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.