Cryptography
Cryptography: General

[1] Alex Biryukov, Praveen Gauravaram, Jian Guo, Dmitry Khovratovich, San Ling, Krystian Matusiewicz, Ivica Nikolić, Josef Pieprzyk, and Huaxiong Wang, *Cryptanalysis of the LAKE hash family*, Fast Software Encryption, Lecture Notes in Computer Science, vol. 5665, Springer, Berlin, 2009, pp. 156–179.

[2] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire, *New families of quadratic almost perfect nonlinear trinomials and multinomials*, Finite Fields Appl. **14** (2008), no. 3, 703–714. MR MR2435056

[3] An Braeken, Christopher Wolf, and Bart Preneel, *Classification of highly nonlinear Boolean power functions with a randomised algorithm for checking normality*, 2004.

[4] Marcus Brinkmann and Gregor Leander, *On the classification of APN functions up to dimension five*, Des. Codes Cryptogr. **49** (2008), no. 1-3, 273–288. MR MR2438456

[5] Johannes Buchmann, Carlos Coronado, Martin Dring, Daniela Engelbert, Christoph Ludwig, Raphael Overbeck, Arthur Schmidt, Ulrich Vollmer, and Ralf-Philipp Weinmann, *Post-quantum signatures*, 2004.

[6] Kelley Burgin, *The nonexistence of a bijective almost perfect nonlinear function of order 16*, Master's thesis, Auburn University, Alabama, 2002.

[7] Denis Charles, Kamal Jain, and Kristin Lauter, *Signatures for network coding*, International Journal of Information and Coding Theory **1** (2009), no. 1, 3–14.

[8] Mihai Cipu, *Dickson polynomials that are permutations*, Serdica Math. J. **30** (2004), no. 2-3, 177–194. MR MR2098331 (2005g:11244)

[9] Scott Contini and Igor E. Shparlinski, *On Stern's attack against secret truncated linear congruential generators*, Information Security and Privacy, Lecture Notes in Computer Science, vol. 3574, Springer Berlin / Heidelberg, 2005, pp. 52–60.

[10] Scott Contini and Yiqun Lisa Yin, *Improved cryptanalysis of securID*, 2003.

[11] ———, *Fast software-based attacks on SecurID*, Fast Software Encryption (Berlin), Lecture Notes in Computer Science, vol. 3017, Springer-Verlag, 2004, pp. 454–471.

[12] Deepak Dalai, *On some necessary conditions of boolean functions to resist algebraic attacks*, Ph D thesis, Indian Statistical Institute, Kolkata, India, 2006.

[13] Alexander W. Dent and Steven D. Galbraith, *Hidden pairings and trapdoor DDH groups*, Algorithmic Number Theory (Berlin, 2006), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2006, p. pp.15.

[14] Jintai Ding, Bo-Yin Yang, Chia-Hsin Owen Chen, Ming-Shing Chen, and Chen-Mou Cheng, *New differential-algebraic attacks and reparametrization of Rainbow*, Applied Cryptography and Network Security, Lecture Notes in Computer Science, vol. 5037, Springer, 2008, pp. 242–257.

[15] D.G. Farmer and K.J. Horadam, *Presemifield bundles over GF*(p^3), IEEE International Symposium on Information Theory, 2008. ISIT 2008 (2008), 2613–2616.

[16] Steven D. Galbraith, Colm Ó hÉigeartaigh, and Caroline Sheedy, *Simplified pairing computation and security implications*, J. Math. Cryptol. **1** (2007), no. 3, 267–281. MR MR2372156 (2009a:94027)

[17] Willi Geiselmann and Rainer Steinwandt, *Cryptanalysis of a hash function proposed at ICISC 2006*, Information Security and Cryptology - ICISC 2007, Lecture Notes in Computer Science, vol. 4817/2007, Springer Berlin / Heidelberg, 2007, pp. 1–10.

[18] Willi Geiselmann, Rainer Steinwandt, and Thomas Beth, *Attacking the affine parts of SFLASH*, Cryptography and Coding, Lecture Notes in Comput. Sci., vol. 2260, Springer, Berlin, 2001, pp. 355–359. MR MR2074529

[19] ______, *Revealing the affine parts of SFLASHv1, SFLASHv2, and FLASH*, Actas de la VII Reunisn Espaqola de Criptologma y Seguridad de la Informacisn, vol. 7, 2002, pp. 305–314.

[20] Markus Grassl and Rainer Steinwandt, *Cryptanalysis of an authentication scheme using truncated polynomials*, 2008.

[21] K. J. Horadam and D. G. Farmer, *Bundles, presemifields and nonlinear functions*, Des. Codes Cryptogr. **49** (2008), no. 1-3, 79–94. MR MR2438442

[22] Georg Illies and Marian Margraf, *Attacks on the ESA-PSS-04-151 MAC scheme*, Selected Areas in Cryptography, Lecture Notes in Computer Science, vol. 4876/2007, Springer Berlin / Heidelberg, 2007, pp. 296–310.

[23] Mariusz Jakubowski, Prasad Naldurg, Vijay Patankar, and Ramarathnam Venkatesan, *Software integrity checking expressions (ICEs) for robust tamper detection*, Information Hiding, Lecture Notes in Computer Science, vol. 4567, 2008, pp. 96–111.

[24] Gohar M. Kyureghyan and Alexander Pott, *On the linear complexity of the Sidelnikov-Lempel-Cohn-Eastman sequences*, Proceedings of the Conference on Finite Geometries (Oberwolfach, 2001), vol. 29, 2003, pp. 149–164. MR MR1993164 (2004g:94036)

[25] P. Loidreau and V. Shorin, *Application of Gröbner bases techniques for searching new sequences with good periodic correlation properties*, IEEE International Symposium on Information Theory (ISIT), Adelaide, 2005.

[26] Bart Preneel (ed.), *Advances in Cryptology—Eurocrypt 2000*, Lecture Notes in Computer Science, vol. 1807, Berlin, Springer-Verlag, 2000. MR MR1772020 (2001b:94028)

[27] N. P. Smart, *Attacks on asymmetric cryptosystems: An analysis of Goubin's refined power analysis attack*, Cryptographic Hardware and Embedded Systems, Lecture Notes in Comput. Sci., vol. 2779, Springer, Berlin, 2003, pp. 281–290.

[28] Rainer Steinwandt, Markus Grassl, Willi Geiselmann, and Thomas Beth, *Weakness in the* $\mathrm{SL}_2(F_{2^n})$ *hashing scheme*, Advances in Cryptology—CRYPTO 2000 (Santa Barbara, CA), Lecture Notes in Comput. Sci., vol. 1880, Springer, Berlin, 2000, pp. 287–299. MR MR1850050 (2002i:94053)

Block Ciphers

[1] Martin Albrecht, *Algebraic attacks on the Courtois Toy cipher*, Cryptologia **32** (2008), no. 3, 220–276.

[2] Martin Albrecht and Carlos Cid, *Algebraic techniques in differential cryptanalysis*, Fast Software Encryption (Orr Dunkelman, ed.), Lecture Notes in Computer Science, vol. 5665, Springer, 2009, pp. 193–208.

[3] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, *PRESENT: An ultra-lightweight block cipher*, Cryptographic Hardware and Embedded Systems - CHES 2007, Lecture Notes in Computer Science, vol. 4727/2007, Springer Berlin / Heidelberg, 2007, pp. 450–466.

[4] Andrey Bogdanov and Andrey Pyshkin, *Algebraic side-channel collision attacks on AES*, 2007.

[5] Johannes Buchmann, Andrei Pyshkin, and Ralf-Philipp Weinmann, *Block ciphers sensitive to Gröbner basis attacks*, Topics in Cryptology—CT-RSA 2006, Lecture Notes in Comput. Sci., vol. 3860, Springer, Berlin, 2006, pp. 313–331. MR MR2243996 (2007e:94052)

[6] Stanislav Bulygin and Michael Brickenstein, *Obtaining and solving systems of equations in key variables only for the small variants of AES*, 2008.

[7] ———, *Obtaining and solving systems of equations in key variables only for the small variants of AES*, Math. Comput. Sci. **3** (2010), no. 2, 185–200.

[8] Chris Charnes, Martin Rötteler, and Thomas Beth, *On homogeneous bent functions*, Applied Algebra, Algebraic Algorithms and Error-correcting Codes (Melbourne, 2001), Lecture Notes in Comput. Sci., vol. 2227, Springer, Berlin, 2001, pp. 249–259. MR MR1913471 (2003e:94065)

[9] ———, *Homogeneous bent functions, invariants, and designs*, Des. Codes Cryptogr. **26** (2002), no. 1-3, 139–154. MR MR1919874 (2003h:05043)

[10] C. Cid, S. Murphy, and M. Robshaw, *Computational and algebraic aspects of the advanced encryption standard*, Seventh International Workshop on Computer Algebra in Scientific Computing, CASC 2004, St. Petersburg, Russia, 2004, pp. 93–103.

[11] ———, *Small scale variants of the AES*, LNCS 3557, Eds. Gilbert, H. and Handschuh, H., Springer, 2005, pp. 145–162.

[12] Carlos Cid, Sean Murphy, and Matthew Robshaw, *Algebraic Aspects of the Advanced Encryption Standard*, Springer, New York, 2006. MR MR2250327

[13] Nicolas T. Courtois and Gregory V. Bard, *Algebraic cryptanalysis of the data encryption standard*, Cryptography and Coding, Lecture Notes in Computer Science, vol. 4887/2007, Springer Berlin / Heidelberg, 2007, pp. 152–169.

[14] Nicolas T. Courtois, Gregory V. Bard, and David Wagner, *Algebraic and slide attacks on KeeLoq*, 2007.

[15] Jintai Ding, Bo-Yin Yang, Chen-Mou Cheng, Owen Chen, and Vivien Dubois, *Breaking the symmetry: A way to resist the new differential attack*, 2007.

[16] Tobias Eibach, Gunnar Völkel, and Enrico Pilz, *Optimising Gröbner bases on Bivium*, Math. Comput. Sci. **3** (2010), no. 2, 159–172.

[17] Jeremy Erickson, Jintai Ding, and Chris Christensen, *Algebraic cryptanalysis of SMS4: Gröbner basis attack and SAT attack compared*, Information, Security and Cryptology – ICISC 2009 (Donghoon Lee and Seokhie Hong, eds.), Lecture Notes in Computer Science, vol. 5984, Springer Berlin/Heidelberg, 2010, pp. 73–86.

[18] Jean-Charles Faugére and Ludovic Perret, *Algebraic cryptanalysis of Curry and Flurry using correlated messages*, 2008.

[19] Willi Geiselmann and Rainer Steinwandt, *A short comment on the affine parts of SFLASHv3*, 2003.

[20] Krystian Matusiewicz, Scott Contini, and Josef Pieprzyk, *Weaknesses of the fork-256 compression function*, 2006, pp. 1–21.

[21] Nele Mentens, Lejla Batina, Bart Preneel, and Ingrid Verbauwhede, *A systematic evaluation of compact hardware implementations for the Rijndael S-box*, Topics in Cryptology—CT-RSA 2005, Lecture Notes in Comput. Sci., vol. 3376, Springer, Berlin, 2005, pp. 323–333. MR MR2174386

[22] Sean Simmons, *Algebraic cryptanalysis of simplified AES**, Cryptologia **33** (2009), no. 4, 305–314.

Stream Ciphers

[1] M. Afzal and A. Masood, *Algebraic cryptanalysis of a NLFSR based stream cipher*, 3rd International Conference on Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. (2008), 1–6.

[2] Mehreen Afzal and Ashraf Masood, *Resistance of stream ciphers to algebraic recovery of internal secret states*, Third International Conference on Convergence and Hybrid Information Technology, 2008. ICCIT '08 **2** (2008), 625–630.

[3] Mehreen Afzal, Ashraf Masood, and Naveed Shehzad, *Improved results on algebraic cryptanalysis of A5/2*, Communications in Computer and Information Science **12** (2008), no. 4, 182–189.

[4] Sultan Zayid Al-Hinai1, Ed Dawson, Matt Henricksen, and Leonie Simpson, *On the security of the LILI family of stream ciphers against algebraic attacks*, Information Security and Privacy, Lecture Notes in Computer Science, vol. 4586/2007, Springer Berlin / Heidelberg, 2007, pp. 11–28.

[5] Anne Canteaut, *Open problems related to algebraic attacks on stream ciphers*, WCC 2005, Lecture Notes in Comput. Sci., vol. 3969, Springer, Berlin, 2006, pp. 120–134.

[6] Scott Contini and Igor E. Shparlinski, *On Stern's attack against secret truncated linear congruential generators*, Information Security and Privacy, Lecture Notes in Computer Science, vol. 3574, Springer Berlin / Heidelberg, 2005, pp. 52–60.

[7] Tobias Eibach, Enrico Pilz, and Gunnar Völkel, *Attacking Bivium using SAT solvers*, Theory and Applications of Satisfiability Testing, SAT 2008, Lecture Notes in Computer Science, vol. 4996, Springer, Berlin, 2008, pp. 63–76.

[8] Aline Gouget, Hervé Sibert, Come Berbain, Nicolas Courtois, Blandine Debraize, and Chris Mitchell, *Analysis of the bit-search generator and sequence compression techniques*, Fast Software Encryption (Berlin), Lecture Notes in Computer Science, vol. 3557, Springer-Verlag, 2005, pp. 196–214.

[9] Antoine Joux and Frédéric Muller, *A chosen IV attack against Turing*, Selected Areas in Cryptography, Lecture Notes in Comput. Sci., vol. 3006, Springer, Berlin, 2004, pp. 194–207. MR MR2094730 (2005f:94106)

[10] P. Loidreau and V. Shorin, *Application of Gröbner bases techniques for searching new sequences with good periodic correlation properties*, IEEE International Symposium on Information Theory (ISIT), Adelaide, 2005.

[11] Cameron McDonald, Chris Charnes, and Josef Pieprzyk, *An algebraic analysis of Trivium ciphers based on the boolean satisfiability problem*, 2007.

[12] Deike Priemuth-Schmid and Alex Biryukov, *Slid pairs in Salsa*20 *and Trivium.*

[13] Werner Schindler and Le Van Ly, *How to embed short cycles into large nonlinear feedback-shift registers*, Security in Communications Networks: 4th International Conference, SCN 2004, Amalfi, Italy, September 8-10, 2004, Revised Selected Papers, Lecture Notes in Comput. Sci., vol. 3352, Springer, Berlin, 2005, p. 367.

[14] Kenneth Koon-Ho Wong, *Applications of finite field computation to cryptology: Extension field arithmetic in public key systems and algebraic attacks on stream ciphers*, Phd, Queensland University of Technology, 2008.

[15] Haina Zhang and Xiaoyun Wang, *Cryptanalysis of stream cipher grain family*, 2009.

Public Key Cryptography

See also Curve-Based Public Key Cryptography

[1] Daniel J. Bernstein, *Batch binary edwards*, Advances in Cryptology - CRYPTO 2009, Lecture Notes in Comput. Sci., vol. 5677, Springer, Berlin, 2009, pp. 317–336.

[2] Luk Bettale, Jean-Charles Faugère, and Ludovic Perret, *Cryptanalysis of the TRMS signature scheme of PKC'05*, Progress in Cryptology, AfricaCrypt 2008, Lecture Notes in Computer Science, vol. 5023, Springer Berlin/Heidelberg, 2008, pp. 143–155.

[3] Olivier Billet and Gilles Macario-Rat, *Cryptanalysis of the square cryptosystems*, Advances in Cryptology – ASIACRYPT 2009, Lecture Notes in Comput. Sci., vol. 5912, Springer, Berlin, 2009, pp. 451–468.

[4] Simon R. Blackburn, Carlos Cid, and Steven D. Galbraith, *Cryptanalysis of a cryptosystem based on Drinfeld modules*, 2003.

[5] Jens-Matthias Bohli, Stefan Röhrich, and Rainer Steinwandt, *Key substitution attacks revisited: Taking into account malicious signers*, 2006, pp. 30–36.

[6] Jens-Matthias Bohli, Rainer Steinwandt, María Isabel González Vasco, and Consuelo Martínez, *Weak keys in MST_1*, Des. Codes Cryptogr. **37** (2005), no. 3, 509–524. MR MR2177649

[7] Wieb Bosma, James Hutton, and Eric R. Verheul, *Looking beyond XTR*, Advances in Cryptology—Asiacrypt 2002, Lecture Notes in Comput. Sci., vol. 2501, Springer, Berlin, 2002, pp. 46–63. MR MR2087376 (2006c:94016)

[8] Charles Bouillaguet, Pierre-Alain Fouque1, Antoine Joux, and Joana Treger, *A family of weak keys in HFE (and the corresponding practical key-recovery)*, pp. 1–16.

[9] An Braeken, Christopher Wolf, and Bart Preneel, *A study of the security of unbalanced oil and vinegar signature schemes*, Topics in Cryptology—CT-RSA 2005, Lecture Notes in Comput. Sci., vol. 3376, Springer, Berlin, 2005, pp. 29–43. MR MR2174368

[10] Chia-Hsin Owen Chen, Ming-Shing Chen, Jintai Ding, Fabian Werner, and Bo-Yin Yang, *Odd-char multivariate hidden field equations*, 2008.

[11] Jiun-Ming Chen and Bo-Yin Yang, *Building secure tame-like multivariate public-key cryptosystems: The new TTS*, Information Security and Privacy: 10th Australasian Conference, ACISP 2005, Brisbane, Australia, July 4-6, 2005. Proceedings, Lecture Notes in Comput. Sci., vol. 3574, Springer, Berlin, 2005, p. 518.

[12] Robert S. Coulter, George Havas, and Marie Henderson, *Giesbrecht's algorithm, the HFE cryptosystem and Ore's p^s-polynomials*, Computer Mathematics (Matsuyama, 2001), Lecture Notes Ser. Comput, vol. 9, World Sci. Publ., River Edge, NJ, 2001, pp. 36–45. MR MR1877440 (2002m:11103)

[13] J. Ding, J. E. Gower, D. Schmidt, C. Wolf, and Z. Yin, *Complexity estimates for the F_4 attack on the perturbed Matsumoto-Imai cryptosystem*, Cryptography and coding, Lecture Notes in Comput. Sci., vol. 3796, Springer, Berlin, 2005, pp. 262–277. MR MR2235262 (2007f:94036)

[14] Jintai Ding, Jason E. Gower, and Dieter Schmidt, *Multivariate public key cryptosystems*, Springer, Berlin, 2006.

[15] Jintai Ding and Dieter Schmidt, *Cryptanalysis of HFEv and internal perturbation of HFE*, Public Key Cryptography—PKC 2005, Lecture Notes in Comput. Sci., vol. 3386, Springer, Berlin, 2005, pp. 288–301. MR MR2174048 (2006j:94061)

[16] Jintai Ding, Dieter Schmidt, and Fabian Werner, *Algebraic attack on HFE revisited*, Information Security, Lecture Notes in Comput. Sci., vol. 5222, Springer, Berlin, 2008, pp. 215–227.

[17] Jintai Ding and John Wagner, *Cryptanalysis of rational multivariate public key cryptosystems*, 2007.

[18] Bettina Eick and Delaram Kahrobaei, *Polycyclic groups: A new platform for cryptology?*, 2004.

[19] L. Hernandez Encinas, J. Munoz Masque, and A. Queiruga Dios, *Analysis of the efficiency of the Chor–Rivest cryptosystem implementation in a safe-parameter range*, Information Sciences **To appear** (2009).

[20] Jean-Charles Faugère and Antoine Joux, *Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases*, Advances in Cryptology—CRYPTO 2003, Lecture Notes in Comput. Sci., vol. 2729, Springer, Berlin, 2003, pp. 44–60. MR MR2093185 (2005e:94140)

[21] Patrick Felke, *Computing the uniformity of power mappings: A systematic approach with the multi-variate method over finite fields of odd characteristic*, PhD Thesis, Ruhr Universität Bochum, 2005.

[22] Michelle Feltz, *On the conjugacy problem in groups and its variants*, Master thesis in mathematics, University of Fribourg, 2010.

[23] Pierre-Alain Fouque, Gilles Macario-Rat, Ludovic Perret, and Jacques Stern, *Total break of the l-IC signature scheme*, Public Key Cryptography, PKC 2008, Lecture Notes in Computer Science, vol. 4939, Springer, 2008, pp. 1–17.

[24] Pierre-Alain Fouque, Gilles Macario-Rat, and Jacques Stern, *Key recovery on hidden monomial multivariate schemes*, Advances in Cryptology, EUROCRYPT 2008, Lecture Notes in Computer Science, vol. 4965, Springer Berlin/Heidelberg, 2008, pp. 19–30.

[25] Pierrick Gaudry and Éric Schost, *A low-memory parallel version of Matsuo, Chao, and Tsujii's algorithm*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 208–222. MR MR2137355 (2005m:11237)

[26] Volker Gebhardt, *A new approach to the conjugacy problem in Garside groups*, J. Algebra **292** (2005), no. 1, 282–302. MR MR2166805

[27] Willi Geiselmann, Willi Meier, and Rainer Steinwandt, *An attack on the isomorphisms of polynomials problem with one secret*, Int. J. Inf. Secur. (2003), no. 2, 59–64.

[28] Willi Geiselmann and Rainer Steinwandt, *Cryptanalysis of a knapsack-like cryptosystem*, Period. Math. Hungar. **45** (2002), no. 1-2, 35–41. MR MR1955191 (2003m:94062)

[29] ———, *Yet another sieving device*, Topics in Cryptology—CT-RSA 2004, Lecture Notes in Comput. Sci., vol. 2964, Springer, Berlin, 2004, pp. 278–291. MR MR2092251

[30] ———, *Non-wafer-scale sieving hardware for the NFS: another attempt to cope with 1024-bit*, Advances in cryptology—EUROCRYPT 2007, Lecture Notes in Comput. Sci., vol. 4515, Springer, Berlin, 2007, pp. 466–481. MR MR2449226 (2009h:94125)

[31] María Isabel González Vasco, Martin Rötteler, and Rainer Steinwandt, *On minimal length factorizations of finite groups*, Experiment. Math. **12** (2003), no. 1, 1–12. MR MR2002670 (2004h:20035)

[32] María Isabel González Vasco and Rainer Steinwandt, *Clouds over a public key cryptosystem based on Lyndon words*, Inform. Process. Lett. **80** (2001), no. 5, 239–242. MR MR1864974 (2003h:94037)

[33] ———, *Obstacles in two public key cryptosystems based on group factorizations*, Tatra Mt. Math. Publ. **25** (2002), 23–37, TATRACRYPT '01 (Liptovský Ján). MR MR1976471 (2004f:94061)

[34] Markus Grassl, Ivana Ilić, Spyros Magliveras, and Rainer Steinwandt, *Cryptanalysis of the Tillich–Zémor hash function*, J. Cryptology **online first** (2010), 1–9.

[35] Markus Grassl and Rainer Steinwandt, *Cryptanalysis of an authentication scheme using truncated polynomials*, Inform. Process. Lett. **Article in Press** (2009).

[36] Anja Groch, Dennis Hofheinz, and Rainer Steinwandt, *A practical attack on the root problem in braid groups*, Algebraic methods in cryptography, Contemp. Math., vol. 418, Amer. Math. Soc., Providence, RI, 2006, pp. 121–131. MR MR2389293

[37] Guillaume Hanrot and Damien Stehlé, *Improved analysis of Kannan's shortest lattice vector algorithm (extended abstract)*, Advances in cryptology—CRYPTO 2007, Lecture Notes in Comput. Sci., vol. 4622, Springer, Berlin, 2007, pp. 170–186. MR MR2419600

[38] Xin Jiang, Jintai Ding, and Lei Hu, *Kipnis-Shamir attack on HFE revisited*, Information Security and Cryptology, Lecture Notes in Computer Science, vol. 4990, Springer Berlin/Heidelberg, 2008, pp. 399–411.

[39] Ellen Jochemsz and Alexander May, *A polynomial time attack on RSA with private CRT-exponents smaller than $N^{0.073}$*, Advances in cryptology—CRYPTO 2007, Lecture Notes in Comput. Sci., vol. 4622, Springer, Berlin, 2007, pp. 395–411. MR MR2423861

[40] Antoine Joux, Sébastien Kunz-Jacques, Frédéric Muller, and Pierre-Michel Ricordel, *Cryptanalysis of the tractable rational map cryptosystem*, Public Key Cryptography—PKC 2005, Lecture Notes in Comput. Sci., vol. 3386, Springer, Berlin, 2005, pp. 258–274. MR MR2174046

[41] Arkadius Kalka, Mina Teicher, and Boaz Tsaban, *Cryptanalysis of the algebraic eraser and short expressions of permutations as products*, 2008.

[42] Wolfgang Lempken and Tran van Trung, *On minimal logarithmic signatures of finite groups*, Experiment. Math. **14** (2005), no. 3, 257–269. MR MR2172704

[43] Françoise Levy-dit-Vehel and Ludovic Perret, *Polynomial equivalence problems and applications to multivariate cryptosystems*, Progress in Cryptology—Indocrypt 2003, Lecture Notes in Comput. Sci., vol. 2904, Springer, Berlin, 2003, pp. 235–251. MR MR2092385 (2005e:94175)

[44] Françoise Levy-dit Vehel and Ludovic Perret, *A Polly Cracker system based on satisfiability*, Coding, cryptography and combinatorics, Progr. Comput. Sci. Appl. Logic, vol. 23, Birkhäuser, Basel, 2004, pp. 177–192. MR MR2090648 (2005e:94176)

[45] Le Van Ly, *Polly Two: A new algebraic polynomial-based public-key scheme*, Appl. Algebra Engrg. Comm. Comput. **17** (2006), no. 3-4, 267–283. MR MR2233786

[46] Mohamed Saied Emam Mohamed, Jintai Ding, and Johannes Buchmann, *Algebraic cryptanalysis of MQQ public key cryptosystem by mutantxl*, 2008.

[47] Naoki Ogura and Shigenori Uchiyama, *Remarks on the attack of Fouque et al. against the lIC scheme*, 2008.

[48] ———, *Cryptanalysis of the birational permutation signature scheme over a non-commutative ring*, 2009.

[49] Ayoub Otmani, Jean-Pierre Tillich, and Leonard Dallot, *Cryptanalysis of two McEliece cryptosystems based on quasi-cyclic codes*, 2008.

[50] Ayoub Otmani, Jean-Pierre Tillich, and Léonard Dallot, *Cryptanalysis of two McEliece cryptosystems based on quasi-cyclic codes*, Math. Comput. Sci. **3** (2010), no. 2, 129–140.

[51] Ludovic Perret, *A fast cryptanalysis of the isomorphism of polynomials with one secret problem*, Advances in Cryptology - Eurocrypt 2005, Lecture Notes in Computer Science, vol. 3494, Springer Berlin/Heidelberg, 2005, pp. 354–370.

[52] Albrecht Petzoldt and Johannes Buchmann, *A multivariate signature scheme with an almost cyclic public key*, 2007.

[53] Albrecht Petzoldt, Stanislav Bulygin, and Johannes Buchmann, *Selecting parameters for the rainbow signature scheme – Extended version*, 2010, p. 21.

[54] Benjamin Smith, *Isogenies and the discrete logarithm problem in Jacobians of genus 3 hyperelliptic curves*, Advances in Cryptology, Eurocrypt 2008, Lecture Notes in Computer Science, vol. 4965, Springer Berlin/Heidelberg, 2008, pp. 163–180.

[55] Rainer Steinwandt, *Loopholes in two public key cryptosystems using the modular group*, Public Key Cryptography (Cheju Island, 2001), Lecture Notes in Comput. Sci., vol. 1992, Springer, Berlin, 2001, pp. 180–189. MR MR1898034

[56] ———, *A ciphertext-only attack on Polly Two*, Appl. Algebra Engrg. Comm. Comput. **21** (2010), no. 2, 85–92. MR 2600705 (2011b:94046)

[57] Rainer Steinwandt and Regine Endsuleit, *A note on timing attacks based on the evaluation of polynomials*, 2000.

[58] Rainer Steinwandt, Willi Geiselmann, and Regine Endsuleit, *Attacking a polynomial-based cryptosystem: Polly cracker*, Int. J. Inf. Secur. **1** (2002), no. 3, 143–148.

[59] Shigeo Tsujii, Kohtaro Tadaki, and Ryou Fujita, *Proposal for piece in hand matrix: General concept for enhancing security of multivariate public key cryptosystems*, IEICE Trans A: Fundamentals **E90-A** (2007), no. 5, 992–999.

[60] Shigeo Tsujii, Kohtaro Tadaki, and Ryou Fujita, *Nonlinear piece-in-hand matrix method for enhancing security of multivariate public key cryptosystems*, 2008.

[61] Shigeo Tsujii, Kohtaro Tadaki, Masahito Gotaishi, Ryo Fujita, and Masao Kasahara, *Proposal of PPS multivariate public key cryptosystems*, 2009, p. 21 pages.

[62] Valeérie Gauthier Umaña and Gregor Leander, *Practical key recovery attacks on two McEliece variants*, 2009, pp. 1–19.

[63] Eric R. Verheul, *Evidence that XTR is more secure than supersingular elliptic curve cryptosystems*, J. Cryptology **17** (2004), no. 4, 277–296. MR MR2090558

[64] Zhiwei Wang, Xuyun Nie, Shihui Zheng, Yixian Yang, and Zhihui Zhang, *A new construction of multivariate Public Key Encryption Scheme through internally perturbed plus*, Computational Science and Its Applications, ICCSA 2008, Lecture Notes in Computer Science, vol. 5073, Springer, 2008, pp. 1–13.

[65] Christopher Wolf, An Braeken, and Bart Preneel, *Efficient cryptanalysis of RSE(2) PKC and RSSE(2) PKC*, Security in Communication Networks: Fourth International Conference, SCN 2004, Amalfi, Italy, September 8-10, 2004, Lecture Notes in Comput. Sci., vol. 3352, Springer, Berlin, 2005, pp. 294–309.

[66] ———, *On the security of stepwise triangular systems*, Des. Codes Cryptogr. **40** (2006), no. 3, 285–302. MR MR2251321

[67] W. Christopher Wolf, *Multivariate quadratic polynomials in public key cryptography*, 2005.

[68] Kenneth Koon-Ho Wong, *Applications of finite field computation to cryptology: Extension field arithmetic in public key systems and algebraic attacks on stream ciphers*, Phd, Queensland University of Technology, 2008.

[69] Kenneth Koon-Ho Wong, Gregory V. Bard, and Robert H. Lewis, *Partitioning multivariate polynomial equations via vertex separators for algebraic cryptanalysis and mathematical applications*, 2009.

[70] Bo-Yin Yang, Chen-Mou Cheng, Bor-Rong Chen, and Chen Jiun-Ming, *Implementing minimized multivariate public-key cryptosystems on low-resource embedded systems*, 2005.

Curve-Based Cryptography

[1] Toru Akishita, Masanobu Katagi, Izuru Kitamura, and Tsuyoshi Takagi, *Some improved algorithms for hyperelliptic curve cryptosystems using degenerate divisors*, Information Security and Cryptology. ICISC 2004: 7th International Conference, Seoul, Korea, December 2–3, 2004, Lecture Notes in Comput. Sci., vol. 3506, Springer, Berlin, 2005, p. 296.

[2] Christine Abegail Antonio, Satoru Nakamula, and Ken Nakamula, *Comparing implementation efficiency of ordinary and squared pairings*, IACR eprint:2007:457 (2007).

[3] Christine Abegail Antonio, Satoru Tanaka, and Ken Nakamula, *Implementing cryptographic pairings over curves of embedding degrees 8 and 10*, 2007.

[4] Seigo Arita, Kazuto Matsuo, Koh-ichi Nagao, and Mahoro Shimura, *A Weil descent attack against elliptic curve cryptosystems over quartic extension fields*, IEICE Trans. Fundamentals **E89-A** (2006), no. 5, 28.

[5] Daniel V. Bailey, Brian Baldwin, Lejla Batina, Daniel J. Bernstein, Peter Birkner, Joppe W. Bos, Gauthier van Damme, Giacomo de Meulenaer, Junfeng Fan, Tim Gneysu, Frank Gurkaynak, Thorsten Kleinjung, Tanja Lange, Nele Mentens, Christof Paar, Francesco Regazzoni, Peter Schwabe, and Leif Uhsadel, *The Certicom Challenges ECC2-X*, Tech. report, 2009.

[6] M. Barbosa, A. Moss, and D. Page, *Compiler assisted elliptic curve cryptography*, On the Move to Meaningful Internet Systems 2007: CoopIS, DOA, ODBASE, GADA, and IS, Lecture Notes in Computer Science, vol. 4804/2007, Springer Berlin / Heidelberg, 2007, pp. 1785–1802.

[7] ———, *Constructive and destructive use of compilers in elliptic curve cryptography*, J. Cryptology **Online first** (2008), 23.

[8] Paulo S. L. M. Barreto, B. Lynn, and M. Scott, *Constructing elliptic curves with prescribed embedding degrees*, Security in Communication Networks: Third International Conference,SCN 2002,Amalfi,Italy,September 11-13,2002. Revised Papers., Lecture Notes in Comput. Sci., vol. 2576, Springer, Berlin, 2003, p. 257.

[9] Abdolali Basiri, Andreas Enge, Jean-Charles Faugère, and Nicolas Gürel, *Implementing the arithmetic of $C_{3,4}$ curves*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 87–101. MR MR2137346 (2006a:14101)

[10] Mark Bauer, Edlyn Teske, and Annegret Weng, *Point counting on Picard curves in large characteristic*, Math. Comp. **74** (2005), no. 252, 1983–2005 (electronic). MR MR2164107

[11] Daniel J. Bernstein, Peter Birkner, Tanja Lange, and Christiane Peters, *Optimizing double-base elliptic-curve single-scalar multiplication*, Progress in cryptology—INDOCRYPT 2007, Lecture Notes in Comput. Sci., vol. 4859, Springer, Berlin, 2007, pp. 167–182. MR MR2570254

[12] Daniel J. Bernstein and Tanja Lange, *Faster addition and doubling on elliptic curves*, Advances in Cryptology - ASIACRYPT 2007, Lecture Notes in Computer Science, vol. 4833/2007, Springer Berlin / Heidelberg, 2007, pp. 29–50.

[13] Peter Birkner, *Efficient arithmetic on low-genus curves*, Ph D thesis, Technische Universiteit Eindhoven, 2009.

[14] Friederike Brezing and Annegret Weng, *Elliptic curves suitable for pairing based cryptography*, Des. Codes Cryptogr. **37** (2005), no. 1, 133–141. MR MR2165045

[15] Ezra Brown, Bruce T. Myers, and Jerome A. Solinas, *Hyperelliptic curves with compact parameters*, Des. Codes Cryptogr. **36** (2005), no. 3, 245–261. MR MR2162578

[16] Kyo Il Chung, Mun-Kyu Lee, Kunsoo Park, and Tae Jun Park, *Speeding up scalar multiplication in genus 2 hyperelliptic curves with efficient endomorphisms*, ETRI **27** (2005), no. 5, 617–627.

[17] S. Cui, P. Duan, and C. W. Chan, *A new method of building more non-supersingular elliptic curves*, Computational Science and Its Applications, Lecture Notes in Comput. Sci., vol. 3481, Springer, Berlin, 2005, p. 657.

[18] Jan Denef and Frederik Vercauteren, *An extension of Kedlaya's algorithm to Artin-Schreier curves in characteristic 2*, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 308–323. MR MR2041093 (2005d:11088)

[19] Claus Diem, *The GHS attack in odd characteristic*, J. Ramanujan Math. Soc. **18** (2003), no. 1, 1–32. MR MR1966526 (2004a:14030)

[20] ______, *An index calculus algorithm for plane curves of small degree*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 543–557. MR MR2282948

[21] Claus Diem and Emmanuel Thomé, *Index calculus in class groups of non-hyperelliptic curves of genus three*, J. Cryptology **21** (2008), no. 4, 593–611. MR MR2438510

[22] Régis Dupont, Andreas Enge, and François Morain, *Building curves with arbitrary small MOV degree over finite prime fields*, J. Cryptology **18** (2005), no. 2, 79–89. MR MR2148052 (2006c:11073)

[23] I. Duursma, P. Gaudry, and F. Morain, *Speeding up the discrete log computation on curves with automorphisms*, Advances in Cryptology—Asiacrypt'99 (Singapore), Lecture Notes in Comput. Sci., vol. 1716, Springer, Berlin, 1999, pp. 103–121. MR MR1773225

[24] Stéphane Flon, Roger Oyono, and Christophe Ritzenthaler, *Fast addition on non-hyperelliptic genus 3 curves*, Algebraic geometry and its applications, Ser. Number Theory Appl., vol. 5, World Sci. Publ., Hackensack, NJ, 2008, pp. 1–28. MR MR2484046

[25] David Freeman, *Constructing pairing-friendly genus 2 curves with ordinary Jacobians*, Pairing-based cryptography—Pairing 2007, Lecture Notes in Comput. Sci., vol. 4575, Springer, Berlin, 2007, pp. 152–176. MR MR2423638

[26] David Freeman, Michael Scott, and Edlyn Teske, *A taxonomy of pairing-friendly elliptic curves*, Journal of Cryptology **23** (2010), no. 2, 224–280.

[27] S. Galbraith, F. Hess, and F. Vercauteren, *Aspects of pairing inversion*, IEEE Transactions on Information Theory **54** (2008), no. 12, 5719–5728.

[28] S. D. Galbraith, X. Lin, and D. J. Mireles, *Pairings on hyperelliptic curves with a real model*, LNCS 5209, Eds. Galbraith, S. D. and Paterson, K. G.., Springer, 2008, pp. 256–281.

[29] Steven Galbraith, *Disguising tori and elliptic curves*, 2006.

[30] Steven D. Galbraith, *Supersingular curves in cryptography*, Advances in Cryptology—Asiacrypt 2001 (Gold Coast), Lecture Notes in Comput. Sci., vol. 2248, Springer, Berlin, 2001, pp. 495–513. MR MR1934860 (2004b:14037)

[31] ———, *Weil descent of Jacobians*, Discrete Appl. Math. **128** (2003), no. 1, 165–180, International Workshop on Coding and Cryptography (WCC 2001) (Paris). MR MR1991424 (2004m:14046)

[32] Steven D. Galbraith, Michael Harrison, and David J. Mireles Morales, *Efficient hyperelliptic arithmetic using balanced representation for divisors*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, pp. 342–356. MR MR2467851 (2010f:14024)

[33] Steven D. Galbraith, Florian Hess, and Nigel P. Smart, *Extending the GHS Weil descent attack*, Advances in Cryptology—Eurocrypt 2002 (Amsterdam), Lecture Notes in Comput. Sci., vol. 2332, Springer, Berlin, 2002, pp. 29–44. MR MR1975526 (2004f:94060)

[34] Steven D. Galbraith, Xibin Lin, and David J. Mireles Morales, *Pairings on hyperelliptic curves with a real model*, Pairing-Based Cryptography, Pairing 2008, Lecture Notes in Computer Science, vol. 5209, Springer, 2008, pp. 265–281.

[35] P. Gaudry, *Fast genus 2 arithmetic based on theta functions*, 2005.

[36] P. Gaudry, F. Hess, and N. P. Smart, *Constructive and destructive facets of Weil descent on elliptic curves*, J. Cryptology **15** (2002), no. 1, 19–46. MR MR1880933 (2003b:14032)

[37] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng, *The 2-adic CM method for genus 2 curves with application to cryptography*, Advances in cryptology—ASIACRYPT 2006, Lecture Notes in Comput. Sci., vol. 4284, Springer, Berlin, 2006, pp. 114–129. MR MR2444631 (2009j:94110)

[38] Pierrick Gaudry, *An algorithm for solving the discrete log problem on hyperelliptic curves*, Advances in Cryptology—Eurocrypt 2000 (Bruges), Lecture Notes in Comput. Sci., vol. 1807, Springer, Berlin, 2000, pp. 19–34. MR MR1772021

[39] ———, *Index calculus for abelian varieties and the elliptic curve discrete logarithm problem*, 2004.

[40] Pierrick Gaudry and Nicolas Gürel, *An extension of Kedlaya's point-counting algorithm to superelliptic curves*, Advances in Cryptology—Asiacrypt 2001 (Gold Coast), Lecture Notes in Comput. Sci., vol. 2248, Springer, Berlin, 2001, pp. 480–494. MR MR1934859 (2003h:11159)

[41] Pierrick Gaudry and Éric Schost, *Construction of secure random curves of genus 2 over prime fields*, Advances in Cryptology—EuroCrypt 2004, Lecture Notes in Comput. Sci., vol. 3027, Springer, Berlin, 2004, pp. 239–256. MR MR2153176

[42] R. Granger and F. Vercauteren, *On the discrete logarithm problem on algebraic tori*, Crypto 2005: 25th Annual International Cryptology Conference (Santa Barbara, Cal., Lecture Notes in Comput. Sci., vol. 3621, Springer, Berlin, 2005, p. 66.

[43] Robert Granger, *On the static Diffie-Hellman problem on elliptic curves over extension fields*, Advances in Cryptology - ASIACRYPT 2010 (Masayuki Abe, ed.), Lecture Notes in Computer Science, vol. 6477, Springer Berlin/Heidelberg, 2010, pp. 283–302.

[44] Nicolas Gürel, *Extracting bits from coordinates of a point of an elliptic curve*, 2005.

[45] Darrel Hankerson, Koray Karabina, and Alfred Menezes, *Analyzing the Galbraith-Lin-Scott point multiplication method for elliptic curves over binary fields*, 2008.

[46] David Harvey, *Kedlaya's algorithm in larger characteristic*, Int. Math. Res. Not. IMRN (2007), no. 22, Art. ID rnm095, 29. MR MR2376210

[47] F. Hess, *Weil descent attacks*, Advances in Elliptic Curve Cryptography, London Math. Soc. Lecture Note Ser., vol. 317, Cambridge Univ. Press, Cambridge, 2005, pp. 151–180. MR MR2169214

[48] Laura Hitt, *Families of genus 2 curves with small embedding degree*, J. Math. Cryptol. **3** (2009), no. 1, 19–36. MR MR2524253

[49] Koh ichi Nagao, *Decomposed attack for the jacobian of a hyperelliptic curve over an extension field*, 2007.

[50] Farzali A. Izadi and V. Kumar Murty, *Counting points on an abelian variety over a finite field*, Progress in Cryptology—Indocrypt 2003, Lecture Notes in Comput. Sci., vol. 2904, Springer, Berlin, 2003, pp. 323–333. MR MR2092391 (2005f:11127)

[51] Waldyr D. Benits Junior and Steven D. Galbraith, *Constructing pairing-friendly elliptic curves using Gröbner basis reduction*, Cryptography and Coding, Lecture Notes in Computer Science, vol. 4887/2007, Springer Berlin / Heidelberg, 2007, pp. 336–345.

[52] Koray Karabina and Edlyn Teske, *On prime-order elliptic curves with embedding degrees k=3,4, and 6*, Algorithmic Number Theory, Lecture Notes in Computer Science, vol. 5011, Springer, 2008, pp. 102–117.

[53] Masanobu Katagi, Toru Akishita, Izuru Kitamura, and Tsuyoshi Takagi, *Efficient hyperelliptic curve cryptosystems using theta divisors*, IEICE Trans. Fundamentals **E89-A** (2006), no. 1, 151–160.

[54] Masanobu Katagi, Izuru Kitamura, and Tsuyoshi Takagi, *A point halving algorithm for hyperelliptic curves.*

[55] David R. Kohel, *The AGM-$X_0(N)$ Heegner point lifting algorithm and elliptic curve point counting*, Advances in Cryptology—Asiacrypt 2003, Lecture Notes in Comput. Sci., vol. 2894, Springer, Berlin, 2003, pp. 124–136. MR MR2093256 (2005i:11077)

[56] Tanja Lange and Marc Stevens, *Efficient doubling on genus two curves over binary fields*, Selected Areas in Cryptography, Lecture Notes in Comput. Sci., vol. 3357, Springer, Berlin, 2005, pp. 170–181. MR MR2181316

[57] Eunjeong Lee, Hyang-Sook Lee, and Cheol-Min Park, *Efficient and generalized pairing computation on abelian varieties*, IEEE Trans. Inform. Theory **55** (2009), no. 4, 1793–1803. MR MR2582765

[58] Reynald Lercier and David Lubicz, *A quasi-quadratic time algorithm for hyperelliptic curve point counting*, Ramanujan J. **12** (2006), no. 3, 399–423. MR MR2293798 (2008b:11069)

[59] Kazuto Matsuo, Jinhui Chao, and Shigeo Tsujii, *An improved baby step giant step algorithm for point counting of hyperelliptic curves over finite fields*, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 461–474. MR MR2041104 (2005a:11089)

[60] Markus Maurer, Alfred Menezes, and Edlyn Teske, *Analysis of the GHS Weil descent attack on the ECDLP over characteristic two finite fields of composite degree (extended abstract)*, Progress in Cryptology—Indocrypt 2001 (Chennai), Lecture Notes in Comput. Sci., vol. 2247, Springer, Berlin, 2001, pp. 195–213. MR MR1934497

[61] ______, *Analysis of the GHS Weil descent attack on the ECDLP over characteristic two finite fields of composite degree*, LMS J. Comput. Math. **5** (2002), 127–174 (electronic). MR MR1942257 (2003k:94034)

[62] J. Miret, D. Sadornil, J. Tena, R. Tomàs, and M. Valls, *Isogeny cordillera algorithm to obtain cryptographically good elliptic curves*, ACSW '07: Proceedings of the fifth

Australasian symposium on ACSW frontiers, Australian Computer Society, Inc., 2007, pp. 153–157.

[63] Nadia El Mrabet, Nicolas Guillermin, and Sorina Ionica, *A study of pairing computation for curves with embedding degree* 15, 2009.

[64] A. Muzereau, N. P. Smart, and F. Vercauteren, *The equivalence between the DHP and DLP for elliptic curves used in practical applications*, LMS J. Comput. Math. **7** (2004), 50–72 (electronic). MR MR2047214 (2005b:94038)

[65] Laura Hitt O'Connor, Gary McGuire, Michael Naehrig, and Marco Streng, *CM construction of genus 2 curves with p-rank 1*, 2008.

[66] Tae-Jun Park, Mun-Kyu Lee, and Kunsoo Park, *Efficient scalar multiplication in hyperelliptic curves using a new Frobenius expansion*, ICISC 2003: Information Security and Cryptology, Lecture Notes in Comput. Sci., vol. 2971, Springer, Berlin, 2004, pp. 152–165. MR MR2093706 (2005f:94116)

[67] L. J. D. Perez, Ezekiel J. Kachisa, and Michael Scott, *Implementing cryptographic pairings: A Magma tutorial*, 2009.

[68] Tanaka Satoru and Nakamula Ken, *More constructing pairing-friendly elliptic curves for cryptography*, 2007.

[69] Jasper Scholten, *Weil restriction of an elliptic curve over a quadratic extension*, 2004.

[70] Michael Scott and Paulo S. L. M. Barreto, *On a (flawed) proposal to build more pairing-friendly curves*, 2005.

[71] Katsuyuki Takashima, *New families of hyperelliptic curves with efficient Gallant-Lambert-Vanstone method*, Information Security and Cryptology, ICISC 2004: 7th International Conference, Seoul, Korea, December 2-3, 2004, Lecture Notes in Comput. Sci., vol. 3506, Springer, Berlin, 2005, pp. 279–295.

[72] Katsuyuki Takashima, *A new type of fast endomorphisms on Jacobians of hyperelliptic curves and their cryptographic application*, IEICE Trans. Fundamentals **E89-A** (2006), no. 1, 124–133.

[73] ———, *Scaling security of elliptic curves with fast pairing using efficient endomorphisms*, IEICE Trans. Fundamentals **E-90A** (2007), no. 1, 152–159.

[74] ———, *Efficiently computable distortion maps for supersingular curves*, Algorithmic Number Theory, Lecture Notes in Computer Science, vol. 5011, Springer Berlin/Heidelberg, 2008, pp. 88–101.

[75] Satoru Tanaka and Ken Nakamula, *Constructing pairing-friendly elliptic curves using factorization of cyclotomic polynomials*, Pairing-Based Cryptography, Pairing 2008, Lecture Notes in Computer Science, vol. 5209, Springer, 2008, pp. 136–145.

[76] Edlyn Teske, *An elliptic curve trapdoor system (extended abstract)*, High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams, Fields Inst. Commun., vol. 41, Amer. Math. Soc., Providence, RI, 2004, pp. 341–352. MR MR2076258

[77] ———, *An elliptic curve trapdoor system*, J. Cryptology **19** (2006), no. 1, 115–133. MR MR2210901 (2006k:94116)

[78] Frederik Vercauteren, *The hidden root problem*, Pairing-Based Cryptography - Pairing, Lecture Notes in Computer Science, vol. 5209, SpringerLink, Berlin, 2008, pp. 89–99. MR)

[79] Eric R. Verheul, *Evidence that XTR is more secure than supersingular elliptic curve cryptosystems*, J. Cryptology **17** (2004), no. 4, 277–296. MR MR2090558

[80] Annegret Weng, *Generation of random Picard curves for cryptography*, 2004.

[81] ———, *A low-memory algorithm for point counting on Picard curves*, Des. Codes Cryptogr. **38** (2006), no. 3, 383–393. MR MR2195523 (2006j:11168)

[82] Fangguo Zhang, *Twisted ate pairing on hyperelliptic curves and applications*, 2008.

[83] Chang-An Zhao, Fangguo Zhang, and Jiwu Huang, *All pairings are in a group*, IEICE Trans A: Fundamentals **E91-A** (2008), no. 10, 3084–3087.

Protocols

[1] Gregory V. Bard, *The application of polynomials over the field of two elements to a problem in intellectual property*, 2009.

[2] S.T. Dougherty, S. Mesnager, and P. Sole, *Secret-sharing schemes based on self-dual codes*, Information Theory Workshop, 2008. ITW '08. IEEE (2008), 338–342.

[3] Greg Gamble, Barbara M. Macnhaut, Jennifer Seberry, and Anne Penfold Street, *Further results on strongbox secured secret sharing schemes*, Util. Math. **66** (2004), 165–193. MR MR2106217 (2005g:94090)

[4] Shuhui Hou, Tetsutaro Uehara, Yoshitaka Morimura, and Michihiko Minoh, *Fingerprinting codes for live pay-television broadcast via internet*, Multimedia Content Analysis and Mining, Lecture Notes in Computer Science, vol. 4577/2007, Springer Berlin / Heidelberg, 2007, pp. 252–261.

[5] David Jao and Kayo Yoshida, *Boneh-Boyen signatures and the strong Diffie-Hellman problem*, 2009.

[6] Antoine Joux, Reynald Lercier, David Naccache, and Emmanuel Thomé, *Oracle-assisted static Diffie-Hellman is easier than discrete logarithms*, 2008.

[7] Kerem Kaskaloglu and Ferruh Özbudak, *A simple scheme for hierarchical threshold access structures*, 2009, p. 8.

[8] Matthias Krause and Dirk Stegemann, *More on the security of linear RFID authentication protocols*, Selected Areas in Cryptography, Lecture Notes in Comput. Sci., vol. 5867, Springer, Berlin, 2009, pp. 182–196.

[9] Sihem Mesnager, P. Solé, and Steven T. Dougherty, *Secret sharing schemes based on self-dual codes*, Information Theory Workshop, 2008. ITW '08. IEEE (2008), 338 – 342.

[10] Rainer Steinwandt and Viktória I. Villányi, *A one-time signature using run-length encoding*, Inform. Process. Lett. **108** (2008), no. 4, 179–185. MR MR2457922

[11] Suratose Tritilanunt, Colin Boyd, Ernest Foo, and Juan Manuel González Nieto, *Toward non-parallelizable client puzzles*, Cryptology and Network Security, Lecture Notes in Computer Science, vol. 4856/2007, Springer, Berlin/Heidelberg, 2007, pp. 247–264.

Random Number Generators

[1] Michael Feng-Hao Liu, Chi-Jen Lu, Bo-Yin Yang, and Jintai Ding, *Secure PRNGs from specialized polynomial maps over any F_q*, 2007.

[2] D. Schellekens, B. Preneel, and I. Verbauwhede, *FPGA vendor agnostic true random number generator*, Field Programmable Logic and Applications, 2006. FPL '06 (2006).

Computational Methods

[1] Gwénolé Ars, Jean-Charles Faugère, Hideki Imai, Mitsuru Kawazoe, and Makoto Sugita, *Comparison between XL and Gröbner basis algorithms*, Advances in Cryptology—Asiacrypt 2004, Lecture Notes in Comput. Sci., vol. 3329, Springer, Berlin, 2004, pp. 338–353. MR MR2150425 (2006k:13056)

[2] Roberto Maria Avanzi, *Another look at square roots (and other less common operations) in fields of even characteristic*, Selected Areas in Cryptography, Lecture Notes in Computer Science, vol. 4876/2007, Springer Berlin / Heidelberg, 2007, pp. 138–154.

[3] M. Barbosa, R. Noad, D. Page, and N. P. Smart, *First steps toward a cryptography-aware language and compiler.*

[4] Gregory V. Bard, Nicolas T. Courtois, and Chris Jefferson, *Efficient methods for conversion and solution of sparse systems of low-degree multivariate polynomials over* GF(2) *via SAT-solvers*, 2007.

[5] Aurélie Bauer and Antoine Joux, *Toward a rigorous variation of Coppersmith's algorithm on three variables*, Advances in cryptology—EUROCRYPT 2007, Lecture Notes in Comput. Sci., vol. 4515, Springer, Berlin, 2007, pp. 361–378. MR MR2449220

[6] Stanislav Bulygin and Michael Brickenstein, *Obtaining and solving systems of equations in key variables only for the small variants of AES*, 2008.

[7] Wouter Castryck, Hendrik Hubrechts, and Frederik Vercauteren, *Computing zeta functions in families of $C_{a,b}$ curves using deformation*, Algorithmic Number Theory, Lecture Notes in Computer Science, vol. 5011, Springer, 2008, pp. 296–311.

[8] Chia-Hsin Owen Chen, Ming-Shing Chen, Jintai Ding, Fabian Werner, and Bo-Yin Yang, *Odd-char multivariate hidden field equations*, 2008.

[9] Jiun-Ming Chen and Bo-Yin Yang, *All in the XL family: Theory and practice*, Information Security and Cryptology. ICISC 2004: 7th International Conference, Seoul, Korea, December 2–3, 2004, Lecture Notes in Comput. Sci., vol. 3506, Springer, Berlin, 2005, p. 296.

[10] Jean-Charles Faugére and Ludovic Perret, *Algebraic cryptanalysis of Curry and Flurry using correlated messages*, 2008.

[11] Antoine Joux, David Naccache, and Emmanuel Thomé, *When e-th roots become easier than factoring*, Advances in Cryptology - ASIACRYPT 2007, Lecture Notes in Computer Science, vol. 4833/2007, Springer Berlin / Heidelberg, 2007, pp. 13–28.

[12] David R. Kohel, *The AGM-$X_0(N)$ Heegner point lifting algorithm and elliptic curve point counting*, Advances in Cryptology—Asiacrypt 2003, Lecture Notes in Comput. Sci., vol. 2894, Springer, Berlin, 2003, pp. 124–136. MR MR2093256 (2005i:11077)

[13] Czesław Kościelny, *Computing in the composite* $\mathrm{GF}(q^m)$ *of characteristic* 2 *formed by means of an irreducible binomial*, Appl. Math. Comput. Sci. **8** (1998), no. 3, 671–680. MR MR1647512 (99i:94047)

[14] Kazuto Matsuo, Jinhui Chao, and Shigeo Tsujii, *An improved baby step giant step algorithm for point counting of hyperelliptic curves over finite fields*, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 461–474. MR MR2041104 (2005a:11089)

[15] Mohamed Saied Emam Mohamed, Wael Said Abd Elmageed Mohamed, Jintai Ding, and Johannes Buchmann, *MXL2: Solving polynomial equations over GF*(2) *using an improved mutant strategy*, Post-Quantum Cryptography, Lecture Notes in Comput. Sci., vol. 5299, Springer, Berlin, 2008, pp. 203–215.

[16] Naoki Ogura and Shigenori Uchiyama, *Cryptanalysis of the birational permutation signature scheme over a non-commutative ring*, 2009.

[17] Mikael Olofsson, *Vlsi Aspects on Inversion in Finite Fields*, PhD Thesis, Linköpings Universitet, Linköping, Sweden, 2002.

[18] Håvard Raddum and Igor Semaev, *Solving multiple right hand sides linear equations*, Des. Codes Cryptogr. **49** (2008), no. 1-3, 147–160. MR MR2438447

[19] A. J. M. Segers, *Algebraic Attacks from a Gröbner Basis Perspective*, MSc Thesis, Technische Universiteit Eindhoven, 2004.

[20] Igor Semaev, *Sparse boolean equations and circuit lattices*, 2009.

[21] B. Smith, *Isogenies and the discrete logarithm problem in Jacobians of genus* 3 *hyperelliptic curves*, J. Cryptology **22** (2009), no. 4, 505–529.

[22] Makoto Sugita, Mitsuru Kawazoe, and Hideki Imai, *Relation between the XL algorithm and Groebner basis algorithms*, IEICE Trans. Fundamentals **E89-A** (2006), no. 1, 11–18.

[23] Kenneth Koon-Ho Wong, Gregory V. Bard, and Robert H. Lewis, *Partitioning multivariate polynomial equations via vertex separators for algebraic cryptanalysis and mathematical applications*, 2009.