A Bibliography of Papers in *Lecture Notes in Computer Science* (2014): Volumes 8349–??

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/

14 October 2017
Version 1.02

Title word cross-reference

4 [9].

-Round [9].

1 [21].

Achieving [7]. **Adaptively** [16]. **against** [19]. **Amplification** [18].

Based [10]. **Basing** [12]. **Be** [10]. **Bit** [19]. **Bit-Wise** [19]. **Black** [1, 15]. **Black-Box** [1, 15]. **Box** [1, 15]. **Broadcast** [18].

Can [10]. **Characterizing** [13]. **Checkable** [6]. **Chosen** [5]. **Ciphertext** [5]. **Circuits** [1]. **Codes** [20]. **Coding** [19]. **Coin** [10, 12]. **Complete** [13]. **Complexity** [14]. **Composable** [15]. **Computation** [13, 16, 15, 11].

Concurrent [8]. **Constant** [15, 7]. **Constant-Round** [15]. **Construction** [15]. **Continuous** [20]. **Cryptographic** [14].

Encoding [1]. **Encryption** [11]. **Evasive** [2]. **Eve** [21]. **Extractability** [3].

Fair [10]. **Fairness** [13]. **Functions** [2, 14, 10].

Generic [1]. **Graded** [1].

Hashing [21].

Impossibility [12]. **Indistinguishability** [4].

Key [11]. **Knowledge** [9, 6, 8, 7].

Leakage [7]. **Leakage-Resilient** [7]. **linear** [17].

Malicious [21]. **malleable** [19, 20, 8]. **MPC** [4]. **Multi** [17, 15]. **Multi-linear** [17]. **Multi-Party** [15].

Non [19, 20, 8]. **Non-malleable** [19, 20, 8].

Obfuscation [2, 3, 1, 4, 5]. **One** [10, 16, 12]. **One-Sided** [16]. **One-Way** [10, 12]. **Optimally** [10]. **Optimally-Fair** [10].

Party [13, 16, 15]. **Permutations** [12]. **Point** [5]. **Power** [11]. **Probabilistically** [6]. **Proofs** [6]. **Protocol** [15]. **Proximity** [6]. **Public** [11, 12]. **Public-Coin** [12]. **Public-Key** [11].

Resettably [9]. **Resettably-Sound** [9]. **Resilient** [7]. **Round** [9, 4, 15, 7].

Schemes [17]. **Secret** [17]. **Secret-Sharing** [17]. **Secure** [13, 4, 16, 11]. **Security** [5]. **SHA** [21]. **SHA-1** [21]. **Sharing** [17]. **Sided** [16]. **Sound** [9]. **Split** [19]. **Split-State** [19]. **State** [19]. **Statistical** [8].

Tampering [19]. **Tossing** [10]. **Trapdoor** [12]. **Two** [13, 4, 16]. **Two-Party** [13, 16]. **Two-Round** [4].

Variant [21]. **via** [1, 5]. **Virtual** [1].

Way [10, 12]. **Wise** [19]. **Worst** [14].

Zero [9, 6, 8, 7]. **Zero-Knowledge** [6, 7].

References

Brakerski:2014:VBB

[1] Zvika Brakerski and Guy N. Rothblum. Virtual black-box obfuscation for all circuits via generic graded encoding. *Lecture Notes in Computer Science*, 8349:1–25, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-54242-8_1/; http://link.springer.com/content/pdf/bfm:978-3-642-54242-8/1.pdf`.

Barak:2014:OEF

[2] Boaz Barak, Nir Bitansky, Ran Canetti, Yael Tauman Kalai, Omer Paneth, and Amit Sahai. Obfuscation for evasive functions. *Lecture Notes in Computer Science*, 8349:26–51, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-54242-8_2/`.

Boyle:2014:EO

[3] Elette Boyle, Kai-Min Chung, and Rafael Pass. On extractability obfuscation. *Lecture Notes in Computer Science*, 8349:52–73, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-54242-8_3/`.

Garg:2014:TRS

[4] Sanjam Garg, Craig Gentry, Shai Halevi, and Mariana Raykova. Two-round secure MPC from indistinguishability obfuscation. *Lecture Notes in Computer Science*, 8349:74–94, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-54242-8_4/`.

Matsuda:2014:CCS

[5] Takahiro Matsuda and Goichiro Hanaoka. Chosen ciphertext security via point obfuscation. *Lecture Notes in Computer Science*, 8349:95–120, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-54242-8_5/`.

Ishai:2014:PCP

[6] Yuval Ishai and Mor Weiss. Probabilistically checkable proofs of proximity with zero-knowledge. *Lecture Notes in Computer Science*, 8349:121–145, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-54242-8_6/`.

Pandey:2014:ACR

[7] Omkant Pandey. Achieving constant round leakage-resilient zero-knowledge. *Lecture Notes in Computer Science*, 8349:146–166, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-54242-8_7/`.

Orlandi:2014:SCN

[8] Claudio Orlandi, Rafail Ostrovsky, Vanishree Rao, Amit Sahai, and Ivan Visconti. Statistical concurrent non-malleable zero knowledge. *Lecture Notes in Computer Science*, 8349:167–191, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-54242-8_8/`.

Chung:2014:RRS

[9] Kai-Min Chung, Rafail Ostrovsky, Rafael Pass, and Muthuramakrishnan Venkitasubramaniam . 4-round resettably-sound zero knowledge. *Lecture Notes in Computer Science*, 8349:192–216, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-54242-8_9/`.

Dachman-Soled:2014:COF

[10] Dana Dachman-Soled, Mohammad Mahmoody, and Tal Malkin. Can optimally-fair coin tossing be based on one-way functions? *Lecture Notes in Computer Science*, 8349:217–239, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-54242-8_10/`.

Mahmoody:2014:PPK

[11] Mohammad Mahmoody, Hemanta K. Maji, and Manoj Prabhakaran. On the power of public-key encryption in secure computation. *Lecture Notes in Computer Science*, 8349:240–264, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-54242-8_11/`.

Matsuda:2014:IBP

[12] Takahiro Matsuda. On the impossibility of basing public-coin one-way permutations on trapdoor permutations. *Lecture Notes in Computer Science*, 8349:265–290, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-54242-8_12/`.

Asharov:2014:TCC

[13] Gilad Asharov. Towards characterizing complete fairness in secure two-party computation. *Lecture Notes in Computer Science*, 8349:291–316, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-54242-8_13/`.

Beimel:2014:CCW

[14] Amos Beimel, Yuval Ishai, Ranjit Kumaresan, and Eyal Kushilevitz. On the cryptographic complexity of the worst functions. *Lecture Notes in Computer Science*, 8349:317–342, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-54242-8_14/`.

Kiyoshima:2014:CRB

[15] Susumu Kiyoshima, Yoshifumi Manabe, and Tatsuaki Okamoto. Constant-round black-box construction of composable multi-party computation protocol. *Lecture Notes in Computer Science*, 8349:343–367, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-54242-8_15/`.

Hazay:2014:OSA

[16] Carmit Hazay and Arpita Patra. One-sided adaptively secure two-party computation. *Lecture Notes in Computer Science*, 8349:368–393, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-54242-8_16/`.

Beimel:2014:MLS

[17] Amos Beimel, Aner Ben-Efraim, Carles Padró, and Ilya Tyomkin. Multilinear secret-sharing schemes. *Lecture Notes in Computer Science*, 8349:394–418, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-54242-8_17/`.

Hirt:2014:BA

[18] Martin Hirt, Ueli Maurer, and Pavel Raykov. Broadcast amplification. *Lecture Notes in Computer Science*, 8349:419–439, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-54242-8_18/`.

Cheraghchi:2014:NMC

[19] Mahdi Cheraghchi and Venkatesan Guruswami. Non-malleable coding against bit-wise and split-state tampering. *Lecture Notes in Computer*

Science, 8349:440–464, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-54242-8_19/.

Faust:2014:CNM

[20] Sebastian Faust, Pratyay Mukherjee, Jesper Buus Nielsen, and Daniele Venturi. Continuous non-malleable codes. *Lecture Notes in Computer Science*, 8349:465–488, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-54242-8_20/.

Albertini:2014:MHE

[21] Ange Albertini, Jean-Philippe Aumasson, Maria Eichlseder, Florian Mendel, and Martin Schläffer. Malicious hashing: Eve's variant of SHA-1. *Lecture Notes in Computer Science*, 8781:1–19, November 29, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://eprint.iacr.org/2014/694; http://link.springer.com/chapter/10.1007/978-3-319-13051-4_1; https://malicioussha1.github.io/.