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/

25 March 2019
Version 1.04

Title word cross-reference

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).

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).

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). URL `https://doi.org/10.1515%2Fjmc-2018-frontmatter2`.

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`.

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).

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`.

Blackburn:2009:CPK

[BCM09] Simon R. Blackburn, Carlos Cid, and Ciaran Mullan. Crypt-

analysis 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).

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).

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).

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).

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).

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`.

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).

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).

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).

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`.

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).

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`.

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).

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).

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).

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).

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`.

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 $\mathbf{F_{p^k}}$ and application to fast pairing computation. *Journal of Mathematical Cryptology*, 5(1):51–88, 2011. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

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).

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). URL `https://doi.org/10.1515%2Fjmc-2017-0024`.

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).

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. CO-

DEN ???? 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).

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).

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).

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).

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).

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).

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 $\mathbf{F}^*_{\mathbf{24m}}$ and $\mathbf{F}^*_{\mathbf{36m}}$. *Journal of Mathematical Cryptology*, 4(1):1–42, 2010. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

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).

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).

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).

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). URL `https://doi.org/10.1515%2Fjmc-2017-0053`.

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).

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. Nu-

merical 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`.

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).

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).

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).

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 NLFSRs. *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`.

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).

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: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).

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).

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).

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).

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).

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).

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).

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).

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).