A Complete Bibliography of Publications in the *Journal of Mathematical Cryptology*

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
FAX: +1 801 581 4148

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

05 April 2022
Version 1.07

Title word cross-reference

$(2,2)$ [PS20]. $(2,2,2)$ [AJZT19]. $(n+1)$ [ZMD20]. $(p^r-1)/3$ [BW09]. 1 [SW07a]. 2 [AJZT19, Gau07, Hit09, SW07a]. 3 [CC15, LL15, MW12]. 4 [Kar10]. 5 [HL19]. 6 [Kar10]. $ax \equiv b \pmod n$ [GP13]. $\mathrm{GL}_2(\mathbf{F}_{p^n})$ [TNS20]. k [AMW07, BW09]. $\mathbf{F}^*_{\mathbf{2^{4m}}}$ [Kar10]. $\mathbf{F}^*_{\mathbf{3^{6m}}}$ [Kar10]. $\mathbf{F_p}$ [BW09]. $\mathbf{F}_{p^2}$ [DM20]. $\mathbf{F_{p^k}}$ [Duq11]. $\mathbf{Q}(\zeta 2s)$ [BS19]. $\mathcal{M}$ [WP11]. $\mathcal{Q}$ [WP11]. MST_3 [BCM09]. n [DSS20, ZMD20]. $N = p^r q^l$ [LPS17]. p [KMNN19]. $p+q$ [MA17]. ρ [Oka12]. MST_3 [SvT10]. S [ZMD20].

-ary [KMNN19]. **-bit** [ZMD20]. **-boxes** [ZMD20]. **-error** [AMW07, BW09]. **-ideal** [AJZT19]. **-rotation** [CC15]. **-round** [SW07a]. **-server** [SW07a]. **-threshold** [PS20]. **-torsion** [MW12]. **-values** [Oka12].

2019 [DKKS20]. **256** [DT17].

7 [GZ14].

abelian [Rei17]. **aborts** [FS11]. **Abu** [Bla10]. **access** [DS17, GD13, JSN13]. **achieving** [AL11]. **action** [JLLRL20, RS22]. **adaptive** [AL11, FS11]. **add** [FJ13]. **add-rotate-xor** [FJ13]. **addition** [FJ13]. **additive** [BDJ14]. **admit** [DN08]. **Advanced** [Sch08]. **adversary** [Dow15]. **AE** [ASB+18]. **Affine** [CLS16, HWCD11]. **Against** [Joy20, BS19, BBP+20, MSP12, WS09].

References

AlMashrafi:2013:IMI

[ABD+13] Mufeed Al Mashrafi, Harry Bartlett, Ed Dawson, Leonie Simpson, and Kenneth Koon-Ho Wong. Indirect message injection for MAC generation. *Journal of Mathematical Cryptology*, 7(3):253–277, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Alomair:2010:PPS

[ACP10] Basel Alomair, Andrew Clark, and Radha Poovendran. The power of primes: security of authentication based on a universal hash-function family. *Journal of Mathematical Cryptology*, 4(2):121–148, 2010. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Asghar:2014:SCG

[ADPS14] Hassan Jameel Asghar, Yvo Desmedt, Josef Pieprzyk, and Ron Steinfeld. A subexponential construction of graph coloring for multiparty computation. *Journal of Mathematical Cryptology*, 8(4):363–403, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Antal:2017:MCP

[AGH17] Eugen Antal, Otokar Grošek, and Peter Horak. On a mnemonic construction of permutations. *Journal of Mathematical Cryptology*, 11(1):45–53, 2017. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Azizi:2019:CIC

[AJZT19] Abdelmalek Azizi, Idriss Jerrari, Abdelkader Zekhnini, and Mohammed Talbi. Capitulation of the 2-ideal classes of type $(2,2,2)$ of some quartic cyclic number fields. *Journal of Mathematical Cryptology*, 13 (1):27–??, March 2019. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/view/j/jmc.2019.13.issue-1/jmc-2017-0037/jmc-2017-0037.xml`.

Asghar:2017:WIP

[AK17] Hassan Jameel Asghar and Mohamed Ali Kaafar. When are identification protocols with sparse challenges safe? The case of the Coskun and Herley attack. *Journal of Mathematical Cryptology*, 11(3):177–194, 2017. ISSN 1862-2976 (print), 1862-2984 (electronic).

Aravamuthan:2007:ATO

[AL07] Sarang Aravamuthan and Sachin Lodha. The average transmission overhead for broadcast encryption. *Journal of Mathematical Cryptology*, 1(4):373–384, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Attrapadung:2011:FEP

[AL11] Nuttapong Attrapadung and Benoît Libert. Functional encryption for public-attribute inner products: achieving constant-size ciphertexts with adaptive security or support for negation. *Journal of Mathematical Cryptology*, 5(2):115–158, 2011. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Alawatugoda:2017:LRK

[Ala17] Janaka Alawatugoda. On the leakage-resilient key exchange. *Journal of Mathematical Cryptology*, 11(4):215–269, 2017. ISSN 1862-2976 (print), 1862-2984 (electronic).

Aly:2007:ELC

[AMW07] Hassan Aly, Wilfried Meidl, and Arne Winterhof. On the k-error linear complexity of cyclotomic sequences. *Journal of Mathematical Cryptology*, 1(3):

283–296, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Araujo:2020:CHR

[AN20] Filipe Araujo and Samuel Neves. The circulant hash revisited. *Journal of Mathematical Cryptology*, 15(1):250–257, December 3, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2018-0054/html`.

Anonymous:2013:M

[Ano13] Anonymous. Masthead. *Journal of Mathematical Cryptology*, 7(3):i, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/view/j/jmc.2013.7.issue-3/jmc-2013-masthead3/jmc-2013-masthead3.xml`.

Anonymous:2017:F

[Ano17] Anonymous. Frontmatter. *Journal of Mathematical Cryptology*, 11(2):i–iv, June 2017. ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/view/j/jmc.2017.11.issue-2/jmc-2017-frontmatter2/jmc-2017-frontmatter2.xml`.

Anonymous:2018:Fa

[Ano18a] Anonymous. Frontmatter. *Journal of Mathematical Cryptology*, 12(1):i–??, March 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/view/j/jmc.2018.12.issue-1/jmc-2018-frontmatter1/jmc-2018-frontmatter1.xml`.

Anonymous:2018:Fb

[Ano18b] Anonymous. Frontmatter. *Journal of Mathematical Cryptology*, 12(2):i–iv, June 2018. ISSN 1862-2976 (print), 1862-2984 (electronic).

Anonymous:2018:Fc

[Ano18c] Anonymous. Frontmatter. *Journal of Mathematical Cryptology*, 12(3):i–??, September 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/view/j/jmc.2018.12.issue-3/jmc-2018-frontmatter3/jmc-2018-frontmatter3.xml`.

Anonymous:2018:F

[Ano18d] Anonymous. Frontmatter. *Journal of Mathematical Cryptology*, 12(4):i–??, December 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/view/j/jmc.2018.12.issue-4/jmc-2018-frontmatter4/jmc-2018-frontmatter4.xml`.

Anonymous:2019:Fa

[Ano19a] Anonymous. Frontmatter. *Journal of Mathematical Cryptology*, 13(1):i–??, March 2019. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.`

degruyter.com/view/j/jmc.2019.13.issue-1/jmc-2019-frontmatter1/jmc-2019-frontmatter1.xml.

Anonymous:2019:Fb

[Ano19b] Anonymous. Frontmatter. *Journal of Mathematical Cryptology*, 13(2):i–??, June 2019. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL http://www.degruyter.com/view/j/jmc.2019.13.issue-2/jmc-2019-frontmatter2/jmc-2019-frontmatter2.xml.

Anonymous:2019:F

[Ano19c] Anonymous. Frontmatter. *Journal of Mathematical Cryptology*, 13(3–4):i–??, September 2019. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL http://www.degruyter.com/view/j/jmc.2019.13.issue-3-4/jmc-2019-frontmatter3-4/jmc-2019-frontmatter3-4.xml.

Anokhin:2020:PFF

[Ano20] Mikhail Anokhin. Pseudo-free families of computational universal algebras. *Journal of Mathematical Cryptology*, 15(1):197–222, November 25, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/document/doi/10.1515/jmc-2020-0014/html.

Alam:2015:CWD

[AÖY15] Bilal Alam, Ferruh Özbudak, and Oğuz Yayla. Classes of weak Dembowski–Ostrom polynomials for multivariate quadratic cryptosystems. *Journal of Mathematical Cryptology*, 9(1):11–22, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Albrecht:2015:CHL

[APS15] Martin R. Albrecht, Rachel Player, and Sam Scott. On the concrete hardness of learning with errors. *Journal of Mathematical Cryptology*, 9(3):169–203, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Accardi:2015:CSA

[AR15] Luigi Accardi and Massimo Regoli. On a class of strongly asymmetric PKA algorithms. *Journal of Mathematical Cryptology*, 9(3):151–159, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

AlMahri:2018:FFA

[ASB+18] Hassan Qahur Al Mahri, Leonie Simpson, Harry Bartlett, Ed Dawson, and Kenneth Koon-Ho Wong. A fundamental flaw in the ++AE authenticated encryption mode. *Journal of Mathematical Cryptology*, 12(1):37–??, March 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/view/j/jmc.2018.12.issue-1/jmc-2016-0037/jmc-2016-0037.xml.

Avanzi:2008:RLG

[ATW08] R. Avanzi, N. Thériault, and Z. Wang. Rethinking low genus hyperelliptic Jacobian arithmetic over binary fields: interplay of field arithmetic and explicit formulæ. *Journal of Mathematical Cryptology*, 2(3): 227–255, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Banegas:2018:DKE

[BBB+18] Gustavo Banegas, Paulo S. L. M. Barreto, Brice Odilon Boidje, Pierre-Louis Cayrel, Gilbert Ndollane Dione, Kris Gaj, Cheikh Thiécoumba Gueye, Richard Haeussler, Jean Belo Klamti, Ousmane N'diaye, Duc Tri Nguyen, Edoardo Persichetti, and Jefferson E. Ricardini. DAGS: Key encapsulation using dyadic GS codes. *Journal of Mathematical Cryptology*, 12(4):221–??, December 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/view/j/jmc.2018.12.issue-4/jmc-2018-0027/jmc-2018-0027.xml`.

Bindel:2019:EHL

[BBGS19] Nina Bindel, Johannes Buchmann, Florian Göpfert, and Markus Schmidt. Estimation of the hardness of the learning with errors problem with a restricted number of samples. *Journal of Mathematical Cryptology*, 13(1): 47–??, March 2019. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/view/j/jmc.2019.13.issue-1/jmc-2017-0040/jmc-2017-0040.xml`.

Bansal:2019:SSI

[BBP19] Tarun Kumar Bansal, Xavier Boyen, and Josef Pieprzyk. Signcryption schemes with insider security in an ideal permutation model. *Journal of Mathematical Cryptology*, 13(2): 117–150, June 2019. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `http://www.degruyter.com/view/j/jmc.2019.13.issue-2/jmc-2018-0006/jmc-2018-0006.xml`.

Biasse:2020:TBC

[BBP+20] Jean-François Biasse, Xavier Bonnetain, Benjamin Pring, André Schrottenloher, and William Youmans. A trade-off between classical and quantum circuit size for an attack against CSIDH. *Journal of Mathematical Cryptology*, 15(1):4–17, November 17, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2020-0070/html`.

Banegas:2020:DED

[BBPS20] Gustavo Banegas, Paulo S. L. M. Barreto, Edoardo Persichetti, and Paolo Santini. Designing efficient dyadic operations for cryptographic applications. *Journal of Mathe-*

matical Cryptology, 14(1):95–109, June 19, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/document/doi/10.1515/jmc-2015-0054/html.

Brown:2012:RWS

[BC12] Alyssa Brown and Thomas W. Cusick. Recursive weights for some Boolean functions. *Journal of Mathematical Cryptology*, 6(2):105–135, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL http://www.degruyter.com/view/j/jmc.2012.6.issue-2/jmc-2011-0020/jmc-2011-0020.xml.

Bootland:2020:EPC

[BCIV20] Carl Bootland, Wouter Castryck, Ilia Iliashenko, and Frederik Vercauteren. Efficiently processing complex-valued data in homomorphic encryption. *Journal of Mathematical Cryptology*, 14(1):55–65, June 14, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/document/doi/10.1515/jmc-2015-0051/html.

Blackburn:2009:CPK

[BCM09] Simon R. Blackburn, Carlos Cid, and Ciaran Mullan. Cryptanalysis of the MST_3 public key cryptosystem. *Journal of Mathematical Cryptology*, 3(4): 321–338, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Blackburn:2011:CTM

[BCM11] Simon R. Blackburn, Carlos Cid, and Ciaran Mullan. Cryptanalysis of three matrix-based key establishment protocols. *Journal of Mathematical Cryptology*, 5(2):159–168, 2011. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Bootland:2020:FCP

[BCSV20] Carl Bootland, Wouter Castryck, Alan Szepieniec, and Frederik Vercauteren. A framework for cryptographic problems from linear algebra. *Journal of Mathematical Cryptology*, 14(1):202–217, July 21, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/document/doi/10.1515/jmc-2019-0032/html.

Broon:2021:ITH

[BDFM21] Fouazou Lontouo Perez Broon, Thinh Dang, Emmanuel Fouotsa, and Dustin Moody. Isogenies on twisted Hessian curves. *Journal of Mathematical Cryptology*, 15(1):345–358, March 16, 2021. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/document/doi/10.1515/jmc-2020-0037/html.

Bos:2014:CBA

[BDJ14] Joppe W. Bos, Alina Dudeanu, and Dimitar Jetchev. Collision bounds for the additive Pollard rho algorithm for solving discrete logarithms. *Journal of Mathematical Cryptology*, 8 (1):71–92, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Baumeister:2012:ALS

[BdW12] Barbara Baumeister and Jan-Hendrik de Wiljes. Aperiodic logarithmic signatures. *Journal of Mathematical Cryptology*, 6 (1):21–37, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Bourgeois:2009:AAN

[BF09] Gérald Bourgeois and Jean-Charles Faugère. Algebraic attack on NTRU using Witt vectors and Gröbner bases. *Journal of Mathematical Cryptology*, 3 (3):205–214, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Brier:2020:NNT

[BFJN20] Éric Brier, Houda Ferradi, Marc Joye, and David Naccache. New number-theoretic cryptographic primitives. *Journal of Mathematical Cryptology*, 14(1):224–235, August 1, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2019-0035/html`.

Bouillaguet:2012:FWK

[BFJT12] Charles Bouillaguet, Pierre-Alain Fouque, Antoine Joux, and Joana Treger. A family of weak keys in HFE and the corresponding practical key-recovery. *Journal of Mathematical Cryptology*, 5(3–4):247–275, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Bettale:2009:HAS

[BFP09] Luk Bettale, Jean-Charles Faugère, and Ludovic Perret. Hybrid approach for solving multivariate systems over finite fields. *Journal of Mathematical Cryptology*, 3(3):177–197, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Bianco:2016:CTZ

[BG16] Giulia Bianco and Elisa Gorla. Compression for trace zero points on twisted Edwards curves. *Journal of Mathematical Cryptology*, 10(1):15–34, 2016. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Boura:2020:CCR

[BGGJ20] Christina Boura, Nicolas Gama, Mariya Georgieva, and Dimitar Jetchev. CHIMERA: Combining Ring-LWE-based fully homomorphic encryption schemes. *Journal of Mathematical Cryptology*, 14(1):316–338, August 7, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2019-0026/html`.

Boneh:2020:MNI

[BGK+20] Dan Boneh, Darren Glass, Daniel Krashen, Kristin Lauter, Shahed Sharif, Alice Silverberg, Mehdi Tibouchi, and Mark Zhandry. Multiparty non-interactive key exchange and more from isogenies on elliptic curves. *Journal of Mathematical Cryptology*, 14(1):5–14, June 14, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/document/doi/10.1515/jmc-2015-0047/html.

Basu:2008:CCE

[BGMP08] Riddhipratim Basu, Shirshendu Ganguly, Subhamoy Maitra, and Goutam Paul. A complete characterization of the evolution of RC4 pseudo random generation algorithm. *Journal of Mathematical Cryptology*, 2(3): 257–289, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Bisson:2011:CER

[Bis11] Gaetan Bisson. Computing endomorphism rings of elliptic curves under the GRH. *Journal of Mathematical Cryptology*, 5 (2):101–113, 2011. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Blake:2009:ORS

[BK09] Ian F. Blake and Vladimir Kolesnikov. One-round secure comparison of integers. *Journal of Mathematical Cryptology*, 3(1):37–68, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Brown:2022:CM

[BKL22] Daniel R. L. Brown, Neal Koblitz, and Jason T. LeGrow. Cryptanalysis of "MAKE". *Journal of Mathematical Cryptology*, 16(1):98–102, January 2022. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/document/doi/10.1515/jmc-2021-0016/html. See [RS22].

Blackburn:2009:CCG

[Bla09] Simon R. Blackburn. Cryptanalysing the critical group: efficiently solving Biggs's discrete logarithm problem. *Journal of Mathematical Cryptology*, 3(3): 199–203, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Blackburn:2010:DLP

[Bla10] Simon R. Blackburn. The discrete logarithm problem modulo one: cryptanalysing the Ariffin–Abu cryptosystem. *Journal of Mathematical Cryptology*, 4(2): 193–198, 2010. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Bhattacharjee:2021:OVF

[BLLN21] Arghya Bhattacharjee, Cuauhtemoc Mancillas López, Eik List, and Mridul Nandi. The Oribatida v1.3 family of lightweight authenticated encryption schemes.

Journal of Mathematical Cryptology, 15(1):305–344, January 29, 2021. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/document/doi/10.1515/jmc-2020-0018/html.

Bockle:2009:MRT

[Böc09] Gebhard Böckle. The Miller–Rabin test with randomized exponents. *Journal of Mathematical Cryptology*, 3(4):307–319, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Boxall:2012:HPF

[Box12] John Boxall. Heuristics on pairing-friendly elliptic curves. *Journal of Mathematical Cryptology*, 6(2):81–104, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/view/j/jmc.2012.6.issue-2/jmc-2011-0004/jmc-2011-0004.xml?format=INT.

Biasse:2020:FRO

[BP20] Jean-François Biasse and Benjamin Pring. A framework for reducing the overhead of the quantum oracle for use with Grover's algorithm with applications to cryptanalysis of SIKE. *Journal of Mathematical Cryptology*, 15(1):143–156, November 17, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/document/doi/10.1515/jmc-2020-0080/html.

Basso:2022:SGA

[BP22] Andrea Basso and Fabien Pazuki. On the supersingular GPST attack. *Journal of Mathematical Cryptology*, 16(1):14–19, January 2022. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/document/doi/10.1515/jmc-2021-0020/html.

Blake:2007:SDC

[BS07] Ian F. Blake and Igor E. Shparlinski. Statistical distribution and collisions of VSH. *Journal of Mathematical Cryptology*, 1(4):329–349, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Biasse:2019:QAA

[BS19] Jean-François Biasse and Fang Song. On the quantum attacks against schemes relying on the hardness of finding a short generator of an ideal in $\mathbf{Q}(\zeta 2s)$. *Journal of Mathematical Cryptology*, 13(3–4):151–??, September 2019. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL http://www.degruyter.com/view/j/jmc.2019.13.issue-3-4/jmc-2015-0046/jmc-2015-0046.xml.

Banin:2012:DLP

[BT12] Matan Banin and Boaz Tsaban. The discrete logarithm problem in Bergman's non-representable ring. *Journal of Mathematical Cryptology*, 6(2): 171–182, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/view/j/jmc.2012.6.issue-2/jmc-2012-0014/jmc-2012-0014.xml.

Brandstatter:2009:ELC

[BW09] Nina Brandstätter and Arne Winterhof. k-error linear complexity over $\mathbf{F_p}$ of subsequences of Sidelnikov sequences of period $(p^r - 1)/3$. *Journal of Mathematical Cryptology*, 3(3): 215–225, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Chakraborty:2020:NAP

[CAR20] Suvradip Chakraborty, Janaka Alawatugoda, and Chandrasekaran Pandu Rangan. New approach to practical leakage-resilient public-key cryptography. *Journal of Mathematical Cryptology*, 14(1):172–201, July 11, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/document/doi/10.1515/jmc-2019-0014/html.

Choi:2007:CHP

[CBW07] Su-Jeong Choi, Simon R. Blackburn, and Peter R. Wild. Cryptanalysis of a homomorphic public-key cryptosystem over a finite group. *Journal of Mathematical Cryptology*, 1(4):351–358, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Cusick:2015:TRS

[CC15] Thomas W. Cusick and Younhwan Cheon. Theory of 3-rotation symmetric cubic Boolean functions. *Journal of Mathematical Cryptology*, 9(1): 45–62, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Cheon:2020:ACV

[CCH+20] Jung Hee Cheon, Wonhee Cho, Minki Hhan, Jiseung Kim, and Changmin Lee. Algorithms for CRT-variant of approximate greatest common divisor problem. *Journal of Mathematical Cryptology*, 14(1):397–413, October 20, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/document/doi/10.1515/jmc-2019-0031/html.

Carlet:2014:LSO

[CDGM14] Claude Carlet, Jean-Luc Danger, Sylvain Guilley, and Houssem Maghrebi. Leakage squeezing: optimal implementation and security evaluation. *Journal of Mathematical Cryptology*, 8(3):249–295, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Chatterjee:2018:CPB

[CDK18] Sanjit Chatterjee, M. Prem Laxman Das, and R. Kabaleeshwaran. Converting pairing-based cryptosystems from composite to prime order setting — a comparative analysis. *Journal of Mathematical Cryptology*, 12(3):159–??, September 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/view/j/jmc.2018.12.issue-3/jmc-2017-0042/jmc-2017-0042.xml`.

Chakraborti:2018:ONL

[CDN18] Avik Chakraborti, Nilanjan Datta, and Mridul Nandi. On the optimality of non-linear computations for symmetric key primitives. *Journal of Mathematical Cryptology*, 12(4):241–??, December 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/view/j/jmc.2018.12.issue-4/jmc-2017-0011/jmc-2017-0011.xml`.

Castryck:2020:HFS

[CDS20] Wouter Castryck, Thomas Decru, and Benjamin Smith. Hash functions from superspecial genus-2 curves using Richelot isogenies. *Journal of Mathematical Cryptology*, 14(1):268–292, August 7, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2019-0021/html`.

Chen:2015:SSK

[CEM15] Jiageng Chen, Keita Emura, and Atsuko Miyaji. SKENO: Secret key encryption with non-interactive opening. *Journal of Mathematical Cryptology*, 9 (2):63–74, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Coron:2020:ICA

[CG20] Jean-Sébastien Coron and Agnese Gini. Improved cryptanalysis of the AJPS Mersenne based cryptosystem. *Journal of Mathematical Cryptology*, 14(1):218–223, July 21, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2019-0027/html`.

Chen:2013:SCM

[CGK13] Yanling Chen, Danilo Gligoroski, and Svein J. Knapskog. On a special class of multivariate quadratic quasigroups (MQQs). *Journal of Mathematical Cryptology*, 7(2):111–141, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Childs:2014:QCD

[CI14] Andrew M. Childs and Gábor Ivanyos. Quantum computation of discrete logarithms in semigroups. *Journal of Mathematical Cryptology*, 8(4):405–416, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Childs:2014:CEC

[CJS14] Andrew Childs, David Jao, and Vladimir Soukharev. Constructing elliptic curve isogenies in quantum subexponential time. *Journal of Mathematical Cryptology*, 8(1):1–29, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Carlet:2016:CPM

[CJST16] Claude Carlet, David Joyner, Pantelimon Stănică, and Deng Tang. Cryptographic properties of monotone Boolean functions. *Journal of Mathematical Cryptology*, 10(1):1–14, 2016. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `http://www.degruyter.com/view/j/jmc.2016.10.issue-1/jmc-2014-0030/jmc-2014-0030.xml`.

Colo:2020:OSI

[CK20] Leonardo Colò and David Kohel. Orienting supersingular isogeny graphs. *Journal of Mathematical Cryptology*, 14(1):414–437, October 23, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2019-0034/html`.

Colbourn:2009:RCP

[CL09] Charles J. Colbourn and Alan C. H. Ling. A recursive construction for perfect hash families. *Journal of Mathematical Cryptology*, 3(4):291–306, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Cusick:2009:CBS

[CLS09] Thomas W. Cusick, Yuan Li, and Pantelimon Stănică. On a conjecture for balanced symmetric Boolean functions. *Journal of Mathematical Cryptology*, 3(4):273–290, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Cusick:2016:AEM

[CLS16] Thomas W. Cusick, K. V. Lakshmy, and M. Sethumadhavan. Affine equivalence of monomial rotation symmetric Boolean functions: a Pólya's theorem approach. *Journal of Mathematical Cryptology*, 10(3–4):145–156, 2016. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Cheon:2020:EPS

[CLS20] Jung Hee Cheon, Kristin Lauter, and Yongsoo Song. Editor's preface for the Second Annual MathCrypt Proceedings volume. *Journal of Mathematical Cryptology*, 15(1):1–3, November 17, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2020-0170/html`.

Cheon:2020:PFA

[CLY20] Jung Hee Cheon, Kristin Lauter, and Donggeon Yhee. Preface to the First Annual MathCrypt Proceedings volume. *Journal of Mathe-*

matical Cryptology, 14(1):1–4, June 19, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2020-0060/html`.

Chakraborty:2022:MMA

[CN22] Bishwajit Chakraborty and Mridul Nandi. The mF mode of authenticated encryption with associated data. *Journal of Mathematical Cryptology*, 16(1): 73–97, January 2022. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2020-0054/html`.

Ciet:2011:CEC

[CQS11] Mathieu Ciet, Jean-Jacques Quisquater, and Francesco Sica. Compact elliptic curve representations. *Journal of Mathematical Cryptology*, 5(1):89–100, 2011. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Cascudo:2021:NSM

[CS21] Ignacio Cascudo and Reto Schnyder. A note on secure multiparty computation via higher residue symbols. *Journal of Mathematical Cryptology*, 15(1): 284–297, January 29, 2021. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2020-0013/html`.

Csirmaz:2020:SSD

[Csi20] Laszlo Csirmaz. Secret sharing and duality. *Journal of Mathematical Cryptology*, 15(1):157–173, November 25, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2019-0045/html`.

Craven:2022:EGT

[CW22] Matthew J. Craven and John R. Woodward. Evolution of group-theoretic cryptology attacks using hyper-heuristics. *Journal of Mathematical Cryptology*, 16(1): 49–63, January 2022. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2021-0017/html`.

Chee:2012:BCE

[CWZ12] Yeow Meng Chee, Huaxiong Wang, and Liang Feng Zhang. On the Bringer–Chabanne EPIR protocol for polynomial evaluation. *Journal of Mathematical Cryptology*, 5(3–4):277–301, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Dibert:2014:ISS

[DC14] Alexander Dibert and László Csirmaz. Infinite secret sharing — examples. *Journal of Mathematical Cryptology*, 8(2): 141–168, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Duquesne:2014:ECP

[DEF14] Sylvain Duquesne, Nadia El Mrabet, and Emmanuel Fouotsa. Efficient computation of pairings on Jacobi quartic elliptic curves. *Journal of Mathematical Cryptology*, 8(4):331–362, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Dolev:2015:TEP

[DGG+15] Shlomi Dolev, Juan Garay, Niv Gilboa, Vladimir Kolesnikov, and Yelena Yuditsky. Towards efficient private distributed computation on unbounded input streams. *Journal of Mathematical Cryptology*, 9(2):79–94, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

DeMicheli:2020:CON

[DHS20] Gabrielle De Micheli, Nadia Heninger, and Barak Shani. Characterizing overstretched NTRU attacks. *Journal of Mathematical Cryptology*, 14(1):110–119, June 14, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2015-0055/html`.

DeFeo:2014:TQR

[DJP14] Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *Journal of Mathematical Cryptology*, 8(3):209–247, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

DiCrescenzo:2020:DPG

[DKKS20] Giovanni Di Crescenzo, Matluba Khodjaeva, Delaram Kahrobaei, and Vladimir Shpilrain. Delegating a product of group exponentiations with application to signature schemes (submission to special NutMiC 2019 issue of JMC). *Journal of Mathematical Cryptology*, 14(1):438–459, October 30, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2019-0036/html`.

Delaplace:2020:CWB

[DM20] Claire Delaplace and Alexander May. Can we beat the square root bound for ECDLP over $\mathbf{F}_{p^2}$ via representation? *Journal of Mathematical Cryptology*, 14(1):293–306, August 18, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2019-0025/html`.

Demirkiran:2008:CHC

[DN08] Cevahir Demirkiran and Enric Nart. Counting hyperelliptic curves that admit a Koblitz model. *Journal of Mathematical Cryptology*, 2(2):163–179, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Dowden:2015:SMT

[Dow15] Chris Dowden. Secure message transmission in the presence of a fully generalised adversary. *Journal of Mathematical Cryptology*, 9(4):205–214, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Daemen:2007:PDC

[DR07] Joan Daemen and Vincent Rijmen. Probability distributions of correlation and differentials in block ciphers. *Journal of Mathematical Cryptology*, 1(3): 221–242, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Dehkordi:2017:CCG

[DS17] Massoud Hadian Dehkordi and Ali Safi. The complexity of the connected graph access structure on seven participants. *Journal of Mathematical Cryptology*, 11(1):25–35, 2017. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Dey:2018:GRB

[DS18] Sabyasachi Dey and Santanu Sarkar. Generalization of Roos bias in RC4 and some results on key–keystream relations. *Journal of Mathematical Cryptology*, 12(1):43–??, March 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/view/j/jmc.2018.12.issue-1/jmc-2016-0061/jmc-2016-0061.xml`.

Doroz:2020:FNE

[DS20] Yarkin Doröz and Berk Sunar. Flattening NTRU for evaluation key free homomorphic encryption. *Journal of Mathematical Cryptology*, 14(1):66–83, June 14, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2015-0052/html`.

Dugardin:2021:SMD

[DSG21] Margaux Dugardin, Werner Schindler, and Sylvain Guilley. Stochastic methods defeat regular RSA exponentiation algorithms with combined blinding methods. *Journal of Mathematical Cryptology*, 15(1):408–433, April 20, 2021. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2020-0010/html`.

Dachman-Soled:2020:SRL

[DSGKS20a] Dana Dachman-Soled, Huijing Gong, Mukul Kulkarni, and Aria Shahverdi. (In)Security of Ring-LWE under partial key exposure. *Journal of Mathematical Cryptology*, 15(1):72–86, November 17, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2020-0075/html`.

Dachman-Soled:2020:TRA

[DSGKS20b] Dana Dachman-Soled, Huijing Gong, Mukul Kulkarni, and Aria Shahverdi. Towards a ring analogue of the leftover hash lemma. *Journal of Mathematical Cryptology*, 15(1):87–110, November 17, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2020-0076/html`.

DiScala:2020:CNV

[DSS20] Antonio J. Di Scala, Carlo Sanna, and Edoardo Signorini. On the condition number of the Vandermonde matrix of the n th cyclotomic polynomial. *Journal of Mathematical Cryptology*, 15(1):174–178, November 25, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2020-0009/html`.

Dehkordi:2017:MDZ

[DT17] Massoud Hadian Dehkordi and Roghayeh Taghizadeh. Multiple differential-zero correlation linear cryptanalysis of reduced-round CAST-256. *Journal of Mathematical Cryptology*, 11(2): 55–62, June 2017. ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/view/j/jmc.2017.11.issue-2/jmc-2016-0054/jmc-2016-0054.xml`.

Duquesne:2011:RAA

[Duq11] Sylvain Duquesne. RNS arithmetic in $\mathbf{F}_{\mathbf{p}^k}$ and application to fast pairing computation. *Journal of Mathematical Cryptology*, 5(1):51–88, 2011. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Ekeraa:2021:QAC

[Eke21] Martin Ekerå. Quantum algorithms for computing general discrete logarithms and orders with tradeoffs. *Journal of Mathematical Cryptology*, 15(1):359–407, April 22, 2021. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2020-0006/html`.

Engelbert:2007:SMT

[EOS07] D. Engelbert, R. Overbeck, and A. Schmidt. A summary of McEliece-type cryptosystems and their security. *Journal of Mathematical Cryptology*, 1(2): 151–199, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Ferradi:2020:RSP

[FGG+20] Houda Ferradi, Rémi Géraud, Sylvain Guilley, David Naccache, and Mehdi Tibouchi. Recovering secrets from prefix-dependent leakage. *Journal of Mathematical Cryptology*, 14(1): 15–24, June 14, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/document/doi/10.1515/jmc-2015-0048/html.

Fuji-Hara:2008:TCM

[FHLMW08] Ryoh Fuji-Hara, Xiyang Li, Ying Miao, and Dianhua Wu. A TWOOA construction for multi-receiver multi-message authentication codes. *Journal of Mathematical Cryptology*, 2(1):9–28, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Field:2013:UCT

[FJ13] Rebecca E. Field and Brant C. Jones. Using carry-truncated addition to analyze add-rotate-xor hash algorithms. *Journal of Mathematical Cryptology*, 7 (2):97–110, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Fotiadis:2018:GPF

[FK18] Georgios Fotiadis and Elisavet Konstantinou. Generating pairing-friendly elliptic curve parameters using sparse families. *Journal of Mathematical Cryptology*, 12(2):83–99, June 2018. ISSN 1862-2976 (print), 1862-2984 (electronic).

Fancsali:2008:SAF

[FL08] Sz. L. Fancsali and P. Ligeti. Some applications of finite geometry for secure network coding. *Journal of Mathematical Cryptology*, 2(3):209–225, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Flori:2013:ECF

[FM13] Jean-Pierre Flori and Sihem Mesnager. An efficient characterization of a family of hyperbent functions with multiple trace terms. *Journal of Mathematical Cryptology*, 7(1):43–68, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Fischer:2009:SRF

[FMS09] Simon Fischer, Willi Meier, and Dirk Stegemann. Some remarks on FCSRs and implications for stream ciphers. *Journal of Mathematical Cryptology*, 3 (3):227–236, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Frougny:2008:MWE

[FS08] Christiane Frougny and Wolfgang Steiner. Minimal weight expansions in Pisot bases. *Journal of Mathematical Cryptology*, 2(4):365–392, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Friedlander:2009:DSS

[FS09] John B. Friedlander and Igor E. Shparlinski. On the density of some special primes. *Journal of Mathematical Cryptology*, 3(3): 265–271, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Fischlin:2011:SBS

[FS11] Marc Fischlin and Dominique Schröder. Security of blind signatures under aborts and applications to adaptive oblivious transfer. *Journal of Mathematical Cryptology*, 5(2):169–203, 2011. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Farashahi:2009:HEC

[FSV09] Reza R. Farashahi, Igor E. Shparlinski, and José Felipe Voloch. On hashing into elliptic curves. *Journal of Mathematical Cryptology*, 3(4):353–360, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Gallant:2012:FDL

[Gal12] Robert P. Gallant. Finding discrete logarithms with a set orbit distinguisher. *Journal of Mathematical Cryptology*, 6(1):1–20, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Gaudry:2007:FGA

[Gau07] P. Gaudry. Fast genus 2 arithmetic based on theta functions. *Journal of Mathematical Cryptology*, 1(3):243–265, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Gharahi:2013:PSS

[GD13] Motahhareh Gharahi and Massoud Hadian Dehkordi. Perfect secret sharing schemes for graph access structures on six participants. *Journal of Mathematical Cryptology*, 7(2):143–146, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Goel:2020:SSA

[GGD20] Neha Goel, Indivar Gupta, and B. K. Dass. Survey on SAP and its application in public-key cryptography. *Journal of Mathematical Cryptology*, 14(1): 144–152, July 3, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2016-0004/html`.

Garber:2015:LBA

[GKL15] David Garber, Delaram Kahrobaei, and Ha T. Lam. Length-based attacks in polycyclic groups. *Journal of Mathematical Cryptology*, 9(1):33–43, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Galbraith:2007:SPC

[GÓS07] Steven D. Galbraith, Colm Ó hÉigeartaigh, and Caroline Sheedy. Simplified pairing computation and security implications. *Journal of Mathematical Cryptology*, 1(3):267–281, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Gaal:2009:SNE

[GP09] István Gaál and Michael E. Pohst. On solving norm equations in global function fields. *Journal of Mathematical Cryptology*, 3(3):237–248, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Grosek:2013:CS

[GP13] Otokar Grošek and Štefan Porubský. Coprime solutions to $ax \equiv b \pmod{n}$. *Journal of Mathematical Cryptology*, 7(3): 217–224, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Gupta:2017:ADT

[GPR17] Kishan Chand Gupta, Sumit Kumar Pandey, and Indranil Ghosh Ray. Applications of design theory for the constructions of MDS matrices for lightweight cryptography. *Journal of Mathematical Cryptology*, 11(2):85–116, June 2017. ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/view/j/jmc.2017.11.issue-2/jmc-2016-0013/jmc-2016-0013.xml.

Galbraith:2009:DMS

[GPRS09] Steven D. Galbraith, Jordi Pujolàs, Christophe Ritzenthaler, and Benjamin Smith. Distortion maps for supersingular genus two curves. *Journal of Mathematical Cryptology*, 3(1):1–18, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Grzeskowiak:2020:VLS

[Grz20] Maciej Grześkowiak. A variant of the large sieve inequality with explicit constants. *Journal of Mathematical Cryptology*, 14(1):307–315, August 7, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/document/doi/10.1515/jmc-2019-0022/html.

Gutierrez:2009:FSW

[Gut09] Jaime Gutierrez. Foreword: Second Workshop on Mathematical Cryptology. *Journal of Mathematical Cryptology*, 3(3): 175–176, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). Held in Santander, October 23–25, 2008.

Galbraith:2013:SPH

[GZ13] Steven D. Galbraith and Chang-An Zhao. Self-pairings on hyperelliptic curves. *Journal of Mathematical Cryptology*, 7(1):31–42, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). See erratum [GZ14].

Galbraith:2014:ESP

[GZ14] Steven D. Galbraith and Chang-An Zhao. Erratum: Self-pairings on hyperelliptic curves [J. Math. Cryptol. **7** (2013), 31–42] [MR3101014]. *Journal of Mathematical Cryptology*, 8 (1):93, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). See [GZ13].

Harayama:2007:WSB

[HF07] Tomohiro Harayama and Donald K. Friesen. Weil sum for birthday attack in multivariate quadratic cryptosystem. *Journal of Mathematical Cryptology*, 1(1):79–104, 2007. CODEN ????

ISSN 1862-2976 (print), 1862-2984 (electronic).

Hinek:2008:SMP

[Hin08] M. Jason Hinek. On the security of multi-prime RSA. *Journal of Mathematical Cryptology*, 2(2): 117–147, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Hitt:2009:FGC

[Hit09] Laura Hitt. Families of genus 2 curves with small embedding degree. *Journal of Mathematical Cryptology*, 3(1):19–36, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Huang:2020:QSP

[HKP+20] Ming-Deh Huang, Michiel Kosters, Christophe Petit, Sze Ling Yeo, and Yang Yun. Quasi-subfield polynomials and the elliptic curve discrete logarithm problem. *Journal of Mathematical Cryptology*, 14(1): 25–38, June 14, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/document/doi/10.1515/jmc-2015-0049/html.

Hinek:2009:ALS

[HL09] M. Jason Hinek and Charles C. Y. Lam. Another look at some fast modular arithmetic methods. *Journal of Mathematical Cryptology*, 3(2):165–174, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Hinek:2010:CMA

[HL10] M. Jason Hinek and Charles C. Y. Lam. Common modulus attacks on small private exponent RSA and some fast variants (in practice). *Journal of Mathematical Cryptology*, 4(1):57–93, 2010. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Harsanyi:2019:EIR

[HL19] Károly Harsányi and Péter Ligeti. Exact information ratios for secret sharing on small graphs with girth at least 5. *Journal of Mathematical Cryptology*, 13(2):107–??, June 2019. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL http://www.degruyter.com/view/j/jmc.2019.13.issue-2/jmc-2018-0024/jmc-2018-0024.xml.

Heuberger:2007:MWC

[HM07] Clemens Heuberger and James A. Muir. Minimal weight and colexicographically minimal integer representations. *Journal of Mathematical Cryptology*, 1(4): 297–328, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Hartung:2008:ISB

[HS08] Rupert J. Hartung and Claus-Peter Schnorr. Identification and signatures based on NP-hard problems of indefinite quadratic forms. *Journal of Mathematical Cryptology*, 2(4):

327–341, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Hameed:2015:CIW

[HS15a] Ali Hameed and Arkadii Slinko. A characterisation of ideal weighted secret sharing schemes. *Journal of Mathematical Cryptology*, 9(4):227–244, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Henry:2015:LAR

[HS15b] Kevin J. Henry and Douglas R. Stinson. Linear approaches to resilient aggregation in sensor networks. *Journal of Mathematical Cryptology*, 9(4):245–272, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Hakuta:2010:EAS

[HST10] Keisuke Hakuta, Hisayoshi Sato, and Tsuyoshi Takagi. Efficient arithmetic on subfield elliptic curves over small finite fields of odd characteristic. *Journal of Mathematical Cryptology*, 4(3): 199–238, 2010. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Hoffstein:2020:SSF

[HSWZ20] Jeffrey Hoffstein, Joseph H. Silverman, William Whyte, and Zhenfei Zhang. A signature scheme from the finite field isomorphism problem. *Journal of Mathematical Cryptology*, 14(1): 39–54, June 14, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2015-0050/html`.

Haridas:2014:SAM

[HVV14] Deepthi Haridas, Sarma Venkataraman, and Geeta Varadan. Security analysis of modified Rivest scheme. *Journal of Mathematical Cryptology*, 8(3):297–303, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Hisil:2011:EAG

[HWCD11] Huseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter, and Ed Dawson. An exploration of affine group laws for elliptic curves. *Journal of Mathematical Cryptology*, 5(1):1–50, 2011. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Jirakitpuwapat:2018:NMC

[JCK+18] Wachirapong Jirakitpuwapat, Parin Chaipunya, Poom Kumam, Sompong Dhompongsa, and Phatiphat Thounthong. New methods of construction of Cartesian authentication codes from geometries over finite commutative rings. *Journal of Mathematical Cryptology*, 12 (3):119–??, September 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/view/j/jmc.2018.12.issue-3/jmc-2017-0057/jmc-2017-0057.xml`.

Jiang:2014:PAP

[Jia14] Shaoquan Jiang. Persistent asymmetric password-based key exchange. *Journal of Mathematical Cryptology*, 8(1):31–70, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Jao:2020:STP

[JLLRL20] David Jao, Jason LeGrow, Christopher Leonardi, and Luis Ruiz-Lopez. A subexponential-time, polynomial quantum space algorithm for inverting the CM group action. *Journal of Mathematical Cryptology*, 14(1): 129–138, June 14, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2015-0057/html`.

Joye:2020:EPR

[JLNN20] Marc Joye, Oleksandra Lapiha, Ky Nguyen, and David Naccache. The eleventh power residue symbol. *Journal of Mathematical Cryptology*, 15(1): 111–122, November 17, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2020-0077/html`.

Jha:2016:RSG

[JN16] Ashwin Jha and Mridul Nandi. Revisiting structure graphs: applications to CBC–MAC and EMAC. *Journal of Mathematical Cryptology*, 10(3–4):157–180, 2016. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Joye:2020:PEA

[Joy20] Marc Joye. Protecting ECC against fault attacks: The ring extension method revisited. *Journal of Mathematical Cryptology*, 14(1):254–267, August 1, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2019-0030/html`.

Joux:2020:PNT

[JP20] Antoine Joux and Jacek Pomykała. Preface for the Number-Theoretic Methods in Cryptology conferences. *Journal of Mathematical Cryptology*, 14(1):393–396, October 13, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2019-0111/html`.

Jhanwar:2013:USI

[JSN13] Mahabir P. Jhanwar and Reihaneh Safavi-Naini. Unconditionally-secure ideal robust secret sharing schemes for threshold and multilevel access structure. *Journal of Mathematical Cryptology*, 7(4):279–296, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Justus:2014:DQR

[Jus14] Benjamin Justus. The distribution of quadratic residues and non-residues in the Goldwasser–Micali type of cryptosystem. *Journal of Mathematical Cryptology*, 8(2):115–140, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Justus:2015:DQR

[Jus15] Benjamin Justus. The distribution of quadratic residues and non-residues in the Goldwasser–Micali type of cryptosystem. II. *Journal of Mathematical Cryptology*, 9(2):115–137, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Wei:2012:FMP

[jWW12] Tzer jen Wei and Lih-Chung Wang. A fast mental poker protocol. *Journal of Mathematical Cryptology*, 6(1):39–68, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Karabina:2010:FCC

[Kar10] Koray Karabina. Factor-4 and 6 compression of cyclotomic subgroups of $\mathbf{F}^*_{2^{4m}}$ and $\mathbf{F}^*_{3^{6m}}$. *Journal of Mathematical Cryptology*, 4(1):1–42, 2010. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Karmakar:2020:EPF

[Kar20a] Sudhangshu B. Karmakar. An elementary proof of Fermat's Last Theorem for all even exponents. *Journal of Mathematical Cryptology*, 14(1):139–142, July 3, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2016-0018/html`. See retraction [Kar20b].

Karmakar:2020:REP

[Kar20b] Sudhangshu B. Karmakar. Retraction of: An elementary proof of Fermat's Last Theorem for all even exponents. *Journal of Mathematical Cryptology*, 14 (1):143, July 3, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2017-2000/html`. See [Kar20a].

Kortelainen:2010:MAG

[KHK10] Juha Kortelainen, Kimmo Halunen, and Tuomas Kortelainen. Multicollision attacks and generalized iterated hash functions. *Journal of Mathematical Cryptology*, 4(3):239–270, 2010. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Koblitz:2008:ALN

[KM08] Neal Koblitz and Alfred Menezes. Another look at non-standard discrete log and Diffie–Hellman problems. *Journal of Mathematical Cryptology*, 2(4):311–326, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Koblitz:2013:ALH

[KM13] Neal Koblitz and Alfred Menezes. Another look at HMAC. *Journal of Mathematical Cryptology*,

7(3):225–251, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Kaji:2019:PEP

[KMNN19] Shizuo Kaji, Toshiaki Maeno, Koji Nuida, and Yasuhide Numata. Polynomial expressions of p-ary auction functions. *Journal of Mathematical Cryptology*, 13(2):69–??, June 2019. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL http://www.degruyter.com/view/j/jmc.2019.13.issue-2/jmc-2018-0016/jmc-2018-0016.xml.

Karabina:2010:AEW

[KMPS10] Koray Karabina, Alfred Menezes, Carl Pomerance, and Igor E. Shparlinski. On the asymptotic effectiveness of Weil descent attacks. *Journal of Mathematical Cryptology*, 4(2):175–191, 2010. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Kotov:2020:AKP

[KMU20] Matvei Kotov, Anton Menshov, and Alexander Ushakov. Attack on kayawood protocol: uncloaking private keys. *Journal of Mathematical Cryptology*, 15 (1):237–249, December 1, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/document/doi/10.1515/jmc-2019-0015/html.

Kurosawa:2013:NLR

[KNP13] Kaoru Kurosawa, Ryo Nojima, and Le Trieu Phong. New leakage-resilient CCA-secure public key encryption. *Journal of Mathematical Cryptology*, 7 (4):297–312, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Koblitz:2007:ALA

[Kob07] Neal Koblitz. Another look at automated theorem-proving. *Journal of Mathematical Cryptology*, 1(4):385–403, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Koblitz:2012:ALA

[Kob12] Neal Koblitz. Another look at automated theorem-proving II. *Journal of Mathematical Cryptology*, 5(3–4):205–224, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Kim:2020:EAC

[KT20] Taechan Kim and Mehdi Tibouchi. Equidistribution among cosets of elliptic curve points in intervals. *Journal of Mathematical Cryptology*, 14(1):339–345, August 7, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/document/doi/10.1515/jmc-2019-0020/html.

Kotov:2015:ACP

[KU15] Matvei Kotov and Alexander Ushakov. Analysis of a certain polycyclic-group-based cryptosystem. *Journal of Mathematical Cryptology*, 9(3):161–167, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Kotov:2018:AKE

[KU18] Matvei Kotov and Alexander Ushakov. Analysis of a key exchange protocol based on tropical matrix algebra. *Journal of Mathematical Cryptology*, 12(3):137–??, September 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/view/j/jmc.2018.12.issue-3/jmc-2016-0064/jmc-2016-0064.xml`.

Kushwaha:2018:ILB

[Kus18] Prabhat Kushwaha. Improved lower bound for Diffie–Hellman problem using multiplicative group of a finite field as auxiliary group. *Journal of Mathematical Cryptology*, 12(2):101–118, June 2018. ISSN 1862-2976 (print), 1862-2984 (electronic).

Kousidis:2019:FFD

[KW19] Stavros Kousidis and Andreas Wiemers. On the first fall degree of summation polynomials. *Journal of Mathematical Cryptology*, 13(3–4):229–??, September 2019. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `http://www.degruyter.com/view/j/jmc.2019.13.issue-3-4/jmc-2017-0022/jmc-2017-0022.xml`.

Laarhoven:2020:AVC

[Laa20] Thijs Laarhoven. Approximate Voronoi cells for lattices, revisited. *Journal of Mathematical Cryptology*, 15(1):60–71, November 17, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2020-0074/html`.

Li:2007:SAC

[LC07] Yuan Li and T. W. Cusick. Strict avalanche criterion over finite fields. *Journal of Mathematical Cryptology*, 1(1):65–78, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Lavauzelle:2019:GCP

[LdV19] Julien Lavauzelle and Françoise Levy dit Vehel. Generic constructions of PoRs from codes and instantiations. *Journal of Mathematical Cryptology*, 13(2):81–??, June 2019. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `http://www.degruyter.com/view/j/jmc.2019.13.issue-2/jmc-2018-0018/jmc-2018-0018.xml`.

Laine:2015:TMT

[LL15] Kim Laine and Kristin Lauter. Time-memory trade-offs for index calculus in genus 3. *Journal of Mathematical Cryptology*, 9(2):95–114, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Luykx:2015:TPB

[LMPW15] Atul Luykx, Bart Mennink, Bart Preneel, and Laura Winnen. Two-permutation-based hashing with binary mixing. *Journal of Mathematical Cryptology*, 9(3):139–150, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Lamberger:2009:NSC

[LNR09] Mario Lamberger, Tomislav Nad, and Vincent Rijmen. Numerical solvers and cryptanalysis. *Journal of Mathematical Cryptology*, 3(3):249–263, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Lu:2017:CRV

[LPS17] Yao Lu, Liqiang Peng, and Santanu Sarkar. Cryptanalysis of an RSA variant with moduli $N = p^r q^l$. *Journal of Mathematical Cryptology*, 11(2):117–130, June 2017. ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/view/j/jmc.2017.11.issue-2/jmc-2016-0025/jmc-2016-0025.xml.

Lesavourey:2020:SPI

[LPS20] Andrea Lesavourey, Thomas Plantard, and Willy Susilo. Short principal ideal problem in multicubic fields. *Journal of Mathematical Cryptology*, 14(1): 359–392, August 20, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/document/doi/10.1515/jmc-2019-0028/html.

Lange:2007:DSS

[LS07] Tanja Lange and Igor E. Shparlinski. Distribution of some sequences of points on elliptic curves. *Journal of Mathematical Cryptology*, 1(1):1–11, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Laing:2018:SRR

[LS18] Thalia M. Laing and Douglas R. Stinson. A survey and refinement of repairable threshold schemes. *Journal of Mathematical Cryptology*, 12(1):57–??, March 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/view/j/jmc.2018.12.issue-1/jmc-2017-0058/jmc-2017-0058.xml.

Longrigg:2008:CSC

[LU08] Jonathan Longrigg and Alexander Ushakov. Cryptanalysis of the shifted conjugacy authentication protocol. *Journal of Mathematical Cryptology*, 2(2): 109–116, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Mohammed:2017:RNF

[MA17] Ahmed Mohammed and Abdulrahman Alkhelaifi. RSA: A number of formulas to improve the search for $p + q$. *Journal of Mathematical Cryptology*, 11(4): 195–203, 2017. ISSN 1862-2976 (print), 1862-2984 (electronic).

Magliveras:2013:F

[Mag13] Spyros S. Magliveras. Foreword. *Journal of Mathematical Cryptology*, 7(3):181–182, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/view/j/jmc.2013.7.issue-3/jmc-2013-5001/jmc-2013-5001.xml.

Maze:2012:AKD

[Maz12] Gérard Maze. Analysis of a key distribution scheme in secure multicasting. *Journal of Mathematical Cryptology*, 6(1):69–80, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Menezes:2007:ALH

[Men07] Alfred Menezes. Another look at HMQV. *Journal of Mathematical Cryptology*, 1(1):47–64, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Marti-Farre:2010:SSS

[MFP10] Jaume Martí-Farré and Carles Padró. On secret sharing schemes, matroids and polymatroids. *Journal of Mathematical Cryptology*, 4(2):95–120, 2010. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Mie:2008:PTR

[Mie08] Thilo Mie. Polylogarithmic two-round argument systems. *Journal of Mathematical Cryptology*, 2(4):343–363, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Martin:2007:CGC

[MN07] Keith Martin and Siaw-Lynn Ng. The combinatorics of generalised cumulative arrays. *Journal of Mathematical Cryptology*, 1(1):13–32, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Morales:2008:ADE

[Mor08] David J. Mireles Morales. An attack on disguised elliptic curves. *Journal of Mathematical Cryptology*, 2(1):1–8, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Murphy:2008:GVC

[MP08] S. Murphy and M. B. Paterson. A geometric view of cryptographic equation solving. *Journal of Mathematical Cryptology*, 2(1):63–107, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Murphy:2020:DPD

[MP20] Sean Murphy and Rachel Player. Discretisation and product distributions in Ring-LWE. *Journal of Mathematical Cryptology*, 15(1):45–59, November 17, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/document/doi/10.1515/jmc-2020-0073/html.

Moody:2016:ISF

[MPST16] Dustin Moody, Souradyuti Paul, and Daniel Smith-Tone. Indifferentiability security of the fast wide pipe hash: breaking the birthday barrier. *Journal of Mathematical Cryptology*, 10(2): 101–133, 2016. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

McGuire:2020:LST

[MR20] Gary McGuire and Oisín Robinson. Lattice sieving in three dimensions for discrete log in medium characteristic. *Journal of Mathematical Cryptology*, 15(1):223–236, November 25, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2020-0008/html`.

Mouha:2012:CIR

[MSP12] Nicky Mouha, Gautham Sekar, and Bart Preneel. Challenging the increased resistance of regular hash functions against birthday attacks. *Journal of Mathematical Cryptology*, 6(3–4):229–248, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/view/j/jmc.2012.6.issue-3-4/jmc-2011-0010/jmc-2011-0010.xml`.

Myasnikov:2008:RSA

[MU08] Alexei G. Myasnikov and Alexander Ushakov. Random subgroups and analysis of the length-based and quotient attacks. *Journal of Mathematical Cryptology*, 2(1):29–61, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Mosina:2010:MSA

[MU10] Natalia Mosina and Alexander Ushakov. Mean-set attack: cryptanalysis of Sibert et al. authentication protocol. *Journal of Mathematical Cryptology*, 4 (2):149–174, 2010. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Myasnikov:2014:CMC

[MU14] Alex D. Myasnikov and Alexander Ushakov. Cryptanalysis of matrix conjugation schemes. *Journal of Mathematical Cryptology*, 8(2):95–114, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Mullan:2011:CVS

[Mul11] Ciaran Mullan. Cryptanalysing variants of Stickel's key agreement scheme. *Journal of Mathematical Cryptology*, 4(4):365–373, 2011. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Murphy:2012:ELH

[Mur12] Sean Murphy. The effectiveness of the linear hull effect. *Journal of Mathematical Cryptology*, 6 (2):137–147, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/view/j/jmc.2012.6.issue-2/jmc-2011-0025/jmc-2011-0025.xml`.

Moody:2012:FEC

[MW12] Dustin Moody and Hongfeng Wu. Families of elliptic curves with rational 3-torsion. *Journal of Mathematical Cryptology*, 5(3–4):225–246, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Nandi:2009:ISA

[Nan09] Mridul Nandi. Improved security analysis for OMAC as a pseudorandom function. *Journal of Mathematical Cryptology*, 3(2):133–148, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Nandi:2008:ISA

[NM08] Mridul Nandi and Avradip Mandal. Improved security analysis of PMAC. *Journal of Mathematical Cryptology*, 2(2): 149–162, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Nandi:2016:SJS

[NP16] Mridul Nandi and Tapas Pandit. On the security of joint signature and encryption revisited. *Journal of Mathematical Cryptology*, 10(3–4):181–221, 2016. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Nandi:2019:PSP

[NP19] Mridul Nandi and Tapas Pandit. Predicate signatures from pair encodings via dual system proof technique. *Journal of Mathematical Cryptology*, 13(3–4):197–??, September 2019. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `http://www.degruyter.com/view/j/jmc.2019.13.issue-3-4/jmc-2017-0007/jmc-2017-0007.xml`.

Neven:2009:HFR

[NSW09] Gregory Neven, Nigel P. Smart, and Bogdan Warinschi. Hash function requirements for Schnorr signatures. *Journal of Mathematical Cryptology*, 3(1):69–87, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Nguyen:2008:SAS

[NV08] Phong Q. Nguyen and Thomas Vidick. Sieve algorithms for the shortest vector problem are practical. *Journal of Mathematical Cryptology*, 2(2):181–207, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Okano:2012:VCF

[Oka12] Keiji Okano. On the ρ-values of complete families of pairing-friendly elliptic curves. *Journal of Mathematical Cryptology*, 6 (3–4):249–268, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/view/j/jmc.2012.6.issue-3-4/jmc-2012-0011/jmc-2012-0011.xml?format=INT`.

Orumiehchiha:2013:SAL

[OPSB13] Mohammad Ali Orumiehchiha, Josef Pieprzyk, Ron Steinfeld, and Harry Bartlett. Security analysis of linearly filtered NLF-SRs. *Journal of Mathematical Cryptology*, 7(4):313–332, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Omar:2014:FHF

[OS14] Sami Omar and Houssem Sabri. Fast hash functions and convolution product. *Journal of Mathematical Cryptology*, 8(2): 169–187, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Partala:2018:AGD

[Par18] Juha Partala. Algebraic generalization of Diffie–Hellman key exchange. *Journal of Mathematical Cryptology*, 12(1):1–??, March 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/view/j/jmc.2018.12.issue-1/jmc-2017-0015/jmc-2017-0015.xml.

Persichetti:2012:CMK

[Per12] Edoardo Persichetti. Compact McEliece keys based on quasi-dyadic Srivastava codes. *Journal of Mathematical Cryptology*, 6 (2):149–169, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/view/j/jmc.2012.6.issue-2/jmc-2011-0099/jmc-2011-0099.xml.

Pandey:2020:ICE

[PGS20] Atul Pandey, Indivar Gupta, and Dhiraj Kumar Singh. Improved cryptanalysis of a ElGamal cryptosystem based on matrices over group rings. *Journal of Mathematical Cryptology*, 15 (1):266–279, December 20, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/document/doi/10.1515/jmc-2019-0054/html.

Popov:2017:DTP

[Pop17] Serguei Popov. On a decentralized trustless pseudo-random number generation algorithm. *Journal of Mathematical Cryptology*, 11(1):37–43, 2017. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Poulakis:2016:NLA

[Pou16] Dimitrios Poulakis. New lattice attacks on DSA schemes. *Journal of Mathematical Cryptology*, 10(2):135–144, 2016. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Pinto:2018:BPF

[PP18] Eduardo Carvalho Pinto and Christophe Petit. Better path-finding algorithms in LPS Ramanujan graphs. *Journal of Mathematical Cryptology*, 12(4): 191–??, December 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/view/j/jmc.2018.12.issue-4/jmc-2017-0051/jmc-2017-0051.xml.

Pomykala:2020:IFC

[PR20] Jacek Pomykała and Maciej Radziejewski. Integer factoring and compositeness witnesses. *Journal of Mathematical Cryptology*, 14(1):346–358, August 20, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/document/doi/10.1515/jmc-2019-0023/html.

Paterson:2008:TAS

[PS08] M. B. Paterson and D. R. Stinson. Two attacks on a sensor network key distribution scheme of Cheng and Agrawal. *Journal of Mathematical Cryptology*, 2 (4):393–403, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Paterson:2015:OCI

[PS15] Maura B. Paterson and Douglas R. Stinson. Optimal constructions for ID-based one-way-function key predistribution schemes realizing specified communication graphs. *Journal of Mathematical Cryptology*, 9 (4):215–225, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Paterson:2020:EAC

[PS20] Maura B. Paterson and Douglas R. Stinson. On the equivalence of authentication codes and robust $(2, 2)$-threshold schemes. *Journal of Mathematical Cryptology*, 15(1):179–196, November 25, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/document/doi/10.1515/jmc-2019-0048/html.

Paterson:2013:CTF

[PSU13] Maura B. Paterson, Douglas R. Stinson, and Jalaj Upadhyay. A coding theory foundation for the analysis of general unconditionally secure proof-of-retrievability schemes for cloud storage. *Journal of Mathematical Cryptology*, 7(3):183–216, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Paterson:2018:MPP

[PSU18] Maura B. Paterson, Douglas R. Stinson, and Jalaj Upadhyay. Multi-prover proof of retrievability. *Journal of Mathematical Cryptology*, 12(4):203–??, December 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/view/j/jmc.2018.12.issue-4/jmc-2018-0012/jmc-2018-0012.xml.

Reichl:2017:TLS

[Rei17] Dominik Reichl. Tame logarithmic signatures of abelian groups. *Journal of Mathematical Cryptology*, 11(4):205–214, 2017. ISSN 1862-2976 (print), 1862-2984 (electronic).

Reid:2021:UIE

[Rei21] Elizabeth M. Reid. Using inclusion/exclusion to find bent and balanced monomial rotation symmetric functions. *Journal of Mathematical Cryptology*, 15 (1):298–304, January 29, 2021. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2020-0021/html`.

Rudy:2020:RTK

[RM20] Dylan Rudy and Chris Monico. Remarks on a tropical key exchange system. *Journal of Mathematical Cryptology*, 15(1): 280–283, December 20, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2019-0061/html`.

Rahman:2022:MMA

[RS22] Nael Rahman and Vladimir Shpilrain. MAKE: a matrix action key exchange. *Journal of Mathematical Cryptology*, 16(1): 64–72, January 2022. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2020-0053/html`. See successful attack [BKL22].

Ruinskiy:2007:LBC

[RST07] Dima Ruinskiy, Adi Shamir, and Boaz Tsaban. Length-based cryptanalysis: the case of Thompson's group. *Journal of Mathematical Cryptology*, 1(4): 359–372, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Raddum:2018:MSB

[RZ18] Håvard Raddum and Pavol Zajac. MRHS solver based on linear algebra and exhaustive search. *Journal of Mathematical Cryptology*, 12(3):143–??, September 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/view/j/jmc.2018.12.issue-3/jmc-2017-0005/jmc-2017-0005.xml`.

Schindler:2008:ASM

[Sch08] Werner Schindler. Advanced stochastic methods in side channel analysis on block ciphers in the presence of masking. *Journal of Mathematical Cryptology*, 2(3):291–310, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Scholl:2017:IEC

[Sch17] Travis Scholl. Isolated elliptic curves and the MOV attack. *Journal of Mathematical Cryptology*, 11(3):131–146, 2017. ISSN 1862-2976 (print), 1862-2984 (electronic).

Sha:2014:NIC

[Sha14] Min Sha. On the non-idealness of cyclotomic families of pairing-friendly elliptic curves. *Journal of Mathematical Cryptology*, 8

(4):417–440, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Shokrieh:2010:MPD

[Sho10] Farbod Shokrieh. The monodromy pairing and discrete logarithm on the Jacobian of finite graphs. *Journal of Mathematical Cryptology*, 4(1):43–56, 2010. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Sica:2020:FH

[Sic20] Francesco Sica. Factoring with hints. *Journal of Mathematical Cryptology*, 15(1):123–130, November 17, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/document/doi/10.1515/jmc-2020-0078/html.

Silverman:2007:OPS

[Sil07] Robert D. Silverman. Optimal parameterization of SNFS. *Journal of Mathematical Cryptology*, 1(2):105–124, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Santini:2022:RFC

[SPB22] Paolo Santini, Edoardo Persichetti, and Marco Baldi. Reproducible families of codes and cryptographic applications. *Journal of Mathematical Cryptology*, 16(1):20–48, January 2022. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/document/doi/10.1515/jmc-2020-0003/html.

Sipasseuth:2019:EGG

[SPS19] Arnaud Sipasseuth, Thomas Plantard, and Willy Susilo. Enhancing Goldreich, Goldwasser and Halevi's scheme with intersecting lattices. *Journal of Mathematical Cryptology*, 13(3–4):169–??, September 2019. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL http://www.degruyter.com/view/j/jmc.2019.13.issue-3-4/jmc-2016-0066/jmc-2016-0066.xml.

Sepahi:2012:NSN

[SPSS12] Reza Sepahi, Josef Pieprzyk, Siamak F. Shahandashti, and Berry Schoenmakers. New security notions and relations for public-key encryption. *Journal of Mathematical Cryptology*, 6 (3–4):183–227, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Saxena:2009:CPB

[SS09] Amitabh Saxena and Ben Soh. A cryptographic primitive based on hidden-order groups. *Journal of Mathematical Cryptology*, 3(2):89–132, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Samajder:2016:ALN

[SS16a] Subhabrata Samajder and Palash Sarkar. Another look at normal approximations in cryptanalysis. *Journal of Mathematical Cryptology*, 10(2):69–99, 2016. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Swanson:2016:USS

[SS16b] Colleen M. Swanson and Douglas R. Stinson. Unconditionally secure signature schemes revisited. *Journal of Mathematical Cryptology*, 10(1):35–67, 2016. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Samajder:2017:RUB

[SS17] Subhabrata Samajder and Palash Sarkar. Rigorous upper bounds on data complexities of block cipher cryptanalysis. *Journal of Mathematical Cryptology*, 11(3):147–175, 2017. ISSN 1862-2976 (print), 1862-2984 (electronic).

Saraswat:2017:SAP

[SSA17] Vishal Saraswat, Rajeev Anand Sahu, and Amit K. Awasthi. A secure anonymous proxy signcryption scheme. *Journal of Mathematical Cryptology*, 11(2):63–84, June 2017. ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/view/j/jmc.2017.11.issue-2/jmc-2015-0014/jmc-2015-0014.xml`.

Singh:2011:PDE

[SSS11] Rajesh P. Singh, A. Saikia, and B. K. Sarma. Poly-dragon: an efficient multivariate public key cryptosystem. *Journal of Mathematical Cryptology*, 4(4):349–364, 2011. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Stinson:2014:EDS

[SU14] Douglas R. Stinson and Jalaj Upadhyay. Is extracting data the same as possessing data? *Journal of Mathematical Cryptology*, 8(2):189–207, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Svaba:2010:PKC

[SvT10] Pavol Svaba and Tran van Trung. Public key cryptosystem MST_3: cryptanalysis and realization. *Journal of Mathematical Cryptology*, 4(3):271–315, 2010. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Staszewski:2013:SAL

[SvT13] Reiner Staszewski and Tran van Trung. Strongly aperiodic logarithmic signatures. *Journal of Mathematical Cryptology*, 7(2):147–179, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/view/j/jmc.2013.7.issue-2/jmc-2013-5000/jmc-2013-5000.xml`.

Stinson:2007:SRQ

[SW07a] D. R. Stinson and R. Wei. Some results on query processes and reconstruction functions for unconditionally secure 2-server 1-round binary private information retrieval protocols. *Journal of Mathematical Cryptology*, 1(1):33–46, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Stinson:2007:EST

[SW07b] D. R. Stinson and J. Wu. An efficient and secure two-flow zero-knowledge identification protocol. *Journal of Mathematical Cryptology*, 1(3):201–220, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Sparr:2015:RFK

[SW15] Rüdiger Sparr and Ralph Wernsdorf. The round functions of KASUMI generate the alternating group. *Journal of Mathematical Cryptology*, 9(1):23–32, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Tischhauser:2011:NCA

[Tis11] Elmar Tischhauser. Nonsmooth cryptanalysis, with an application to the stream cipher MICKEY. *Journal of Mathematical Cryptology*, 4(4): 317–348, 2011. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Tassa:2013:OEM

[TJBY13] Tamir Tassa, Ayman Jarrous, and Yonatan Ben-Ya'akov. Oblivious evaluation of multivariate polynomials. *Journal of Mathematical Cryptology*, 7 (1):1–29, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Takahashi:2020:AAS

[TKF+20] Yasushi Takahashi, Momonari Kudo, Ryoya Fukasaku, Yasuhiko Ikematsu, Masaya Yasuda, and Kazuhiro Yokoyama. Algebraic approaches for solving isogeny problems of prime power degrees. *Journal of Mathematical Cryptology*, 15(1):31–44, November 17, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2020-0072/html`.

Tsaban:2015:CMS

[TL15] Boaz Tsaban and Noam Lifshitz. Cryptanalysis of the MORE symmetric key fully homomorphic encryption scheme. *Journal of Mathematical Cryptology*, 9(2):75–78, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Tomkins:2020:NZT

[TNS20] Hayley Tomkins, Monica Nevins, and Hadi Salmasian. New Zémor–Tillich type hash functions over $\mathrm{GL}_2(\mathbf{F}_{p^n})$. *Journal of Mathematical Cryptology*, 14(1): 236–253, August 1, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2019-0033/html`.

Taraskin:2020:TIB

[TSJL20] Oleg Taraskin, Vladimir Soukharev, David Jao, and Jason T. LeGrow. Towards isogeny-based password-authenticated key establishment. *Journal of Mathematical Cryptology*, 15(1):18–30, November 17, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/document/doi/10.1515/jmc-2020-0071/html.

Tibouchi:2020:OBA

[TW20] Mehdi Tibouchi and Alexandre Wallet. One bit is all it takes: A devastating timing attack on BLISS's non-constant time sign flips. *Journal of Mathematical Cryptology*, 15(1):131–142, November 17, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/document/doi/10.1515/jmc-2020-0079/html.

Urbanik:2020:NTS

[UJ20] David Urbanik and David Jao. New techniques for SIDH-based NIKE. *Journal of Mathematical Cryptology*, 14(1):120–128, June 14, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/document/doi/10.1515/jmc-2015-0056/html.

vanTrung:2018:CSA

[vT18] Tran van Trung. Construction of strongly aperiodic logarithmic signatures. *Journal of Mathematical Cryptology*, 12(1):23–??, March 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/view/j/jmc.2018.12.issue-1/jmc-2017-0048/jmc-2017-0048.xml.

vonzurGathen:2009:SSP

[vzGS09] Joachim von zur Gathen and Igor E. Shparlinski. Subset sum pseudorandom numbers: fast generation and distribution. *Journal of Mathematical Cryptology*, 3(2):149–163, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

vonzurGathen:2013:GSP

[vzGS13] Joachim von zur Gathen and Igor E. Shparlinski. Generating safe primes. *Journal of Mathematical Cryptology*, 7(4):333–365, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Walker:2007:PHF

[WC07] Robert A. Walker II and Charles J. Colbourn. Perfect Hash families: constructions and existence. *Journal of Mathematical Cryptology*, 1(2):125–150, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Wang:2013:MCN

[WL13] Tianze Wang and Dongdai Lin. A method for counting the number of polynomial equivalence classes. *Journal of Mathematical Cryptology*, 7(1):69–95, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Wolf:2011:EKU

[WP11] Christopher Wolf and Bart Preneel. Equivalent keys in $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic public key systems. *Journal of Mathematical Cryptology*, 4(4): 375–415, 2011. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Wu:2009:EIP

[WS09] J. Wu and D. R. Stinson. An efficient identification protocol secure against concurrent-reset attacks. *Journal of Mathematical Cryptology*, 3(4):339–352, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Wunderer:2019:DAH

[Wun19] Thomas Wunderer. A detailed analysis of the hybrid lattice-reduction and meet-in-the-middle attack. *Journal of Mathematical Cryptology*, 13(1): 1–??, March 2019. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/view/j/jmc.2019.13.issue-1/jmc-2016-0044/jmc-2016-0044.xml`.

Yasuda:2020:SDD

[Yas20] Masaya Yasuda. Self-dual DeepBKZ for finding short lattice vectors. *Journal of Mathematical Cryptology*, 14(1):84–94, June 14, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2015-0053/html`.

Yoon:2015:NMC

[Yoo15] Kisoon Yoon. A new method of choosing primitive elements for Brezing–Weng families of pairing-friendly elliptic curves. *Journal of Mathematical Cryptology*, 9(1):1–9, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Yasuda:2014:EDR

[YYS+14] Masaya Yasuda, Kazuhiro Yokoyama, Takeshi Shimoyama, Jun Kogure, and Takeshi Koshiba. On the exact decryption range for Gentry–Halevi's implementation of fully homomorphic encryption. *Journal of Mathematical Cryptology*, 8(3): 305–329, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Yasuda:2017:ADS

[YYS+17] Masaya Yasuda, Kazuhiro Yokoyama, Takeshi Shimoyama, Jun Kogure, and Takeshi Koshiba. Analysis of decreasing squared-sum of Gram–Schmidt lengths for short lattice vectors. *Journal of Mathematical Cryptology*, 11(1):1–24, 2017. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Yokoyama:2020:CBS

[YYTK20] Kazuhiro Yokoyama, Masaya Yasuda, Yasushi Takahashi, and Jun Kogure. Complexity bounds on Semaev's naive index calculus method for ECDLP. *Journal of Mathematical Cryptology*, 14 (1):460–485, October 30, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/document/doi/10.1515/jmc-2019-0029/html.

Zajac:2013:NMS

[Zaj13] Pavol Zajac. A new method to solve MRHS equation systems and its connection to group factorization. *Journal of Mathematical Cryptology*, 7(4): 367–381, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Zhou:2022:CCB

[ZHM+22] Yu Zhou, Jianyong Hu, Xudong Miao, Yu Han, and Fuzhong Zhang. On the confusion coefficient of Boolean functions. *Journal of Mathematical Cryptology*, 16(1):1–13, January 2022. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/document/doi/10.1515/jmc-2021-0012/html.

Zhang:2021:SBS

[ZLA21] Jing Zhang, Yuan Li, and John O. Adeyeye. Sensitivities and block sensitivities of elementary symmetric Boolean functions. *Journal of Mathematical Cryptology*, 15(1):434–453, April 22, 2021. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/document/doi/10.1515/jmc-2020-0042/html.

Zhou:2020:CPB

[ZMD20] Yu Zhou, Daoguang Mu, and Xinfeng Dong. On cryptographic properties of $(n+1)$-bit S-boxes constructed by known n-bit S-boxes. *Journal of Mathematical Cryptology*, 15(1):258–265, December 8, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/document/doi/10.1515/jmc-2020-0004/html.

Zhang:2020:PPV

[ZSN20] Liang Feng Zhang and Reihaneh Safavi-Naini. Privacy-preserving verifiable delegation of polynomial and matrix functions. *Journal of Mathematical Cryptology*, 14(1):153–171, July 3, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/document/doi/10.1515/jmc-2018-0039/html.