# 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.