcting codes. *Designs, Codes, and Cryptography*, 93(8):3283–3302, August 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01627-7`.

**Maji:2025:CMC**

[3432] Makhan Maji, Sihem Mesnager, and Kalyan Hansda. Characterizations for minimal codes: graph theory approach and algebraic approach over finite chain rings. *Designs, Codes, and Cryptography*, 93(8):3303–3335, August 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01636-6`.

**Alavi:2025:FTS**

[3433] Seyed Hassan Alavi. On flag-transitive symmetric $(v, k, 4)$ designs. *Designs, Codes, and Cryptography*, 93(8):3337–3359, August 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01642-8`.

**Gatti:2025:ECA**

[3434] Barbara Gatti, Gábor Korchmáros, and Gioia Schulte. Evaluation codes arising from symmetric polynomials. *Designs, Codes, and Cryptography*, 93 (8):3361–3373, August 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01637-5`.

**Guo:2025:TCR**

[3435] Chun Guo, Xiao Wang, and Yu Yu. On tweakable correlation robust hashing against key leakages. *Designs, Codes, and Cryptography*, 93(8):3375–3412, August 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01641-9`.

**Matthews:2025:CAA**

[3436] Gretchen L. Matthews and Emily McMillon. A combinatorial approach to avoiding weak keys in

the BIKE cryptosystem. *Designs, Codes, and Cryptography*, 93(8):3413–3436, August 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01643-7`.

**Ye:2025:MCC**

[3437] Zuo Ye, Omer Sabary, and Ohad Elishco. More on codes for combinatorial composite DNA. *Designs, Codes, and Cryptography*, 93(8):3437–3462, August 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01634-8`.

**Rodrigues:2025:PRG**

[3438] B. G. Rodrigues and Patrick Solé. Primitive rank 3 groups, binary codes, and 3-designs. *Designs, Codes, and Cryptography*, 93(9):3463–3479, September 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01647-3`.

**Gassner:2025:ISD**

[3439] Niklas Gassner, Julia Lieb, and Michael Schaller. Information-set decoding for convolutional codes. *Designs, Codes, and Cryptography*, 93(9):3481–3505, September 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01649-1`.

**Bezzateev:2025:SRG**

[3440] Sergey Bezzateev and Natalia Shekhunova. Self-reversible generalized $(L, G)$-codes. *Designs, Codes, and Cryptography*, 93(9):3507–3519, September 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01648-2`.

**Esposito:2025:HSD**

[3441] Antonio Corbo Esposito, Rosa Fera, and Francesco Romeo. Hilbert series and degrees of regularity of Oil & Vinegar and mixed quadratic systems. *Designs, Codes, and Cryptography*, 93(9):3521–3541, September 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01644-6`.

**Herranz:2025:CAS**

[3442] Javier Herranz and Germán Sáez. $(k, n)$-consecutive access structures. *Designs, Codes, and Cryptography*, 93(9):3543–3563, September 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01651-7`.

**Abel:2025:ILB**

[3443] R. Julian R. Abel, Ingo Janiszczak, and Reiner Staszewski. Improvements for lower bounds of mutually orthogonal Latin squares of sizes 54, 96 and 108. *Designs, Codes, and Cryptography*, 93(9):3565–3573, September 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01629-5`.

**Matsui:2025:EAQ**

[3444] Hajime Matsui and Kakeru Kaneko. Entanglement-assisted quantum error-correcting codes via quasi-cyclic codes with complementary duals. *Designs, Codes, and Cryptography*, 93(9):3575–3591, September 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01650-8`.

**Cavicchioni:2025:CLR**

[3445] Giulia Cavicchioni, Eleonora Guerrini, and Alessio Meneghetti. A class of locally recoverable codes over finite chain rings. *Designs, Codes, and Cryptography*, 93(9):3593–3618, September 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01653-5`.

**Oggier:2025:ARB**

[3446] Frédérique Oggier, Shengwei Liu, and Hongwei Liu. About the Rankin and Bergé–Martinet constants from a coding theory view point. *Designs, Codes, and Cryptography*, 93(9):3619–3640, September 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01654-4`.

**Faraoun:2025:OSG**

[3447] Kamel Mohamed Faraoun and Nadia El Mrabet. Optimizing and securing GLV multiplication over BLS pairings-friendly curves. *Designs, Codes, and Cryptography*, 93(9):3641–3669, September 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01646-4`.

**Cui:2025:DUC**

[3448] Yuehui Cui and Jinquan Luo. Differential uniformity and constacyclic code from some power mapping. *Designs, Codes, and Cryptography*, 93(9):3671–3687, September 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01662-4`.

**Jorgensen:2025:CCN**

[3449] Søren Fuglede Jørgensen. On the clique covering numbers of Johnson graphs. *Designs, Codes, and Cryptography*, 93(9):3689–3705, September 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01663-3`.

**Zhou:2025:IMS**

[3450] Yanyan Zhou, Senpeng Wang, and Bin Hu. Improved method of searching for boomerang distinguishers on Feistel structures-applications to WARP, TWINE, LBlock, LBlock-s, and ALLPC. *Designs, Codes, and Cryptography*, 93(9):3707–3731, September 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01639-3`.

**Ali:2025:CCG**

[3451] Shakir Ali, Nuh Aydin, and Atif Ahmad Khan. Constacyclic codes

over general mixed alphabets and their applications. *Designs, Codes, and Cryptography*, 93(9):3733–3760, September 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01652-6`.

**Lin:2025:IDS**

[3452] Xiaoen Lin, Le He, and Hongbo Yu. Internal differential structure: preimage attacks on up to 5-round Keccak. *Designs, Codes, and Cryptography*, 93(9): 3761–3808, September 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01655-3`.

**Francati:2025:ESS**

[3453] Danilo Francati and Daniele Venturi. Evolving secret sharing revisited: computational security and succinctness. *Designs, Codes, and Cryptography*, 93(9):3809–3861, September 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01658-0`.

**Buratti:2025:SHS**

[3454] M. Buratti and A. Pasotti. Shiftable Heffter spaces. *Designs, Codes, and Cryptography*, 93(9):3863–3874, September 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01657-1`.

**Borodachov:2025:BDP**

[3455] S. V. Borodachov, P. G. Boyvalenkov, and M. M. Stoyanova. Bounds on discrete potentials of spherical $(k, k)$-designs. *Designs, Codes, and Cryptography*, 93(9):3875–3902, September 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01659-z`.

**Bose:2025:BCC**

[3456] Mrinal Kanti Bose, Udaya Parampalli, and Abhay Kumar Singh. Binary cyclic codes from permutation polynomials over $\mathbf{F}_{2^m}$. *Designs, Codes, and Cryptography*, 93(9):3903–3932, September 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01661-5`.

**Wu:2025:CIP**

[3457] Danyao Wu and Pingzhi Yuan. The compositional inverses of the permutation polynomials from trace functions over finite fields. *Designs, Codes, and Cryptography*, 93(9):3933–3953, September 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-025-01670-4`.

**Lin:2025:GCT**

[3458] Hao Lin, Mingqiang Wang, and Kaitai Liang. Generic construction of threshold ring signatures and lattice-based instantiations. *Designs, Codes, and Cryptography*, 93(9):3955–4017, September 2025. CODEN

DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01660-6.

**Kajiura:2025:DPD**

[3459] Hiroki Kajiura, Koji Momihara, and Utano Ogata. Divisible pre-difference sets for approximating integrations over finite groups. *Designs, Codes, and Cryptography*, 93(9):4019–4042, September 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01665-1.

**Liu:2025:NAX**

[3460] Yong Liu, Zejun Xiang, and Shasha Zhang. A novel algorithm for the $k$-XOR problem. *Designs, Codes, and Cryptography*, 93(9):4043–4081, September 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01667-z.

**Zhang:2025:FRP**

[3461] Tongliang Zhang, Haibin Kan, and Hanbing Zhao. Further results on permutation pentanomials over finite fields with characteristic two. *Designs, Codes, and Cryptography*, 93(9):4083–4112, September 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01673-1.

**Ball:2025:CGT**

[3462] Simeon Ball, Michel Lavrauw, and Tabriz Popatia. Correction to: Griesmer type bounds for additive codes over finite fields, integral and fractional MDS codes. *Designs, Codes, and Cryptography*, 93(9):4113–4115, September 2025. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-025-01681-1. See [3285].