Computational Methods

11-04 and 11Yxx

[1] Fadwa S. Abu Muriefah, Florian Luca, and Alain Togbé, *On the Diophantine equation* $x^2 + 5^a 13^b = y^n$, Glasg. Math. J. **50** (2008), no. 1, 175–181. MR MR2381741 (2008m:11071)

[2] Fatima K. Abu Salem and Kamal Khuri-Makdisi, *Fast Jacobian group operations for* $C_{3,4}$ *curves over a large finite field*, LMS J. Comput. Math. **10** (2007), 307–328 (electronic). MR MR2335723

[3] Ali Akhavi and Damien Stehlé, *Speeding-up lattice reduction with random projections (extended abstract)*, LATIN 2008: Theoretical informatics, Lecture Notes in Comput. Sci., vol. 4957, Springer, Berlin, 2008, pp. 293–305. MR MR2472745

[4] Bill Allombert, *An efficient algorithm for the computation of Galois automorphisms*, Math. Comp. **73** (2004), no. 245, 359–375 (electronic). MR MR2034127 (2004k:11193)

[5] 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.

[6] Eric Bach and Denis Charles, *The hardness of computing an eigenform*, Computational arithmetic geometry, Contemp. Math., vol. 463, Amer. Math. Soc., Providence, RI, 2008, pp. 9–15. MR MR2459985 (2009i:11051)

[7] Werner Backes and Susanne Wetzel, *An efficient LLL gram using buffered transformations*, Computer Algebra in Scientific Computing, Lecture Notes in Computer Science, vol. 4770/2007, Springer Berlin / Heidelberg, 2007, pp. 31–44.

[8] David H. Bailey, Jonathan M. Borwein, Vishaal Kapoor, and Eric W. Weisstein, *Ten problems in experimental mathematics*, Amer. Math. Monthly **113** (2006), no. 6, 481–509. MR MR2231135 (2007b:65001)

[9] Stéphane Ballet, *Quasi-optimal algorithms for multiplication in the extensions of* $\mathbf{F_{16}}$ *of degree 13, 14 and 15*, J. Pure Appl. Algebra **171** (2002), no. 2-3, 149–164. MR MR1904474 (2003b:11133)

[10] M. Bauer, M. J. Jacobson, Jr., Y. Lee, and R. Scheidler, *Construction of hyperelliptic function fields of high three-rank*, Math. Comp. **77** (2008), no. 261, 503–530 (electronic). MR MR2353964

[11] Michael Beck, Eric Pine, Wayne Tarrant, and Kim Yarbrough Jensen, *New integer representations as the sum of three cubes*, Math. Comp. **76** (2007), no. 259, 1683–1690 (electronic). MR MR2299795 (2007m:11170)

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

[13] 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

[14] Daniel J. Bernstein, Peter Birkner, Tanja Lange, and Christiane Peters, *ECM using Edwards curves*, 2008.

[15] 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.

[16] Amnon Besser and Rob De Jeu, li(p)*-service? an algorithm for computing p-adic polyalgorithms*, Math. Comp. **77** (2008), no. 262, 1105–1134. MR MR2373194

[17] Peter Birkner, *Efficient divisor class halving on genus two curves*, Selected Areas in Cryptography, Lecture Notes in Computer Science, vol. 4356, Springer, Berlin/Heidelberg, pp. 317–326.

[18] Werner Bley and Robert Boltje, *Computation of locally free class groups*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 72–86. MR MR2282916

[19] Jonathan Borwein and David Bailey, *Mathematics by Experiment*, A K Peters Ltd., Natick, MA, 2004, Plausible reasoning in the 21st century. MR MR2033012 (2005b:00012)

[20] Wieb Bosma, *Some computational experiments in number theory*, Discovering Mathematics with Magma, Algorithms Comput. Math., vol. 19, Springer, Berlin, 2006, pp. 1–30. MR MR2278921

[21] Wieb Bosma, John Cannon, and Allan Steel, *Lattices of compatibly embedded finite fields*, J. Symbolic Comput. **24** (1997), no. 3-4, 351–369, Computational algebra and number theory (London, 1993). MR MR1484485 (99a:11143)

[22] Wieb Bosma and Bart de Smit, *Class number relations from a computational point of view*, J. Symbolic Comput. **31** (2001), no. 1-2, 97–112, Computational algebra and number theory (Milwaukee, WI, 1996). MR MR1806209 (2002a:11144)

[23] ———, *On arithmetically equivalent number fields of small degree*, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 67–79. MR MR2041074 (2005e:11169)

[24] Wieb Bosma and Ben Kane, *The Aliquot constant*, 2009.

[25] Wieb Bosma and Arjen K. Lenstra, *An implementation of the elliptic curve integer factorization method*, Computational Algebra and Number Theory (Sydney, 1992), Math. Appl., vol. 325, Kluwer Acad. Publ., Dordrecht, 1995, pp. 119–136. MR MR1344926 (96d:11134)

[26] Wieb Bosma and Peter Stevenhagen, *Density computations for real quadratic units*, Math. Comp. **65** (1996), no. 215, 1327–1337. MR MR1344607 (96j:11171)

[27] Johan Bosman, *On the computation of Galois representations associated to level one modular forms*, 2007.

[28] Alin Bostan, Pierrick Gaudry, and Éric Schost, *Linear recurrences with polynomial coefficients and computation of the Cartier-Manin operator on hyperelliptic curves*, Finite Fields and Applications, Lecture Notes in Comput. Sci., vol. 2948, Springer, Berlin, 2004, pp. 40–58. MR MR2092621

[29] Aaron Bradord, Michael Monagan, and Colin Percival, *Integer factorization and computing discrete logarithms in Maple*, Proceedings of the 2006 Maple Conference, 2006, pp. 2–13.

[30] Richard P. Brent, *Factorization of the tenth Fermat number*, Math. Comp. **68** (1999), no. 225, 429–451. MR MR1489968 (99e:11154)

[31] ———, *Recent progress and prospects for integer factorisation algorithms*, Computing and Combinatorics (Sydney, 2000), Lecture Notes in Comput. Sci., vol. 1858, Springer, Berlin, 2000, pp. 3–22. MR MR1866110 (2002h:11138)

[32] ———, *Note on Marsaglia's xorshift random number generators*, J. Stat. Soft **11** (2004), no. 5, 1–5.

[33] Nils Bruin and Michael Stoll, *Deciding existence of rational points on curves: an experiment*, Experiment. Math. **17** (2008), no. 2, 181–189. MR MR2433884

[34] Nils Bruin and Michael Stoll, *Two-cover descent on hyperelliptic curves*, 2008.

[35] ———, *The Mordell-Weil sieve: Proving non-existence of rational points on curves*, LMS J. Comput. Math **13** (2010), 272–306.

[36] David G. Cantor and Daniel M. Gordon, *Factoring polynomials over p-adic fields*, Algorithmic Number Theory (Leiden, 2000), Lecture Notes in Comput. Sci., vol. 1838, Springer, Berlin, 2000, pp. 185–208. MR MR1850606 (2002f:11175)

[37] Robert Carls, *Explicit Frobenius lifts on elliptic curves*, 2009.

[38] ———, *Fast point counting on genus two curves in characteristic three*, 2010.

[39] 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.

[40] Antoine Chambert-Loir, *Compter (rapidement) le nombre de solutions d'equations dans les corps finis*, 2006.

[41] Hugo Chapdelaine, *Computation of p-units in ray class fields of real quadratic number fields*, Math. Comp. **78** (2009), 2307–2345.

[42] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll, *Explicit n-descent on elliptic curves. I. Algebra*, J. reine angew. Math. **615** (2008), 121–155. MR MR2384334

[43] J. E. Cremona and D. Rusin, *Efficient solution of rational conics*, Math. Comp. **72** (2003), no. 243, 1417–1441 (electronic). MR MR1972744 (2004a:11137)

[44] M. Daberkow, *Computing with subfields*, J. Symbolic Comput. **24** (1997), no. 3-4, 371–384, Computational algebra and number theory (London, 1993). MR MR1484486 (98k:11185)

[45] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörnig, and K. Wildanger, *KANT V4*, J. Symbolic Comput. **24** (1997), no. 3-4, 267–283, Computational algebra and number theory (London, 1993). MR MR1484479 (99g:11150)

[46] Lassina Dembélé, *Quaternionic Manin symbols, Brandt matrices, and Hilbert modular forms*, Math. Comp. **76** (2007), no. 258, 1039–1057 (electronic). MR MR2291849

[47] Lassina Dembélé, *On the computation of algebraic modular forms on compact inner forms of GSp_4*, 2009.

[48] Lassina Dembélé and Steve Donnelly, *Computing Hilbert modular forms over fields with nontrivial class group*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, pp. 371–386. MR MR2467859 (2010d:11149)

[49] Francisco Diaz y Diaz, Jean-François Jaulent, Sebastian Pauli, Michael Pohst, and Florence Soriano-Gafiuk, *A new algorithm for the computation of logarithmic l-class groups of number fields*, Experiment. Math. **14** (2005), no. 1, 65–74. MR MR2146520 (2006d:11154)

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

[51] ———, *Index calculus in class groups of plane curves of small degree*, 2005.

[52] ———, *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

[53] Jintai Ding, Jason E. Gower, and Dieter S. Schmidt, *Zhuang-Zi: A new algorithm for solving multivariate polynomial equations over a finite field*, 2006.

[54] Jacques Dubrois and Jean-Guillaume Dumas, *Efficient polynomial time algorithms computing industrial-strength primitive roots*, Inform. Process. Lett. **97** (2006), no. 2, 41–45. MR MR2187046 (2006h:68064)

[55] Sylvain Duquesne, *Montgomery ladder for all genus 2 curves in characteristic 2*, Arithmetic of Finite Fields, Lecture Notes in Computer Science, vol. 5130, Springer, 2008, pp. 174–188.

[56] 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

[57] Luca De Feo, *Fast algorithms for computing isogenies between ordinary elliptic curves in small characteristic*, J. Number Theory **To appear** (2010).

[58] Claus Fieker, *Applications of the class field theory of global fields*, Discovering Mathematics with Magma, Algorithms Comput. Math., vol. 19, Springer, Berlin, 2006, pp. 31–62. MR MR2278922

[59] ———, *Sparse representation for cyclotomic fields*, Experiment. Math. **16** (2007), no. 4, 493–500. MR MR2378488

[60] Claus Fieker and Willem A. de Graaf, *Finding integral linear dependencies of algebraic numbers and algebraic Lie algebras*, LMS J. Comput. Math. **10** (2007), 271–287 (electronic). MR MR2320832 (2008f:11119)

[61] Claus Fieker and Michael E. Pohst, *Dependency of units in number fields*, Math. Comp. **75** (2006), no. 255, 1507–1518 (electronic). MR MR2219041 (2007a:11168)

[62] Tom Fisher, *The Hessian of a genus one curve*, 2006.

[63] ———, *The invariants of a genus one curve*, Proc. Lond. Math. Soc. (3) **97** (2008), no. 3, 753–782. MR MR2448246

[64] ———, *Some improvements to 4-descent on an elliptic curve*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, pp. 125–138. MR MR2467841 (2009m:11078)

[65] E. V. Flynn and C. Grattoni, *Descent via isogeny on elliptic curves with large rational torsion subgroups*, J. Symbolic Comput. **43** (2008), no. 4, 293–303. MR MR2402033

[66] Felix Fontein, *The infrastructure of a global field of arbitrary unit rank*, 2008.

[67] Robert Fraatz, *Computation of maximal orders of cyclic extensions of function fields*, PhD Thesis, Technischen Universtät Berlin, 2005.

[68] 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

[69] David Mandell Freeman and Takakazu Satoh, *Constructing pairing-friendly hyperelliptic curves using Weil restriction*, 2010, pp. 1–31.

[70] 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)

[71] 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

[72] 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)

[73] Pierrick Gaudry, Alexander Kruppa, and Paul Zimmermann, *A GMP-based implementation of Schönhage-Strassen's large integer multiplication algorithm*, ISSAC 2007, ACM, New York, 2007, pp. 167–174. MR MR2396199

[74] Willi Geiselmann, Jörn Müller-Quade, and Rainer Steinwandt, *Comment on: "A new representation of elements of finite fields* $\mathrm{GF}(2^m)$ *yielding small complexity arithmetic circuits" by G. Drolet*, IEEE Trans. Comput. **51** (2002), no. 12, 1460–1461. MR MR2012149

[75] Willi Geiselmann and Rainer Steinwandt, *A redundant representation of* $\mathrm{GF}(q^n)$ *for designing arithmetic circuits*, IEEE Trans. Comp **52** (2003), no. 7, 848–853.

[76] ———, *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)

[77] Martine Girard and Leopoldo Kulesz, *Computation of sets of rational points of genus-3 curves via the Demjanenko-Manin method*, LMS J. Comput. Math. **8** (2005), 267–300 (electronic). MR MR2193214

[78] Norbert Goeb, *Computing the automorphism groups of hyperelliptic function fields*, 2003.

[79] Grigor Grigorov, Andrei Jorza, Stefan Patrikis, William A. Stein, and Corina Tarnita, *Computational verification of the birch and swinnerton-dyer conjecture for individual elliptic curves*, Math. Comp **78** (2009), 2397–2425.

[80] J. Guardia, J. Montes, and E. Nart, *Higher Newton polygons and integral bases*, arXiv:0902.3428v1 (2009).

[81] Jordi Guardia, Jesus Montes, and Enric Nart, *Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields*, 2008.

[82] Lajos Hajdu, *Optimal systems of fundamental S-units for LLL-reduction*, Period. Math. Hungar. **59** (2009), no. 1, 53–79. MR MR2544620

[83] G. Hanrot and F. Morain, *Solvability by radicals from an algorithmic point of view*, Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation (New York), ACM, 2001, pp. 175–182 (electronic). MR MR2049746 (2005a:11200)

[84] 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

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

[86] ———, *A cache-friendly truncated FFT*, Theor. Comput. Sci. **410** (2009), no. 27-29, 2649–2658.

[87] Lenwood S. Heath and Nicholas A. Loehr, *New algorithms for generating Conway polynomials over finite fields*, J. Symbolic Comput. **38** (2004), no. 2, 1003–1024. MR MR2093563 (2005g:11247)

[88] 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

[89] Florian Hess, Sebastian Pauli, and Michael E. Pohst, *Computing the multiplicative group of residue class rings*, Math. Comp. **72** (2003), no. 243, 1531–1548 (electronic). MR MR1972751 (2004f:11126)

[90] Hendrik Hubrechts, *Point counting in families of hyperelliptic curves*, Found. Comput. Math. **8** (2008), no. 1, 137–169. MR MR2403533

[91] ———, *Quasi-quadratic elliptic curve point counting using rigid cohomology*, J. Symb. Comput. **44** (2009), no. 9, 1255–1267.

[92] Xavier Taixes i Ventosa and Gabor Wiese, *Computing congruences of modular forms and Galois representations modulo prime powers*, arXiv:0909.2724v2 (2009).

[93] David Jao and Vladimir Soukharev, *A subexponential algorithm for evaluating large degree isogenies*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 6197, Springer, Berlin, 2010, pp. 219–233.

[94] Jean-François Jaulent, Sebastian Pauli, Michael E. Pohst, and Florence Soriano-Gafiuk, *Computation of 2-groups of positive classes of exceptional number fields*, J. Théor. Nombres Bordeaux **20** (2008), no. 3, 715–732. MR MR2523314

[95] Antoine Joux and Reynald Lercier, *Counting points on elliptic curves in medium characteristic*, 2006, p. 15.

[96] Ben Kane, *CM liftings of supersingular elliptic curves*, 2009.

[97] Markus Kirschmer and John Voight, *Algorithmic enumeration of ideal classes for quaternion orders*, SIAM J. Comput **39** (2010), no. 5, 1714–1747.

[98] Jürgen Klüners, *Algorithms for function fields*, Experiment. Math. **11** (2002), no. 2, 171–181. MR MR1959261 (2003k:11193)

[99] Alan G.B. Lauder, *Degenerations and limit Frobenius structures in rigid cohomology*, 2009.

[100] Grégoire Lecerf, *Fast separable factorization and applications*, Appl. Algebra Engrg. Comm. Comput. **19** (2008), no. 2, 135–160. MR MR2389971 (2009b:13069)

[101] D. Lehavi and C. Ritzenthaler, *An explicit formula for the arithmetic-geometric mean in genus 3*, Experiment. Math. **16** (2007), no. 4, 421–440. MR MR2378484 (2008k:14070)

[102] Reynald Lercier and Thomas Sirvent, *On Elkies subgroups of l-torsion points in elliptic curves defined over a finite field*, J. Théor. Nombres Bordeaux **20** (2008), no. 3, 783–797. MR MR2523317

[103] Rudolf Lidl, *Computational problems in the theory of finite fields*, Appl. Algebra Engrg. Comm. Comput. **2** (1991), no. 2, 81–89. MR MR1325520 (95m:11134)

[104] J. M. Miret, R. Moreno, J. Pujolàs, and A. Rio, *Halving for the 2-Sylow subgroup of genus 2 curves over binary fields*, Finite Fields Appl. **15** (2009), no. 5, 569–579. MR MR2554040

[105] Marcel Mohyla and Gabor Wiese, *A computational study of the asymptotic behaviour of coefficient fields of modular forms*, 2009.

[106] Michael Monagan and Mark van Hoeij, *A modular algorithm for computing polynomial GCDs over number fields presented with multiple extensions*.

[107] I. Morel, D. Stehlé, and G. Villard, *Analyse numerique et reduction de reseaux*, 2009.

[108] J.-M. Muller, N. Brisebarre, F. de Dinechin, C.-P. Jeannerod, L. Vincent, G. Melquiond, N. Revol, D. Stehlé, and S. Torres, *Handbook of floating-point arithmetic*, Birkhäuser, Boston, MA, 2009.

[109] Siguna Müller, *On the computation of square roots in finite fields*, Des. Codes Cryptogr. **31** (2004), no. 3, 301–312. MR MR2047886 (2005f:11278)

[110] Phong Q. Nguên and Damien Stehlé, *Floating-point LLL revisited*, Advances in cryptology—EUROCRYPT 2005, Lecture Notes in Comput. Sci., vol. 3494, Springer, Berlin, 2005, pp. 215–233. MR MR2352190 (2008m:94017)

[111] Harris Nover, *Computation of Galois groups associated to the 2-class towers of some imaginary quadratic fields with 2-class group* $c2 \times c2 \times c2$, Journal of Number Theory **129** (2009), no. 1, 231 – 245.

[112] Titus Piezas, *Solving solvable sextics using polynomial decomposition*, 2004.

[113] M. E. Pohst, *Computational aspects of Kummer theory*, Algorithmic number theory (Talence, 1996), Lecture Notes in Comput. Sci., vol. 1122, Springer, Berlin, 1996, pp. 259–272. MR MR1446518 (98f:11112)

[114] Xavier-François Roblot, *Polynomial factorization algorithms over number fields*, J. Symbolic Comput. **38** (2004), no. 5, 1429–1443. MR MR2168722

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

[116] René Schoof, *Computing Arakelov class groups*, Algorithmic number theory: lattices, number fields, curves and cryptography, Math. Sci. Res. Inst. Publ., vol. 44, Cambridge Univ. Press, Cambridge, 2008, pp. 447–495. MR MR2467554

[117] Nigel P. Smart, *The Algorithmic Resolution of Diophantine Equations*, London Mathematical Society Student Texts, vol. 41, Cambridge University Press, Cambridge, 1998. MR MR1689189 (2000c:11208)

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

[119] 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.

[120] Damien Stehlé, *Floating-point LLL: Theoretical and practical aspects*, Proceedings of LLL+25 Conference, 2007 (2009).

[121] Damien Stehlé, *Floating-point LLL: Theoretical and practical aspects*, Information Security and Cryptography: The LLL Algorithm (Berlin Heidelberg) (David Basin, Ueli Maurer, Phong Q. Nguyen, and Brigitte Vallée, eds.), Information Security and Cryptography, Springer, 2010, pp. 179–213.

[122] Damien Stehlé and Paul Zimmermann, *A binary recursive GCD algorithm*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 411–425. MR MR2138011

[123] William A. Stein, *An introduction to computing modular forms using modular symbols*, Algorithmic number theory: lattices, number fields, curves and cryptography, Math. Sci. Res. Inst. Publ., vol. 44, Cambridge Univ. Press, Cambridge, 2008, pp. 641–652. MR MR2467560 (2009k:11085)

[124] 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.

[125] Nicolas M. Thiéry, *Computing minimal generating sets of invariant rings of permutation groups with SAGBI-Gröbner basis*, Discrete Mathematics and Theoretical Computer Science: 4th International Conference, DMTCS 2003, Dijon, France, July 7-12, 2003: Proceedings (Berlin) (Cristian Calude, Michael J. Dinneen, and Vincent

Vajnovszki, eds.), Lecture Notes in Computer Science, vol. 2731, Springer, 2003, pp. 315–328.

[126] Hans-Christian Graf v. Bothmer, *Finite field experiments (with an appendix by Stefan Wiedmann)*, Higher-Dimensional Geometry over Finite Fields, NATO Science for Peace and Security Series, D: Information and Communication Security, vol. 16, IOS Press, 2008, pp. 1–62.

[127] Mark van Hoeij, *Factoring polynomials and the knapsack problem*, J. Number Theory **95** (2002), no. 2, 167–189. MR MR1924096 (2003f:13029)

[128] Gilles Villard, *Certification of the QR factor R and of lattice basis reducedness*, ISSAC 2007, ACM, New York, 2007, pp. 361–368. MR MR2402283

[129] P. G. Walsh, *On a very particular class of Ramanujan-Nagell type equations*, Far East J. Math. Sci. (FJMS) **24** (2007), no. 1, 55–58. MR MR2281854 (2007k:11213)

[130] 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.

[131] Paul Zimmermann and Bruce Dodson, *20 years of ECM*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 525–542. MR MR2282947