This contains the References of the Handbook of Elliptic and Hyperelliptic Curve Cryptography, Henri Cohen, Christophe Doche, and Gerhard Frey, Editors, CRC Press 2006.

References

Numbers in the margin specify the pages where citations occur

[AdDe+ 1999] L. M. Adleman, J. DeMarrais, & M.-D. Huang, *A subexponential algorithm for discrete logarithms over hyperelliptic curves of large genus over GF(q)*, Theoret. Comput. Sci. **226** (1999), 7–18. [512, 515, 516]

[AdHu 1992] L. M. Adleman & M.-D. Huang, *Primality testing and Abelian varieties over finite fields*, Lecture Notes in Math., vol. 1512, Springer-Verlag, Berlin, 1992. [601]

[AdHu 1996] ———, *Counting rational points on curves and abelian varieties over finite fields*, Algorithmic Number Theory Symposium – ANTS II, Lecture Notes in Comput. Sci., vol. 1122, Springer-Verlag, Berlin, 1996, 1–16. [422]

[AdHu 2001] ———, *Counting points on curves and abelian varieties over finite fields*, J. Symbolic Comput. **32** (2001), 171–189. [422]

[AdPo+ 1983] L. Adleman, C. Pomerance, & R. Rumely, *On distinguishing prime numbers from composite numbers*, Ann. of Math. **117** (1983), 173–206. [599]

[AgAr+ 2003] D. Agrawal, B. Archambeault, J. R. Rao, & P. Rohatgi, *The EM Side-Channel(s)*, Cryptographic Hardware and Embedded Systems – CHES 2002, Lecture Notes in Comput. Sci., vol. 2523, Springer-Verlag, Berlin, 2003, 29. [682]

[AgKa+ 2002] M. Agrawal, N. Kayal, & N. Saxena, *PRIMES is in P*, preprint, date Aug. 6th, 2002.
`http://www.cse.iitk.ac.in/primality.pdf` [601]

[AkTa 2003] T. Akishita & T. Takagi, *Zero-value point attacks on elliptic curve cryptosystem*, Information Security Conference – ISC 2003, Lecture Notes in Comput. Sci., vol. 2851, Springer-Verlag, Berlin, 2003, 218–233. [682]

[AlGr+ 1994] R. Alford, A. Granville, & C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math. **139** (1994), 703–722. [593]

[AlMa+ 2002] E. Al-Daoud, R. Mahmod, M. Rushdan, & A. Kilicman, *A new addition formula for elliptic curves over GF(2^n)*, IEEE Trans. on Computers **51** N°8 (2002), 972–975. [293]

[AnAn+ 1999] I. Anshel, M. Anshel, & D. Goldfeld, *An algebraic method for public key cryptography*, Math. Res. Lett. **6** (1999), 287–291. [15]

[Ansi X9.62] ANSI X9.62-1999, *Public key cryptography for the financial services industry: The elliptic curve digital signature algorithm (ECDSA)*, 1999. [13, 570]

[Apecs] I. McConnell, *Maple programs*.
`ftp://ftp.math.mcgill.ca/pub/apecs` [267]

[Atk 1988] A. O. L. Atkin, *The number of points on an elliptic curve modulo a prime*, 1988. E-mail on the Number Theory Mailing List. [414, 421]

[Atk 1991] ———, *The number of points on an elliptic curve modulo a prime*, 1991. E-mail on the Number Theory Mailing List. [414, 415]

[AtMo 1993] A. O. L. Atkin & F. Morain, *Elliptic curves and primality proving*, Math. Comp. **61** (1993), 29–68. [458, 597]

[Ava 2002] R. M. Avanzi, *On multi-exponentiation in cryptography*, Tech. Report 154, AREHCC, 2002. http://citeseer.nj.nec.com/545130.html [155]

[Ava 2004a] ———, *Aspects of hyperelliptic curves over large prime fields in software implementations*, Cryptographic Hardware and Embedded Systems – CHES 2004, Lecture Notes in Comput. Sci., vol. 3156, Springer-Verlag, 2004, 148–162. [267, 352, 704]

[Ava 2004b] ———, *Countermeasures against Differential Power Analysis for hyperelliptic curve cryptosystems*, Cryptographic Hardware and Embedded Systems – CHES 2003, Lecture Notes in Comput. Sci., vol. 2779, Springer-Verlag, Berlin, 2004, 366–381. [700–704]

[Ava 2005a] ———, *A note on the signed sliding window integer recoding and a left-to-right analogue*, Selected Areas in Cryptography – SAC 2004, Lecture Notes in Comput. Sci., vol. 3357, Springer-Verlag, Berlin, 2005, 130–143. [153, 154]

[Ava 2005b] ———, *On the complexity of certain multi-exponentiation techniques in cryptography*, J. Cryptology (2005), to appear. [155]

[Ava 2005c] ———, *Side channel attacks on implementations of curve-based cryptographic primitives*, preprint, extended version of AREHCC-report, 2005. http://eprint.iacr.org/2005/017/ [687, 706]

[AvCe 2005] R. M. Avanzi & E. Cesena, *Trace zero varieties over binary fields for cryptography*, preprint, 2005. [383]

[AvCi+ 2004] R. M. Avanzi, M. Ciet, & F. Sica, *Faster scalar multiplication on Koblitz curves combining point halving with the Frobenius endomorphism*, Public Key Cryptography – PKC 2004, Lecture Notes in Comput. Sci., vol. 2947, Springer-Verlag, 2004, 28–40. [301, 365]

[AvHe+ 2004] R. M. Avanzi, C. Heuberger, & H. Prodinger, *Scalar multiplication on Koblitz curves using the Frobenius endomorphism and its combination with point halving: extensions and mathematical analysis*, preprint, 2004. http://finanz.math.tu-graz.ac.at/~cheub/publications/tauext.pdf [359, 365]

[AvLa 2005] R. M. Avanzi & T. Lange, *Cryptographic applications of trace zero varieties*, preprint, 2005. [13, 383, 386]

[AvMi 2004] R. M. Avanzi & P. Mihăilescu, *Generic efficient arithmetic algorithms for PAFFs (Processor Adequate Finite Fields) and related algebraic structures*, Selected Areas in Cryptography – SAC 2003, Lecture Notes in Comput. Sci., vol. 3006, Springer-Verlag, Berlin, 2004, 320–334. [182, 230, 236]

[AvTh 2004] R. M. Avanzi & N. Thériault, *Random walks and filtering strategies for index calculus*, Manuscripts, 2004. [499, 504, 518]

[BaCh+ 2004] H. Bar-El, H. Choukri, D. Naccache, M. Tunstall, & C. Whelan, *The sorcerer's apprentice guide to fault attacks*, Workshop on Fault Diagnosis and Tolerance in Cryptography – FDTC 2004, 2004. http://www.elet.polimi.it/res/FDTC04/Naccache.pdf [684]

[BaDu+ 2004] R. Barua, R. Dutta, & P. Sarkar, *Provably secure authenticated tree based group key agreement protocol using pairing*, preprint, 2004. http://eprint.iacr.org/2004/90/ [576]

[BaEn+ 2002] A. Basiri, A. Enge, J.-C. Faugère, & N. Gürel, *The arithmetic of Jacobian groups of superelliptic cubics*, Tech. report, INRIA – RR-4618, 2002. [352]

[BaEn+ 2004] ———, *Implementing the arithmetic of $C_{3,4}$ curves*, Algorithmic Number Theory Symposium – ANTS VI, Lecture Notes in Comput. Sci., vol. 3076, Springer-Verlag, Berlin, 2004, 87–101. [352]

[BaHa 1998] R. C. Baker & G. Harman, *Shifted primes without large prime factors*, Acta Arith. **83** N°4 (1998), 331–361. [593]

[Bai 2003] H. Baier, *A fast Java implementation of a provably secure pseudo random bit generator based on the elliptic curve discrete logarithm problem*, Tech. Report TI 7/03, University of Darmstadt, 2003. [735]

[BaKi+ 2002] P. S. L. M. Barreto, H. Y. Kim, B. Lynn, & M. Scott, *Efficient algorithms for pairing-based cryptosystems*, Advances in Cryptology – Crypto 2002, Lecture Notes in Comput. Sci., vol. 2442, Springer-Verlag, Berlin, 2002, 354–368. [389, 580, 583, 589]

[BaKo 1998] R. Balasubramanian & N. Koblitz, *The improbability that an elliptic curve has a sub-exponential discrete log problem under the Menezes–Okamoto–Vanstone algorithm*, J. Cryptology **11** (1998), 141–145. [395, 564, 579, 586]

[BaLy+ 2003] P. S. L. M. Barreto, B. Lynn, & M. Scott, *Constructing elliptic curves with prescribed embedding degrees*, Security in Communication Networks – SCN 2002, Lecture Notes in Comput. Sci., vol. 2576, Springer-Verlag, Berlin, 2003, 257–267. [586, 588]

[BaLy+ 2004a] ———, *Efficient implementation of pairing-based cryptosystems*, J. Cryptology **17** (2004), 321–334. [586, 588]

[BaLy+ 2004b] ———, *On the selection of pairing-friendly groups*, Selected Areas in Cryptography – SAC 2003, Lecture Notes in Comput. Sci., vol. 3006, Springer-Verlag, Berlin, 2004, 17–25. [389]

[BaPa 1998] D. V. Bailey & C. Paar, *Optimal extension fields for fast arithmetic in public key algorithms*, Advances in Cryptology – Crypto 1998, Lecture Notes in Comput. Sci., vol. 1462, Springer-Verlag, Berlin, 1998. [229]

[Bar] P. S. L. M. Barreto, *The pairing-based crypto lounge*. `http://planeta.terra.com.br/informatica/paulobarreto/pblounge.html` [389, 573]

[Bar 1987] P. Barrett, *Implementing the Rivest Shamir and Adleman public key encryption algorithm on a standard digital signal processor*, Advances in Cryptology – Crypto 1986, Lecture Notes in Comput. Sci., vol. 263, Springer-Verlag, Berlin, 1987, 311–323. [179]

[BaWa 1980] R. Baillie & S. S. Wagstaff, Jr., *Lucas pseudoprimes*, Math. Comp. **35** (1980), 1391–1417. [596]

[BaZh 2004] J. Baek & Y. Zheng, *Identity-based threshold decryption*, Public Key Cryptography – PKC 2004, Lecture Notes in Comput. Sci., no. 2947, Springer-Verlag, 2004, 262–276. [578]

[BeBe+ 1989] F. Bergeron, J. Berstel, S. Brlek, & C. Duboc, *Addition chains using continued fractions*, J. Algorithms **10** N°3 (1989), 403–412. [161, 166]

[BeBe+ 1994] F. Bergeron, J. Berstel, & S. Brlek, *Efficient computation of addition chains*, J. Théor. Nombres Bordeaux **6** (1994), 21–38. [162]

[Bec 1998] F. Beck, *Integrated circuit failure analysis – a guide to preparation techniques*, John Wiley & Sons, Ltd., 1998. [671]

[BeDo 2002] P. H. T. Beelen & J. M. Doumen, *Pseudorandom sequences from elliptic curves*, Finite fields with applications to coding theory, cryptography and related areas, Springer-Verlag, 2002, 37–52. [732, 733]

[BeGe+ 1991] T. Beth, W. Geiselmann, & F. Meyer, *Finding (good) normal basis in finite fields*, International Symposium on Symbolic and Algebraic Computations – ISSAC 1991, ACM Press, Bonn, 1991, 173–178. [221]

[BeGo+ 1972] M. Beeler, R. W. Gosper, & R. Schroeppel, *HAKMEM*, Memo 239, Massachusetts Institute of Technology Artificial Intelligence Laboratory, February 1972. [484]

[BeKn 2003] R. Bevan & E. W. Knudsen, *Ways to enhance differential power analysis*, Information Security and Cryptology – ICISC 2002, Lecture Notes in Comput. Sci., vol. 2587, Springer-Verlag, 2003, 327–342. [680]

[BeMc+ 1978] E. R. Berlekamp, R. J. McEliece, & H. C. van Tilborg, *On the inherent intractability of certain coding problems*, IEEE Trans. Inform. Theory **24** N°3 (1978), 384–386. [15]

[Ber 1967] E. R. Berlekamp, *Factoring polynomials over finite fields*, Bell System Tech. J. **46** (1967), 1853–1859. [507]

[Ber 1974] P. Berthelot, *Cohomologie cristalline des schémas de caractéristique $p > 0$*, Lecture Notes in Math., vol. 407, Springer-Verlag, Berlin, 1974. [136]

[Ber 1982] E. R. Berlekamp, *Bit-serial Reed–Solomon encoder*, IEEE Trans. Inform. Theory **IT-28** (1982), 869–874. [35]

[Ber 1986] P. Berthelot, *Géométrie rigide et cohomologie des variétés algébriques de caractéristique p*, Mém. Soc. Math. France (N.S.) N°23 (1986), 3, 7–32, Introductions aux cohomologies p-adiques (Luminy, 1984). [136]

[Ber 1998] D. J. Bernstein, *Detecting perfect powers in essentially linear time*, Math. Comp. **67** N°223 (1998), 1253–1283. [198, 199]

[Ber 2001a] ———, *Multidigit multiplication for mathematicians*, 2001. `http://cr.yp.to/papers.html` [174]

[Ber 2001b] P. Berrizbeitia, *Sharpening "primes in P" for a large family of numbers*, preprint, 2001. `http://lanl.arxiv.org/abs/math.NT/0211334` [601]

[Ber 2002] D. J. Bernstein, *Pippenger's exponentiation algorithm*, 2002. preprint. `http://cr.yp.to/papers.html` [146, 155, 159, 166]

[Ber 2004a] ———, *Proving primality in essentially quartic random time*, preprint, 2004. `http://cr.yp.to/papers.html` [601]

[Ber 2004b] ———, *Scaled remainder trees*, preprint, 2004. `http://cr.yp.to/papers.html` [184]

[BigNum] J.-C. Hervé, B. Serpette, & J. Vuillemin, *BigNum: A portable and efficient package for arbitrary-precision arithmetic*, Tech. report, Digital Paris Research Laboratory, 1989, available via e-mail from `librarian@decprl.dec.com`. [169]

[BiJo 2003] O. Billet & M. Joye, *The Jacobi model of an elliptic curve and Side-Channel Analysis*, Applicable Algebra, Algebraic Algorithms and Error-Correcting Codes – AAECC 2003, Lecture Notes in Comput. Sci., vol. 2643, Springer-Verlag, Berlin, 2003, 34–42. [696]

[BiMe+ 2000] I. Biehl, B. Meyer, & V. Müller, *Differential fault attacks on elliptic curve cryptosystems*, Advances in Cryptology – Crypto 2000, Lecture Notes in Comput. Sci., vol. 1880, Springer-Verlag, Berlin, 2000, 131–146. [684, 685, 706–708]

[Bir 1968] B. J. Birch, *How the number of points of an elliptic curve over a fixed prime field varies*, J. London Math. Soc. **43** (1968), 57–60. [605]

[BiSh 1997] E. Biham & A. Shamir, *Differential fault analysis of secret key cryptosystems*, Advances in Cryptology – Crypto 1997, Lecture Notes in Comput. Sci., vol. 1294, Springer-Verlag, 1997, 513–525. [683]

[Bla 2002] G. Blady, *Die Weil-Restriktion elliptischer Kurven in der Kryptographie*, Master's thesis, Universität-Gesamthochschule Essen, 2002. [383]

[BlBl+ 1986] L. Blum, M. Blum, & M. Shub, *A simple unpredictable pseudo-random number generator*, SIAM J. Comput. **15** (1986), 364–383. [721]

[BlFl] D. Bleichenbacher & A. Flammenkamp, *An efficient algorithm for computing shortest addition chains*. `http://www.uni-bielefeld.de/~achim/ac.dvi` [158]

[BlFu+ 1984] I. F. Blake, R. Fuji-Hara, R. C. Mullin, & S. A. Vanstone, *Computing logarithms in finite fields of characteristic two*, SIAM J. Algebraic Discrete Methods **5** N°2 (1984), 276–285. [508]

[BlGa+ 1994a] I. F. Blake, S. Gao, & R. J. Lambert, *Constructive problems for irreducible polynomials over finite fields*, Proceedings of the 1993 Information Theory and Applications Conference, Lecture Notes in Comput. Sci., vol. 793, Springer-Verlag, Berlin, 1994, 1–23. [217]

[BlGa+ 1994b] I. F. Blake, S. Gao, & R. C. Mullin, *Normal and self dual normal bases from factorization of* $cx^{q+1} + dx^q - ax - b$, SIAM J. Discrete Math. **7** N°3 (1994), 499–512. [35]

[BlGa+ 1996] I. F. Blake, S. Gao, & R. J. Lambert, *Construction and distribution problems for irreducible trinomials over finite fields*, Applications of Finite Fields, Oxford University Press, New York, 1996, 19–32. [217]

[BlMu+ 1984] I. F. Blake, R. C. Mullin, & S. A. Vanstone, *Computing logarithms in* $\mathbb{F}_{2^n}$, Advances in Cryptology – Crypto 1984, Lecture Notes in Comput. Sci., vol. 196, Springer-Verlag, 1984, 73–82. [508]

[BlMu+ 2004] I. F. Blake, K. Murty, & G. Xu, *Refinements of Miller's algorithm for computing Weil/Tate pairing*, preprint, 2004.
`http://eprint.iacr.org/2004/065/` [401]

[BlOt+ 2004] J. Blömer, M. Otto, & J.-P. Seifert, *Sign change fault attacks on elliptic curve cryptosystems*, preprint, 2004.
`http://eprint.iacr.org/2004/227/` [708]

[BlRo+ 1998] I. F. Blake, R. M. Roth, & G. Seroussi, *Efficient arithmetic in GF*(2^n) *through palindromic representation*, Tech. Report HPL-98-134, Hewlett–Packard, August 1998.
`http://www.hpl.hp.com/techreports/98/HPL-98-134.pdf` [218, 221]

[BlSe+ 1999] I. F. Blake, G. Seroussi, & N. P. Smart, *Elliptic curves in cryptography*, London Mathematical Society Lecture Note Series, vol. 265, Cambridge University Press, Cambridge, 1999. [197]

[BlSe+ 2005] ———, *Advances in elliptic curve cryptography*, London Mathematical Society Lecture Note Series, vol. 317, Cambridge University Press, Cambridge, 2005. [687]

[BoBo+ 2005] D. Boneh, X. Boyen, & E.-J. Goh, *Hierarchical Identity Based encryption with constant size ciphertext*, preprint, 2005.
`http://eprint.iacr.org/2005/015/` [578]

[BoCo 1990] J. Bos & M. J. Coster, *Addition chain heuristics*, Advances in Cryptology – Crypto 1989, Lecture Notes in Comput. Sci., vol. 435, Springer-Verlag, Berlin, 1990, 400–407. [162, 163]

[BoDe+ 1997] D. Boneh, R. DeMillo, & R. Lipton, *On the importance of checking cryptographic protocols faults*, Advances in Cryptology – Eurocrypt 1997, Lecture Notes in Comput. Sci., vol. 1233, Springer-Verlag, Berlin, 1997, 37–51. [683, 705]

[BoDi+ 2004] I. Bouw, C. Diem, & J. Scholten, *Ordinary elliptic curves of high rank over* $\overline{\mathbb{F}}_p$ *with constant* j*-invariant*, Manuscripta Math. **114** (2004), 487–501. [131]

[BoFr 2001] D. Boneh & M. Franklin, *Identity based encryption from the Weil pairing*, Advances in Cryptology – Crypto 2001, Lecture Notes in Comput. Sci., vol. 2139, Springer-Verlag, Berlin, 2001, 213–229. [395, 576, 583, 589, 590]

[BoFr 2003] ———, *Identity based encryption from the Weil pairing*, SIAM J. Comput. **32** N°3 (2003), 586–615. [576, 578, 583]

[BoGa+ 2004] A. Bostan, P. Gaudry, & É. Schost, *Linear recurrences with polynomial coefficients and application to integer factorization and Cartier–Manin operator*, Proceedings of Fq7, Lecture Notes in Comput. Sci., vol. 2948, Springer-Verlag, Berlin, 2004, 40–58. [412]

[BoGo+ 1994] A. Bossalaers, R. Govaerts, & J. Vandewalle, *Comparison of three modular reduction functions*, Advances in Cryptology – Crypto 1993, Lecture Notes in Comput. Sci., vol. 773, Springer-Verlag, Berlin, 1994, 175–186. [179, 182]

[BoLe 1995] W. Bosma & A. K. Lenstra, *An implementation of the elliptic curve integer factorization method*, Computational algebra and number theory (W. Bosma & A. van der Poorten, eds.), Kluwer Academic Publishers, 1995. [606]

[BoLy+ 2002] D. Boneh, B. Lynn, & H. Shacham, *Short signatures from the Weil pairing*, Advances in Cryptology – Asiacrypt 2001, Lecture Notes in Comput. Sci., vol. 2248, Springer-Verlag, Berlin, 2002, 514–532. [578, 588, 589]

[BoLy+ 2004] ———, *Short signatures from the Weil pairing*, J. Cryptology **17** (2004), 297–319. [578, 588, 589]

[Boo 1951] A. D. Booth, *A signed binary multiplication technique*, Quarterly J. Mech. Appl. Math. **4** (1951), 236–240. [151]

[Bos 2001] W. Bosma, *Signed bits and fast exponentiation*, J. Théor. Nombres Bordeaux **13** (2001), 27–41. [151]

[BoVe 1996] D. Boneh & R. Venkatesan, *Hardness of computing the most significant bits of secret keys in Diffie–Hellman and related schemes*, Advances in Cryptology – Crypto 1996, Lecture Notes in Comput. Sci., vol. 1109, Springer-Verlag, Berlin, 1996, 129–142. [376, 698]

[Bra 1939] A. Brauer, *On addition chains*, Bull. Amer. Math. Soc. **45** (1939), 736–739. [148, 158]

[BrBr 1996] G. Brassand & P. Bratley, *Fundamentals of Algorithmics*, Prentice-Hall, Inc., Englewood Cliffs NJ, 1996, first published as *Algorithmics — Theory & Practice*, 1988. [4]

[BrCl+ 2004] É. Brier, C. Clavier, & F. Olivier, *Correlation power analysis with a leakage model*, Cryptographic Hardware and Embedded Systems – CHES 2004, Lecture Notes in Comput. Sci., vol. 3156, Springer-Verlag, Berlin, 2004, 16–29. [680]

[BrCu+ 1993] H. Brunner, A. Curiger, & M. Hofstetter, *On computing multiplicative inverses in GF*$(2m)$, IEEE Trans. on Computers **42** N°8 (1993), 1010–1015. [223]

[BrDé+ 2004] É. Brier, I. Déchène, & M. Joye, *Unified point addition formulæ for elliptic curve cryptosystems*, Embedded Cryptographic Hardware: Methodologies & Architectures, Nova Science Publishers, 2004. [695]

[Bre 1980] R. P. Brent, *An improved Monte Carlo factorization algorithm*, BIT **20** (1980), 176–184. The paper can be obtained as a series of `.gif` bitmaps from [Brent]. [485]

[Brent] ———, *homepage*, Oxford University Computing Laboratory. `http://web.comlab.ox.ac.uk/oucl/work/richard.brent` [614, 742]

[BrGo+ 1993] E. F. Brickell, D. M. Gordon, K. S. McCurley, & D. B. Wilson, *Fast exponentiation with precomputation*, Advances in Cryptology – Eurocrypt 1992, Lecture Notes in Comput. Sci., vol. 658, Springer-Verlag, Berlin, 1993, 200–207. [165]

[BrJo 2002] É. Brier & M. Joye, *Weierstraß elliptic curves and side channels attacks*, Public Key Cryptography – PKC 2002, Lecture Notes in Comput. Sci., vol. 2274, Springer-Verlag, 2002, 335–345. [286]

[BrJo 2003] ———, *Fast point multiplication on elliptic curves through isogenies*, Applicable Algebra, Algebraic Algorithms and Error-Correcting Codes – AAECC 2003, Lecture Notes in Comput. Sci., vol. 2643, Springer-Verlag, Berlin, 2003, 43–50. [282, 695, 704]

[BrKu 1978] R. P. Brent & H. T. Kung, *Fast algorithms for manipulating formal power series*, J. Assoc. Comput. Mach. **25** N°4 (1978), 581–595. [225]

[BrKu 1983] ———, *Systolic VLSI arrays for linear-time GCD computation*, VLSI 1983, Elsevier Science Publishers B. V., 1983, 145–154. [205, 223]

[BrMy+ 2001] E. Brown, B. T. Myers, & J. A. Solinas, *Elliptic curves with compact parameters*, Combinatorics and Optimization Research Report CORR 2001-68, University of Waterloo, 2001. `http://www.cacr.math.uwaterloo.ca/techreports/2001/corr2001-68.ps` [382, 383]

[BrSt 2004] R. Bröker & P. Stevenhagen, *Elliptic curves with a given number of points*, Algorithmic Number Theory Symposium – ANTS VI, vol. 3076, Springer-Verlag, Berlin, 2004, 117–131. [567]

[Bru 1966] N. G. de Bruijn, *On the number of positive integers* $\leqslant x$ *and free of prime factors* $> y$*, II*, Indag. Math. **38** (1966), 239–247. [506]

[Bru 1994] P. S. Bruckman, *Lucas pseudoprimes are odd*, Fib. Quart. **32** (1994), 155–157. [595]

[BrWe 2004] F. Brezing & A. Weng, *Elliptic curves suitable for pairing based cryptography*, preprint, 2004. http://eprint.iacr.org/2003/143/ [588]

[BrZi 2003] R. P. Brent & P. Zimmermann, *Random number generators with period divisible by a Mersenne prime*, Computational Science and its Applications – ICCSA 2003, vol. 2667, Springer-Verlag, Berlin, 2003, 1–10. [217]

[BuDe 1995] M. Burmester & Y. Desmedt, *A secure and efficient conference key distribution system*, Advances in Cryptology – Eurocrypt 1994, Lecture Notes in Comput. Sci., vol. 950, Springer-Verlag, Berlin, 1995, 275–286. [13, 575]

[BuDe 1997] ———, *Efficient and secure conference key distribution*, Proceedings of the 1996 Workshop on Security Protocols, Lecture Notes in Comput. Sci., vol. 1189, Springer-Verlag, Berlin, 1997, 119–130. [13, 575]

[BuDe 2004] ———, *Identity based key infrastructures*, Proceedings of the IFIP 2004 World Computer Congress, Kluwer Academic Publishers, 2004. [576]

[BuGo+ 1946] A. W. Burks, H. H. Goldstine, & J. von Neumann, *Preliminary discussion of the logical design of an electronic computing instrument*, Tech. Report Princeton, NJ, Institute for Advanced Study, 1946. [632]

[BuJa+ 1997] J. Buchmann, M. J. Jacobson, Jr., & E. Teske, *On some computational problems in finite abelian groups*, Math. Comp. **66** (1997), 1663–1687. [481]

[Bur 1999] D. Bursky, *Flash and EEPROM storage boost* 8*-bit mcu flexibility*, Electronic Design **47** N°5 (1999). [654]

[BuWi 1988] J. Buchmann & H. C. Williams, *A key-exchange system based on imaginary quadratic fields*, J. Cryptology **1** N°2 (1988), 107–118. [549]

[BuZi 1998] C. Burnikel & J. Ziegler, *Fast recursive division*, Tech. Report MPI-I-98-1-022, Max Planck Institut für Informatik, October 1998. http://data.mpi-sb.mpg.de/internet/reports.nsf/ [187]

[ByDu 2004] B. Byramjee & S. Duquesne, *Classification of genus* 2 *curves over* $\mathbb{F}_{2^n}$ *and optimization of their arithmetic*, preprint, 2004. http://eprint.iacr.org/2004/107/ [334]

[CaEr+ 1983] E. R. Canfield, P. Erdős, & C. Pomerance, *On a problem of Oppenheim concerning factorizatio numerorum*, J. Number Theory **17** (1983), 1–28. [506]

[CaFl 1996] J. W. S. Cassels & E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus* 2, London Mathematical Society Lecture Note Series, vol. 230, Cambridge University Press, 1996. [45, 329]

[CaKo+ 2003] J. Cathalo, F. Koeune, & J.-J. Quisquater, *A new type of timing attack: applications to GPS*, Cryptographic Hardware and Embedded Systems – CHES 2003, Lecture Notes in Comput. Sci., vol. 2779, Springer-Verlag, Berlin, 2003, 291–303. [690]

[Cam 1981] P. Camion, *Factorisation des polynômes de* $\mathbb{F}_q[X]$, Tech. Report RR-0093, INRIA, September 1981, in French. [507]

[Cam 1983] ———, *Improving an algorithm for factoring polynomials over a finite field and constructing large irreducible polynomials*, IEEE Trans. Inform. Theory **29** N°3 (1983), 378–385. [507]

[Camb] Cambridge University, TAMPER Lab homepage. http://www.cl.cam.ac.uk/Research/Security/tamper/ [670]

[Can 1987] D. G. Cantor, *Computing in the Jacobian of a hyperelliptic curve*, Math. Comp. **48** (1987), 95–101. [308]

[Car 1932] L. Carlitz, *The arithmetic of a polynomial in a Galois field*, Amer. J. of Math. **54** (1932), 39–50. [37]

[Car 1994] E. F. Carter, *The generation and application of random numbers*, Forth Dimensions **XVI** N°1 & 2 (1994). [720]

[Car 2003] R. Carls, *Generalized AGM sequences and approximation of canonical lifts*, September 2003. [139, 440]

[Cas 1991] J. W. S. Cassels, *Lectures on elliptic curves*, Cambridge University Press, New York, 1991. [270, 275]

[Cav 2000] S. Cavallar, *Strategies in filtering in the Number Field Sieve*, Algorithmic Number Theory Symposium – ANTS IV, Lecture Notes in Comput. Sci., no. 1838, Springer-Verlag, 2000, 209–232. [504, 509]

[CaZa 1981] D. G. Cantor & H. Zassenhaus, *A new algorithm for factoring polynomials over finite fields*, Math. Comp. **36** N°154 (1981), 587–592. [507]

[Ces 2005] E. Cesena, *Varietá a traccia zero su campi binari: Applicazioni crittografiche*, Master's thesis, Universitá degli Studi di Milano, 2005. [383]

[ChCh 1999] C.-Y. Chen & C.-C. Chang, *Fast modular multiplication algorithm for calculating the product AB modulo N*, Inform. Process. Lett. **72** (1999), 77–81. [202]

[ChCi+ 2004] B. Chevallier-Mames, M. Ciet, & M. Joye, *Low-cost solutions for preventing simple Side-Channel Analysis: Side-Channel Atomicity*, IEEE Trans. on Computers **53** (2004), 760–768. [690–692]

[ChCo+ 1991] L. S. Charlap, R. Coley, & D. P. Robbins, *Enumeration of rational points on elliptic curves over finite fields*, Draft, 1991. [422]

[Che 2000] Z. Chen, *Java card technology for smart cards: Architecture and programmers guide*, Addison-Wesley Publishing Company, Reading, MA, 2000. [659]

[Che 2003] Q. Cheng, *Primality proving via one round ECPP and one iteration in AKS*, preprint, 2003. [601]

[ChHw+ 2004] K. Y. Choi, J. Y. Hwang, & D. H. Lee, *Efficient ID-based group key agreement with bilinear maps*, Public Key Cryptography – PKC 2004, Lecture Notes in Comput. Sci., vol. 2947, Springer-Verlag, 2004, 130–144. [576]

[ChJu 2003] J. H. Cheon & B. Jun, *A polynomial time algorithm for the braid Diffie–Hellman conjugacy problem*, Advances in Cryptology – Crypto 2003, Lecture Notes in Comput. Sci., vol. 2729, IACR and Springer-Verlag, 2003, 212–225. [15]

[ChYu 2002] Y. Choie & D. Yun, *Isomorphism classes of hyperelliptic curves of genus 2 over $\mathbb{F}_q$*, Australasian Conference on Information Security and Privacy – ACISP 2002, Lecture Notes in Comput. Sci., vol. 2384, Springer-Verlag, Berlin, 2002, 190–202. [334, 336]

[Cie 2003] M. Ciet, *Aspects of fast and secure arithmetics for elliptic curve cryptography*, PhD. Thesis, Université Catholique de Louvain, 2003. [684]

[CiJo+ 2003] M. Ciet, M. Joye, K. Lauter, & P. L. Montgomery, *Trading inversions for multiplications in elliptic curve cryptography*, preprint, 2003. `http://eprint.iacr.org/2003/257/` [281, 292]

[CiLa+ 2003] M. Ciet, T. Lange, F. Sica, & J.-J. Quisquater, *Improved algorithms for efficient arithmetic on elliptic curves using fast endomorphisms*, Advances in Cryptology – Eurocrypt 2003, Lecture Notes in Comput. Sci., vol. 2656, Springer-Verlag, 2003, 388–400. [365, 381, 382]

[CiQu+ 2002] M. Ciet, J.-J. Quisquater, & F. Sica, *Preventing differential analysis in GLV elliptic curve scalar multiplication*, Cryptographic Hardware and Embedded Systems – CHES 2002, Lecture Notes in Comput. Sci., vol. 2523, Springer-Verlag, Berlin, 2002, 540–550. [713]

[CoFi+ 2001] N. Courtois, M. Finiasz, & N. Sendrier, *How to achieve a McEliece-based digital signature scheme*, Advances in Cryptology – Asiacrypt 2001, Lecture Notes in Comput. Sci., no. 2248, Springer-Verlag, 2001, 157–174. [15]

[Coh] H. Cohen, *Diophantine Equations, p-adic Numbers and L-functions*, Springer-Verlag, to appear. [587]

[Coh 2000] ———, *A course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 2000, fourth edition. [95, 149, 170, 190, 191, 194, 195, 198, 209, 377, 410, 458, 467, 486, 592, 598, 602, 611]

[Coh 2005] ———, *Analysis of the flexible window powering algorithm*, J. Cryptology **18** N°1 (2005), 63–76. [153, 154]

[CoJo+ 1992] M. J. Coster, A. Joux, B. A. LaMacchia, A. M. Odlyzko, C.-P. Schnorr, & J. Stern, *Improved low-density subset sum algorithms*, Comput. Complexity **2** (1992), 111–128. [376]

[CoKo+ 2001] J.-S. Coron, P. Kocher, & D. Naccache, *Statistics and secret leakage*, Financial Cryptography – FC 2000, Lecture Notes in Comput. Sci., vol. 1962, Springer-Verlag, 2001, 157–173. [680]

[Col 1969] G. E. Collins, *Computing multiplicative inverses in GF(p)*, Math. Comp. **23** (1969), 197–200. [205]

[Col 1980] ———, *Lecture notes on arithmetic algorithms*, 1980. University of Wisconsin. [192]

[CoLe 1984] H. Cohen & H. W. Lenstra, Jr., *Primality testing and Jacobi sums*, Math. Comp. **42** (1984), 297–330. [599]

[CoLe 1987] H. Cohen & A. K. Lenstra, *Implementation of a new primality test*, Math. Comp. **48** (1987), 103–121. [599]

[CoMi+ 1997] H. Cohen, A. Miyaji, & T. Ono, *Efficient elliptic curve exponentiation*, Information and Communication Security – ICICS 1997, Lecture Notes in Comput. Sci., vol. 1334, Springer-Verlag, Berlin, 1997, 282–290. [153]

[CoMi+ 1998] ———, *Efficient elliptic curve exponentiation using mixed coordinates*, Advances in Cryptology – Asiacrypt 1998, Lecture Notes in Comput. Sci., vol. 1514, Springer-Verlag, Berlin, 1998, 51–65. [267, 280, 282, 283, 285, 296, 321, 327, 328]

[Con 2005] S. Contini, *FactorWorld: General purpose factoring records*, 2005. `http://www.crypto-world.com/FactorRecords.html` [7]

[Cop 1984] D. Coppersmith, *Fast evaluation of logarithms in fields of characteristic two*, IEEE Trans. Inform. Theory **30** N°4 (1984), 587–594. [215, 586, 589]

[Cop 1993] ———, *Modifications to the Number Field Sieve*, J. Cryptology **6** (1993), 169–180. [613]

[Cor 1999] J.-S. Coron, *Resistance against differential power analysis for elliptic curve cryptosystems*, Cryptographic Hardware and Embedded Systems – CHES 1999, Lecture Notes in Comput. Sci., vol. 1717, Springer-Verlag, Berlin, 1999, 392–302. [678, 680, 682, 699, 700, 711]

[CoSh 1997] D. Coppersmith & A. Shamir, *Lattice attacks on NTRU*, Advances in Cryptology – Eurocrypt 1997, Lecture Notes in Comput. Sci., vol. 1233, Springer-Verlag, Berlin, 1997, 52–61. [15]

[Coster] M. J. Coster, *homepage*. `http://www.coster.demon.nl/` [162]

[Cou 1996] J. M. Couveignes, *Computing l-isogenies with the p-torsion*, Algorithmic Number Theory Symposium – ANTS II, Lecture Notes in Comput. Sci., vol. 1122, Springer-Verlag, 1996, 59–65. [421]

[CR 2003] Cryptography Research, Inc., *Evaluation of VIA C3 Nehemiah Random Number Generator*, Tech. report, 2003. `http://www.cryptography.com/resources/whitepapers/VIA_rng.pdf` [721]

[Cra 1992] R. Crandall, *Method and apparatus for public key exchange in a cryptographic system*, United States Patent 5, 159, 632, Date: Oct. 27th 1992. [182]

[Cro 2003] E. S. Croot III, *Smooth numbers in short intervals*, preprint, 2003. http://www.math.gatech.edu/~ecroot/papers.html [605]

[CrPo 2001] R. Crandall & C. Pomerance, *Prime numbers, a computational perspective*, Springer-Verlag, Berlin, 2001. [170, 177, 182, 207, 614]

[Dav 2000] R. Davies, *Hardware random number generators*, New Zealand Statistics Conference, 2000. [721]

[Del 1974] P. Deligne, *La conjecture de Weil. I*, Inst. Hautes Études Sci. Publ. Math. **43** (1974), 273–307. [135]

[DeLa 2004a] Y. Desmedt & T. Lange, *Pairing based threshold cryptography improving on Libert, Quisquater, Baek, and Zheng*, preprint, 2004. [578]

[DeLa 2004b] ———, *Pairing variants of Burmester–Desmedt I and Katz–Yung*, preprint, 2004. [576]

[DeLa$^+$ 2004] Y. Desmedt, T. Lange, & M. Burmester, *Exponential improvement on Katz–Yung's constant round authenticated group key exchange and tripartite variants*, preprint, 2004. [575, 576]

[Deu 1941] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272. [138, 423]

[DeVe 2002] J. Denef & F. Vercauteren, *An extension of Kedlaya's algorithm to Artin–Schreier curves in characteristic* 2, Algorithmic Number Theory Symposium – ANTS V, Lecture Notes in Comput. Sci., vol. 2369, Springer-Verlag, Berlin, 2002, 308–323. [453]

[DeVe 2005] ———, *An extension of Kedlaya's algorithm to hyperelliptic curves in characteristic* 2, J. Cryptology (2005), to appear. [453]

[Dhe 1998] J.-F. Dhem, *Design of an efficient public key cryptographic library for RISC-based smart cards*, PhD. Thesis, Faculté des sciences appliquées, Laboratoire de microélectronique, Université catholique de Louvain-la-Neuve, Belgique, 1998. http://users.belgacom.net/dhem/these/these_public.pdf [203, 204]

[DhKo$^+$ 2000] J.-F. Dhem, F. Koeune, P.-A. Leroux, P. Mestre, J.-J. Quisquater, & J.-L. Willems, *A practical implementation of the timing attack*, Smart Card Research and Advanced Application – CARDIS 1998, Lecture Notes in Comput. Sci., vol. 1820, Springer-Verlag, 2000, 167–182. [674, 705]

[Die 2001] C. Diem, *A study on theoretical and practical aspects of Weil-restriction of varieties*, PhD. Thesis, Universität Gesamthochschule Essen, 2001. [125, 383, 534, 536, 539]

[Die 2003] ———, *The GHS-attack in odd characteristic*, J. Ramanujan Math. Soc. **18** N°1 (2003), 1–32. [531, 532, 536, 537]

[Die 2004] ———, *On the discrete logarithm problem in elliptic curves over non-prime finite fields*, 2004. preprint. [541, 543, 586]

[Die 2005] ———, *Index calculus in class groups of plane curves of small degree*, preprint, 2005. http://eprint.iacr.org/2005/119/ [535]

[DiHe 1976] W. Diffie & M. E. Hellman, *New directions in cryptography*, IEEE Trans. Inform. Theory **22** N°6 (1976), 644–654. [xxix, 10]

[DiSc 2003] C. Diem & J. Scholten, *Cover Attacks – A report for the AREHCC project*, 2003. http://www.arehcc.com [383, 539, 540, 557]

[Doc 2005] C. Doche, *Redundant trinomials for finite fields of characteristic* 2, Australasian Conference on Information Security and Privacy – ACISP 2005, Lecture Notes in Comput. Sci., vol. 3574, Springer-Verlag, Berlin, 2005, 122–133. [217]

[Doche] ———, *homepage*. http://www.math.u-bordeaux.fr/~cdoche/ [217]

[DoLe 1995] B. Dodson & A. K. Lenstra, *NFS with four large primes: an explosive experiment*, Advances in Cryptology – Crypto 1995, Lecture Notes in Comput. Sci., vol. 963, Springer-Verlag, Berlin, 1995, 372–385. [509, 613]

[DoLe+ 1981] P. Downey, B. Leong, & R. Sethi, *Computing sequences with addition chains*, SIAM J. Comput. **10** (1981), 638–646. [159]

[DoYu 2003] Y. Dodis & M. Yung, *Exposure-resilience for free: Hierarchical ID-based encryption case*, IEEE Security in Storage 2003, 2003, 45–52. [578]

[DuEn+ 2005] R. Dupont, A. Enge, & F. Morain, *Building curves with arbitrary small MOV degree over finite prime fields*, J. Cryptology **18** N°2 (2005), 79–89. [587, 588]

[DuGa+ 1999] I. Duursma, P. Gaudry, & F. Morain, *Speeding up the discrete log computation on curves with automorphisms*, Advances in Cryptology – Asiacrypt 1999, Lecture Notes in Comput. Sci., vol. 1716, Springer-Verlag, Berlin, 1999, 103–121. [491]

[DuKa 1990] S. R. Dussé & B. S. Kaliski, Jr., *A cryptographic library for the Motorola DSP56000*, Advances in Cryptology – Eurocrypt 1990, Lecture Notes in Comput. Sci., vol. 478, Springer-Verlag, Berlin, 1990, 230–244. [181]

[Duq 2004] S. Duquesne, *Montgomery scalar multiplication for genus 2 curves*, Algorithmic Number Theory Symposium – ANTS VI, Lecture Notes in Comput. Sci., vol. 3076, Springer-Verlag, 2004, 153–168. [328, 334, 697]

[DuWa+ 2003] X. Du, Y. Wang, J. Ge, & Y. Wang, *An improved ID-based authenticated group key agreement scheme*, preprint, 2003.
`http://eprint.iacr.org/2003/260/` [576]

[Dwo 1960] B. Dwork, *On the rationality of the zeta function of an algebraic variety*, Amer. J. Math. **82** (1960), 631–648. [135, 138, 422]

[Ecu 1998] P. L'Ecuyer, *Uniform random number generators*, Proceedings of the 1998 Winter Simulation Conference (1998), 97–104. [719]

[Ecu 2001] ———, *Software for uniform random number generation: Distinguishing the good and the bad*, Proceedings of the 2001 Winter Simulation Conference (2001), 95–105. [719]

[Edi 2003] B. Edixhoven, *Point counting after Kedlaya*, EIDMA-Stieltjes graduate course Leiden, 2003. [452]

[EiLa+ 2003] K. Eisenträger, K. Lauter, & P. L. Montgomery, *Fast elliptic curve arithmetic and improved Weil pairing evaluation*, Topics in Cryptology – CT-RSA 2003, Lecture Notes in Comput. Sci., vol. 2612, Springer-Verlag, Berlin, 2003, 343–354. [281, 292]

[ElG 1985] T. ElGamal, *A public key cryptosystem and a signature scheme based on discrete logarithms*, Advances in Cryptology – Crypto 1984, Lecture Notes in Comput. Sci., vol. 196, Springer-Verlag, Berlin, 1985, 10–18. [154]

[Elk 1991] N. D. Elkies, *Explicit isogenies*, Draft, 1991. [414, 419]

[Elk 1996] R. Elkenbracht-Huizing, *An implementation of the Number Field Sieve*, Experiment. Math. **5** N°3 (1996), 231–253. [614]

[ElSh 2002] E. El Mahassni & I. E. Shparlinski, *On the uniformity of distribution of congruential generators over elliptic curves*, Sequences and their Applications – SETA 2001, Discrete Mathematics and Theoretical Computer Science, Springer-Verlag, 2002, 257–264. [732]

[Eng 2002] A. Enge, *Computing discrete logarithms in high-genus hyperelliptic Jacobians in provably subexponential time*, Math. Comp. **71** N°238 (2002), 729–742. [516, 554]

[EnGa 2002] A. Enge & P. Gaudry, *A general framework for subexponential discrete logarithm algorithms*, Acta Arith. **102** N°1 (2002), 83–103. [496, 499, 500, 516, 554]

[EnSt 2002] A. Enge & A. Stein, *Smooth ideals in hyperelliptic function fields*, Math. Comp. **71** (2002), 1219–1230. [516, 554]

[Ent 1998] K. Entacher, *Bad subsequences of well-known linear congruential pseudorandom number generators*, ACM Transactions on Modeling and Computer Simulation **8** N°1 (1998), 61–70. [720, 729]

[Erd 1956] P. Erdős, *On pseudoprimes and Carmichael numbers*, Publ. Math. Debrecen **4** (1956), 201–206. [593]

[EsSa+ 1998] A. E. Escott, J. C. Sager, A. P. L. Selkirk, & D. Tsapakidis, *Attacking elliptic curve cryptosystems using the parallel Pollard rho method*, CryptoBytes (The technical newsletter of RSA laboratories) **4** N°2 (1998), 15–19.
`http://www.rsa.com/rsalabs/pubs/cryptobytes` [490, 491]

[FaJo 2003] J.-C. Faugère & A. Joux, *Algebraic cryptanalysis of Hidden Field Equations (HFE) using Gröbner bases*, Advances in Cryptology – Crypto 2003, Lecture Notes in Comput. Sci., vol. 2729, IACR and Springer-Verlag, 2003, 44–60. [15]

[FaWa 2004] X. Fan & Y. Wang, *Inversion-free arithmetic on genus 3 hyperelliptic curves*, preprint, 2004.
`http://eprint.iacr.org/2004/223/` [348]

[FeGa+ 1999] S. Feisel, J. von zur Gathen, & M. A. Shokrollahi, *Normal bases via general Gauß periods*, Math. Comp. **68** N°225 (1999), 271–290. [35]

[FeMa+ 1996] R. Ferreira, R. Malzahn, P. Marissen, J.-J. Quisquater, & T. Wille, *FAME: A 3rd generation coprocessor for optimising public key cryptosystems in smart card applications*, Smart Card Research and Advanced Application – CARDIS 1996, Stichting Mathematisch Centrum, CWI, Amsterdam, 1996. [204]

[FiGi+ 2002] W. Fischer, C. Giraud, E. W. Knudsen, & J.P. Seifert, *Parallel scalar multiplication on general elliptic curves over $\mathbb{F}_p$ hedged against non-differential side-channel attacks*, preprint, January 2002.
`http://eprint.iacr.org/2002/007/` [288, 697]

[Fips 140-2] FIPS 140-2, *Security requirements for cryptographic modules*, Federal Information Processing Standards Publication 140-2, 1999.
`http://csrc.nist.gov` [720]

[Fips 186-2] FIPS 186-2, *Digital signature standard*, Federal Information Processing Standards Publication 186-2, 2000.
`http://csrc.nist.gov` [183, 215]

[Fips 197] FIPS 197, *Advanced encryption standard (AES)*, Federal Information Processing Standards Publication 197, 2001.
`http://csrc.nist.gov` [2]

[FlOy 2004] S. Flon & R. Oyono, *Fast arithmetic on Jacobians of Picard curves*, Public Key Cryptography – PKC 2004, Lecture Notes in Comput. Sci., vol. 2947, Springer-Verlag, Berlin, 2004, 55–68. [352]

[FlOy+ 2004] S. Flon, R. Oyono, & C. Ritzenthaler, *Fast addition on non-hyperelliptic genus 3 curves*, preprint, 2004.
`http://eprint.iacr.org/2004/118/` [352]

[FlSa 1997] P. Flajolet & B. Salvy, *The SIGSAM challenges: Symbolic asymptotics in practice*, SIGSAM Bulletin **31** N°4 (1997), 36–47. [412]

[Fly] E. V. Flynn, *Formulas for the Kummer surface of a genus 2 curve*.
`ftp://ftp.liv.ac.uk/pub/genus2/kummer` [330]

[Fly 1993] ———, *The group law on the Jacobian of a curve of genus 2*, J. Reine Angew. Math. **439** (1993), 45–69. [329]

[FoGa+ 2000] M. Fouquet, P. Gaudry, & R. Harley, *An extension of Satoh's algorithm and its implementation*, J. Ramanujan Math. Soc. **15** N°4 (2000), 281–318. [432]

[Fre 1998] G. Frey, *How to disguise an elliptic curve*, Talk at Waterloo workshop on the ECDLP, 1998. http://cacr.math.uwaterloo.ca/conferences/1998/ecc98/slides.html [125, 383]

[Fre 2001] ———, *Applications of arithmetical geometry to cryptographic constructions*, Proceedings of the 1998 Finite Fields and Applications Conference, Springer, Berlin, 2001, 128–161. [131, 383]

[FreeLip] A. K. Lenstra & P. Leyland, *Free version of the LIP package*, 1996. [169]

[Fri 2001] H. R. Frium, *The group law on elliptic curves on Hesse form*, Sixth International Conference on Finite Fields and Applications, Springer-Verlag, Berlin, 2001. See also the technical report CORR 2001-09. http://www.cacr.math.uwaterloo.ca/techreports/2001/corr2001-09.ps [275, 276]

[FrKl+ 2004] J. Franke, T. Kleinjung, F. Morain, & T. Wirth, *Proving the primality of very large numbers with fast ECPP*, Algorithmic Number Theory Symposium – ANTS VI, vol. 3076, Springer-Verlag, Berlin, 2004, 194–207. [597]

[FrLa 2003] G. Frey & T. Lange, *Mathematical background of public key cryptography*, Tech. Report 10, IEM Essen, 2003, To appear in Séminaires et Congrès. [548]

[FrMü+ 1999] G. Frey, M. Müller, & H.-G. Rück, *The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems*, IEEE Trans. Inform. Theory **45** N°5 (1999), 1717–1719. [395, 396, 530, 582]

[FrRü 1994] G. Frey & H.-G. Rück, *A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves*, Math. Comp. **62** (1994), 865–874. [336, 530]

[FrTa 1991] A. Fröhlich & M. Taylor, *Algebraic number theory*, Cambridge Studies in Adv. Math., vol. 27, Cambridge Univ. Press, 1991. [19]

[Fujitsu] Fujitsu Limited, *Fram guide book*. http://www.fujitsu.com/global/services/microelectronics/technical/ [655]

[Ful 1969] W. Fulton, *Algebraic curves: An introduction to algebraic geometry*, Benjamin, 1969. [45]

[GaGa+ 2000] S. Gao, J. von zur Gathen, D. Panario, & V. Shoup, *Algorithms for exponentiation in finite fields*, J. Symbolic Comput. **29** (2000), 879–889. [35, 226, 227]

[GaGe 1996] J. von zur Gathen & J. Gerhard, *Arithmetic and factorization of polynomials over $\mathbb{F}_2$*, International Symposium on Symbolic and Algebraic Computation – ISSAC 1996, 1–9. [220]

[GaGe 1999] ———, *Modern computer algebra*, Cambridge University Press, 1999. [3]

[GaHa 2000] P. Gaudry & R. Harley, *Counting points on hyperelliptic curves over finite fields*, Algorithmic Number Theory Symposium – ANTS IV, vol. 1838, Springer-Verlag, Berlin, 2000, 313–332. [422]

[GaHa+ 2002] S. D. Galbraith, K. Harrison, & D. Soldera, *Implementing the Tate pairing*, Algorithmic Number Theory Symposium – ANTS V, Lecture Notes in Comput. Sci., vol. 2369, Springer-Verlag, Berlin, 2002, 324–337. [389, 393, 400, 401, 580, 581, 583, 584]

[GaHe+ 2002a] S. Galbraith, F. Hess, & N. Smart, *Extending the GHS Weil-descent attack*, Advances in Cryptology – Eurocrypt 2002, Lecture Notes in Comput. Sci., vol. 2332, Springer-Verlag, Berlin, 2002, 29–44. [531, 536]

[GaHe+ 2002b] P. Gaudry, F. Hess, & N. P. Smart, *Constructive and destructive facets of Weil descent on elliptic curves*, J. Cryptology **15** N°1 (2002), 19–46. [531, 534]

[Gal 2001a] S. D. Galbraith, *Supersingular curves in cryptography*, Advances in Cryptology – Asiacrypt 2001, Lecture Notes in Comput. Sci., vol. 2248, Springer-Verlag, Berlin, 2001, 495–513. [124, 336, 584, 590]

[Gal 2001b] ———, *Weil descent of Jacobians*, Workshop on Coding and Cryptography, 2001, Electronic Notes in Discrete Mathematics, vol. 6, Elsevier Science Publishers, 2001. [531]

[GaLa+ 2000] R. P. Gallant, R. J. Lambert, & S. A. Vanstone, *Improving the parallelized Pollard lambda search on anomalous binary curves*, Math. Comp. **69** (2000), 1699–1705. [491]

[GaLa+ 2001] ———, *Faster point multiplication on elliptic curves with efficient endomorphisms*, Advances in Cryptology – Crypto 2001, Lecture Notes in Comput. Sci., vol. 2139, Springer-Verlag, Berlin, 2001, 190–200. [376–378]

[GaLe 1992] S. Gao & H. W. Lenstra, Jr., *Optimal normal bases*, Des. Codes Cryptogr. **2** (1992), 315–323. [217]

[GaMc 2000] S. D. Galbraith & J. McKee, *The probability that the number of points on an elliptic curve over a finite field is a prime*, J. London Math. Soc. (2) **62** N°3 (2000), 671–684. [272]

[GaMc+ 2004] S. D. Galbraith, J. McKee, & P. Valenca, *Ordinary abelian varieties having small embedding degree*, preprint, 2004.
`http://eprint.iacr.org/2004/365/` [589]

[GaMo+ 2001] K. Gandolfi, C. Mourtel, & F. Olivier, *Electronic analysis: concrete results*, Cryptographic Hardware and Embedded Systems – CHES 2001, Lecture Notes in Comput. Sci., vol. 2162, Springer-Verlag, Berlin, 2001, 251–261. [682]

[GaNö 2005] J. von zur Gathen & M. Nöcker, *Polynomial and normal bases for finite fields*, J. Cryptology (2005), to appear. [214, 215, 220]

[Gao 2001] S. Gao, *Abelian groups, Gauß periods and normal bases*, Finite Fields Appl. **7** N°1 (2001), 148–164. [35]

[Gar 1959] H. Garner, *The residue number system*, IRE Transactions on Electronic Computers **EC-8** (1959), 140–147. [197]

[GaSc 2004a] P. Gaudry & É. 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-Verlag, 2004, 239–256. [422, 455, 566, 568, 685]

[GaSc 2004b] ———, *A low-memory parallel version of Matsuo, Chao, and Tsujii's algorithm*, Algorithmic Number Theory Symposium – ANTS VI, Lecture Notes in Comput. Sci., vol. 3076, Springer-Verlag, Berlin, 2004, 208–222. [411]

[GaSc 2005] ———, *Modular equations for hyperelliptic curves*, Math. Comp. **74** N°249 (2005), 429–454 (electronic). [422]

[GaSh 1992] J. von zur Gathen & V. Shoup, *Computing Frobenius maps and factoring polynomials (extended abstract)*, ACM Symposium on Theory of Computing, 1992, 97–105. [507]

[GaSm 1999] S. D. Galbraith & N. P. Smart, *A cryptographic application of Weil descent*, Proceedings of the 1999 Cryptography and Coding Conference, Lecture Notes in Comput. Sci., vol. 1746, Springer-Verlag, Berlin, 1999, 191–200. A version is available as HP Technical report HPL-1999-70. [531]

[GaTh+ 2004] P. Gaudry, N. Thériault, & E. Thomé, *A double large prime variation for small genus hyperelliptic index calculus*, preprint, 2004.
`http://eprint.iacr.org/2004/153/` [523, 525, 554]

[Gau 1973] C. F. Gauss, *Werke*, Georg Olms Verlag, 1973, in German. [434]

[Gau 2000a] P. Gaudry, *Algorithmique des courbes hyperelliptiques et applications à la cryptologie*, PhD. Thesis, École polytechnique, 2000.
`http://www.lix.polytechnique.fr/Labo/Pierrick.Gaudry/publis/` [505]

[Gau 2000b] ———, *An algorithm for solving the discrete log problem on hyperelliptic curves*, Advances in Cryptology – Eurocrypt 2000, vol. 1807, Springer-Verlag, Berlin, 2000, 19–34. [505, 517, 554]

[Gau 2002] ———, *A comparison and a combination of SST and AGM algorithms for counting points of elliptic curves in characteristic* 2, Advances in Cryptology – Asiacrypt 2002, Lecture Notes in Comput. Sci., vol. 2501, Springer-Verlag, Berlin, 2002, 311–327. [433, 441]

[Gau 2004] ———, *Index calculus for abelian varieties and the elliptic curve discrete logarithm problem*, preprint, 2004. http://eprint.iacr.org/2004/073/ [541, 586]

[Ger 1983] J. L. Gerver, *Factoring large numbers with a quadratic sieve*, Math. Comp. **41** (1983), 287–294. [508]

[GeSi 2002] C. Gentry & A. Silverberg, *Hierarchical ID-based encryption*, Advances in Cryptology – Asiacrypt 2002, Lecture Notes in Comput. Sci., no. 2501, Springer-Verlag, 2002, 548–566. [578]

[GeSm 2003] K. Geissler & N. P. Smart, *Computing the $M = UU^t$ integer matrix decomposition*, Proceedings of the 2003 Cryptography and Coding Conference, Lecture Notes in Comput. Sci., vol. 2898, Springer-Verlag, 2003, 223–233. [15]

[Gie 2001] E.-G. Giessmann, *Ein schneller Algorithmus zur Punktevervielfachung, der gegen Seitenkanalattacken resistent ist*, talk at *Workshop über Theoretische und praktische Aspekte von Kryptographie mit Elliptischen Kurven*, Berlin, 2001. [689, 711]

[GiTh 2004] C. Giraud & H. Thiebeauld, *A survey on fault attacks*, Smart Card Research and Advanced Application – CARDIS 2004, Kluwer Academic Publishers, 2004, 159–176. [684]

[GMP] Free Software Foundation, *GNU MP library, version 4.1.4*, 2004. http://www.swox.com/gmp/ [169, 176]

[GoBe+ 2000] G. Gong, T. A. Berson, & D. R. Stinson, *Elliptic curve pseudorandom sequence generators*, Selected Areas in Cryptography – SAC 1999, Lecture Notes in Comput. Sci., vol. 1758, Springer-Verlag, Berlin, 2000, 34–48. [732]

[GoCh 2000] J. Goodman & A. Chandrasekaran, *An energy efficient reconfigurable public key cryptography processor architecture*, Cryptographic Hardware and Embedded Systems – CHES 2000, Lecture Notes in Comput. Sci., vol. 1965, Springer-Verlag, Berlin, 2000, 174–191. [644]

[GoHa+ 1996] D. Gollman, Y. Han, & C. Mitchell, *Redundant integer representations and fast exponentiation*, Des. Codes Cryptogr. **7** (1996), 135–151. [160]

[GoLa 2002] G. Gong & C. C. Y. Lam, *Recursive sequences over elliptic curves*, Sequences and their Applications – SETA 2001, Discrete Mathematics and Theoretical Computer Science, Springer-Verlag, 2002, 182–196. [732]

[GoLe+ 1994] R. A. Golliver, A. K. Lenstra, & K. S. McCurley, *Lattice sieving and trial division*, Algorithmic Number Theory Symposium – ANTS I, Lecture Notes in Comput. Sci., vol. 877, Springer-Verlag, Berlin, 1994, 18–27. [614]

[GoMa+ 2005] M. Gonda, K. Matsuo, K. Aoki, J. Chao, & S. Tsuji, *Improvements of addition algorithm on genus 3 hyperelliptic curves and their implementations*, IEICE Trans. Fundamentals **E88-A** N°1 (2005), 89–96. [348]

[GoMc 1993] D. M. Gordon & K. S. McCurley, *Massively parallel computation of discrete logarithms*, Advances in Cryptology – Crypto 1992, Lecture Notes in Comput. Sci., vol. 740, Springer-Verlag, Berlin, 1993, 312–323. [215, 507]

[Gor 1989] J. Gordon, *Fast multiplicative inverse in modular arithmetic*, Proceedings of the 1986 Cryptography and Coding Conference, Oxford University Press, New York, 1989, 269–279. [192]

[Gor 1998] D. M. Gordon, *A survey of fast exponentiation methods*, J. Algorithms **27** N°1 (1998), 129–146. [146]

[Gou 2003] L. Goubin, *A refined power analysis attack on elliptic curve cryptosystems*, Public Key Cryptography – PKC 2003, Lecture Notes in Comput. Sci., vol. 2567, Springer-Verlag, Berlin, 2003, 199–210. [680–682, 700]

[Gra 1998] J. Grantham, *A probable prime test with high confidence*, J. Number Theory **72** (1998), 32–47, MR 2000e:11160. [596]

[Gra 2001] ———, *Frobenius pseudoprimes*, Math. Comp. **70** (2001), 873–891. [595]

[Gra 2004] T. Granlund, *The GNU Multiple Precision arithmetic library, version 4.1.4*, 2004. http://www.swox.com/gmp [176, 178]

[GrHa 1978] P. Griffiths & J. Harris, *Principles of algebraic geometry*, John Wiley & Sons, Ltd., 1978. [88, 90]

[GrHe+ 2004] P. Grabner, C. Heuberger, & H. Prodinger, *Distribution results for low-weight binary representations for pairs of integers*, Theoret. Comput. Sci. **319** (2004), 307–331. [156]

[GrKn+ 1994] R. L. Graham, D. E. Knuth, & O. Patashnik, *Concrete Mathematics, 2nd edition*, Addison-Wesley Publishing Company, Reading, MA, 1994, first edition 1989. [4]

[Gro 1968] A. Grothendieck, *Crystals and the de Rham cohomology of schemes*, Dix Exposés sur la Cohomologie des Schémas, North-Holland, Amsterdam, 1968, 306–358. [136]

[Gro 2001] J. Grossscḧadl, *A bit-serial unified multiplier architecture for finite fields GF(p) and GF(2^m)*, Cryptographic Hardware and Embedded Systems – CHES 2001, Lecture Notes in Comput. Sci., Springer-Verlag, 2001, 202–219. [644]

[GrPo 2002] A. Granville & C. Pomerance, *Two contradictory conjectures concerning Carmichael numbers*, Math. Comp. **71** (2002), 883–908. [593]

[GuKa+ 2004] C. Guyot, K. Kaveh, & V. M. Patankar, *Explicit algorithm for the arithmetic on the hyperelliptic Jacobians of genus* 3, J. Ramanujan Math. Soc. **19** (2004), 119–159. [348]

[GüLa+ 2000] C. Günter, T. Lange, & A. Stein, *Speeding up the arithmetic on Koblitz curves of genus two*, Selected Areas in Cryptography – SAC 2000, Lecture Notes in Comput. Sci., vol. 2012, Springer-Verlag, Berlin, 2000, 106–117. [367, 368, 374]

[GuPa 1997] J. Guajardo & C. Paar, *Efficient algorithms for elliptic curve cryptosystems*, Advances in Cryptology – Crypto 97, Lecture Notes in Comput. Sci., vol. 1294, Springer-Verlag, Berlin, 1997, 342–356. [296]

[Hal 1994] S. Hallgren, *Linear congruential generators over elliptic curves*, Tech. Report CS-94-143, Carnegie Mellon Univ., 1994. [732]

[HaLó+ 2000] D. Hankerson, J. López, & A. J. Menezes, *Software implementation of elliptic curve cryptography over binary fields*, Cryptographic Hardware and Embedded Systems – CHES 2000, Lecture Notes in Comput. Sci., vol. 1965, Springer-Verlag, Berlin, 2000, 1–24. [267, 291]

[HaMe+ 2003] D. Hankerson, A. J. Menezes, & S. A. Vanstone, *Guide to elliptic curve cryptography*, Springer-Verlag, Berlin, 2003. [172, 215, 219, 223, 231, 234, 267, 301, 570, 571]

[HaMo 2002] J. Ha & S. Moon, *Randomized signed-scalar multiplication of ECC to resist power attacks*, Cryptographic Hardware and Embedded Systems – CHES 2002, Lecture Notes in Comput. Sci., vol. 2523, Springer-Verlag, Berlin, 2002, 551–563. [699]

[Han 1959] W. Hansen, *Zum Scholz–Brauerschen Problem*, J. Reine Angew. Math. **202** (1959), 129–136, in German. [158]

[HaQu+ 2002] G. Hanrot, M. Quercia, & P. Zimmermann, *Chronométrages d'algorithmes multiprécision*, janvier 2002. http://www.pauillac.inria.fr/~quercia/papers/mesures2.tar [187, 188]

[HaQu+ 2004] ———, *The middle product algorithm, I*, Appl. Algebra Engrg. Comm. Comput. **14** N°6 (2004), 415–438. [188]

[Har 1960] B. Harris, *Probability distributions related to random mappings*, Ann. of Math. Statistics **31** (1960), 1045–1062. [483]

[Har 1977] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, vol. 52, Springer-Verlag, 1977. [50]

[Har 2000] R. Harley, *Fast arithmetic on genus* 2 *curves*, 2000. See `http://cristal.inria.fr/~harley/hyper` for `C` source code and further explanations. [313]

[Har 2002a] ———, *Algorithmes avancés pour l'arithmétique des courbes (Advanced algorithms for arithmetic on curves)*, PhD. Thesis, Université Paris 7, 2002. [198]

[Har 2002b] ———, *Asymptotically optimal p-adic point-counting*, e-mail to NMBRTHRY list, December 2002. [240, 254, 263, 434]

[Har 2005] G. Harman, *On the number of Carmichael numbers up to x*, Bull. London Math. Soc. (2005), to appear. [593]

[Has 2000] M. A. Hasan, *Power analysis attacks and algorithmic approaches to their countermeasures for Koblitz curve cryptosystems*, Cryptographic Hardware and Embedded Systems – CHES 2000, Lecture Notes in Comput. Sci., vol. 1965, Springer-Verlag, Berlin, 2000, 93–108. [709, 711]

[Hen 1908] K. Hensel, *Theorie der algebraischen Zahlen*, Leipzig, 1908. [180]

[Hen 1961] H. C. Hendrickson, *Fast high-accuracy binary parallel addition*, IRE Trans. Electronic Computers **10** (1961), 465–468. [633]

[Hes 2003] F. Hess, *The GHS attack revisited*, Advances in Cryptology – Eurocrypt 2003, Lecture Notes in Comput. Sci., vol. 2656, Springer-Verlag, Berlin, 2003, 374–387. [531, 536]

[Hes 2004] ———, *A note on the Tate pairing of curves over finite fields*, Arch. Math. (Basel) **82** (2004), 28–32. [122]

[HeSe+ 2001] F. Hess, G. Seroussi, & N. P. Smart, *Two topics in hyperelliptic cryptography*, Selected Areas in Cryptography – SAC 2000, Lecture Notes in Comput. Sci., vol. 2259, Springer-Verlag, Berlin, 2001, 181–189. [311, 313]

[HeSh 2005] F. Hess & I. E. Shparlinski, *On the linear complexity and multidimensional distribution of congruential generators over elliptic curves*, Des. Codes Cryptogr. **35** (2005), 111–117. [732]

[HiMo 2002] Y. Hitchcock & P. Montague, *A new elliptic curve scalar multiplication algorithm to resist simple power analysis*, Australasian Conference on Information Security and Privacy – ACISP 2002, Lecture Notes in Comput. Sci., vol. 2384, Springer-Verlag, Berlin, 2002, 214–225. [689]

[HiTa 2000] A. Higuchi & N. Takagi, *A fast addition algorithm for elliptic curve arithmetic in $GF(2^n)$ using projective coordinates*, Inform. Process. Lett. **76** (2000), 101–103. [293]

[HoHo+ 2003] J. Hoffstein, N. Howgrawe-Graham, J. Pipher, J. H. Silverman, & W. Whyte, *NTRUSign: Digital Signatures Using the NTRU Lattice*, Topics in Cryptology – CT-RSA 2003, Lecture Notes in Comput. Sci., vol. 2612, Springer-Verlag, Berlin, 2003, 122–140. [14]

[Hol 2003] A. J. Holt, *On computing Discrete Logarithms: Large prime(s) variants*, PhD. Thesis, University of Bath, 2003. [508, 509]

[HoOh+ 1996] S.-M. Hong, S.-Y. Oh, & H. Yoon, *New modular multiplication algorithms for fast modular exponentiation*, Advances in Cryptology – Eurocrypt 1996, Lecture Notes in Comput. Sci., vol. 1070, Springer-Verlag, Berlin, 1996, 166–177. [205]

[HoPi+ 1998] J. Hoffstein, J. Pipher, & J. H. Silverman, *NTRU: a ring-based public key cryptosystem*, Algorithmic Number Theory Symposium – ANTS III, Lecture Notes in Comput. Sci., vol. 1423, Springer-Verlag, Berlin, 1998, 267–288. [14]

[HoSm 2001] N. G. Howgrave-Graham & N. P. Smart, *Lattice attacks on digital signature schemes*, Des. Codes Cryptogr. **23** (2001), 283–290. [376, 698]

[How 2001] E. Howe, *Isogeny classes of abelian varieties with no principal polarizations*, Moduli of abelian varieties (Texel Island, 1999), Progr. Math., vol. 195, Birkhäuser, Basel, 2001, 203–216. [540]

[HuIe 1998] M.-D. Huang & D. Ierardi, *Counting points on curves over finite fields*, J. Symbolic Comput. **25** N°1 (1998), 1–21. [422]

[HuPa 1998] X. Huang & V. Y. Pan, *Fast rectangular matrix multiplication and applications*, J. Complexity **14** N°2 (1998), 257–299. [251]

[IbKi 1975] O. H. Ibarra & C. E. Kim, *Fast approximation algorithms for the knapsack and sum of subsets problems*, J. of the ACM **22** (1975), 463–468. [14]

[Igu 1960] J.-I. Igusa, *Arithmetic variety of moduli for genus two*, Ann. of Math. (2) **72** (1960), 612–649. [101]

[IiMa+ 2002] T. Iijima, K. Matsuo, J. Chao, & S. Tsujii, *Construction of Frobenius maps of twists elliptic curves and its application to elliptic scalar multiplication*, Symposium on Cryptography and Information Security – SCIS 2002. [378]

[InTa+ 1982] I. Ingemarsson, D. T. Tang, & C. W. Wong, *A conference key distribution system*, IEEE Trans. Inform. Theory **28** (1982), 714–720. [575]

[Intel 8051] Literature Department Intel Corporation, *Microcontroller handbook*. [721]

[ISO 1995] ISO group, *International Standard ISO 7810 Identification cards — Physical characteristics*, Tech. report, ISO/IEC Copyright Office, 1995. [648]

[ISO 1999a] ———, *Part 1: Physical characteristics, International Standard ISO/IEC 7816: Identification cards — Integrated circuit(s) cards with contacts*, Tech. report, ISO/IEC Copyright Office, 1995-99. [648, 659–661]

[ISO 1999b] ———, *Part 2: Dimensions and location of the contacts, International Standard ISO/IEC 7816: Identification cards — Integrated circuit(s) cards with contacts*, Tech. report, ISO/IEC Copyright Office, 1995-99. [648, 649, 659–661]

[ISO 1999c] ———, *Part 3: Electronic signals and transmission protocols, International Standard ISO/IEC 7816: Identification cards — Integrated circuit(s) cards with contacts*, Tech. report, ISO/IEC Copyright Office, 1995-99. [648, 650, 659–661]

[ISO 1999d] ———, *Part 4: Interindustry commands for interchange, International Standard ISO/IEC 7816: Identification cards — Integrated circuit(s) cards with contacts*, Tech. report, ISO/IEC Copyright Office, 1995-99. [648, 657, 659–661]

[ISO 2000] ———, *International Standard ISO/IEC 14443: Identification cards — Contactless integrated circuit(s) cards — Proximity cards*, Tech. report, ISO/IEC Copyright Office, 2000. [650, 659, 662]

[ISO 2000a] ———, *Part 1: Physical characteristics, International Standard ISO/IEC 14443: Identification cards — Contactless integrated circuit(s) cards - Proximity cards*, Tech. report, ISO/IEC Copyright Office, 2000. [659, 662]

[ISO 2000b] ———, *Part 2: Radio frequency power and signal interface, International Standard ISO/IEC 14443: Identification cards — Contactless integrated circuit(s) cards — Proximity cards*, Tech. report, ISO/IEC Copyright Office, 2000. [659, 662]

[ISO 2000c] ———, *Part 3: Initialization and anticollision, International Standard ISO/IEC 14443: Identification cards — Contactless integrated circuit(s) cards — Proximity cards*, Tech. report, ISO/IEC Copyright Office, 2000. [659, 662]

[ISO 2000d] ———, *Part 4: Transmission protocol, International Standard ISO/IEC 14443: Identification cards — Contactless integrated circuit(s) cards — Proximity cards*, Tech. report, ISO/IEC Copyright Office, 2000. [659, 662]

[ItTs 1988] T. Itoh & S. Tsujii, *A fast algorithm for computing multiplicative inverses in GF(2^m) using normal bases*, Inform. and Comp. **78** N°3 (1988), 171–177. [225, 234]

[ItTs 1989] ———, *Structure of parallel multipliers for a class of fields GF(2^m)*, Inform. and Comp. **83** (1989), 21–40. [217]

[ItYa+ 2002] K. Itoh, J. Yajima, M. Takaneka, & N. Torii, *DPA countermeasures by improving the window method*, Cryptographic Hardware and Embedded Systems – CHES 2002, Lecture Notes in Comput. Sci., vol. 2523, Springer-Verlag, Berlin, 2002, 303–317. [699]

[IzTa 2002a] T. Izu & T. Takagi, *Fast elliptic curve multiplication with SIMD operations*, Information and Communication Security – ICICS 2002, Lecture Notes in Comput. Sci., vol. 2513, Springer-Verlag, 2002, 217–230. [288, 690]

[IzTa 2002b] ———, *A fast parallel elliptic curve multiplication resistant against Side-Channel Attacks*, Public Key Cryptography – PKC 2002, Lecture Notes in Comput. Sci, vol. 2274, Springer-Verlag, Berlin, 2002, 280–296. [697]

[IzTa 2003a] ———, *Efficient computations of the Tate pairing for the large MOV degrees*, Information Security and Cryptology – ICISC 2002, Lecture Notes in Comput. Sci., vol. 2587, Springer-Verlag, Berlin, 2003, 283–297. [401]

[IzTa 2003b] ———, *Exceptional procedure attack on elliptic curve cryptosystems*, Public Key Cryptography – PKC 2003, Lecture Notes in Comput. Sci, vol. 2567, Springer-Verlag, Berlin, 2003, 224–239. [695, 704]

[JaMe+ 2001] M. J. Jacobson, Jr., A. J. Menezes, & A. Stein, *Solving elliptic curve discrete logarithm problems using Weil descent*, J. Ramanujan Math. Soc. **16** (2001), 231–260. [531]

[Jeb 1993a] T. Jebelean, *An algorithm for exact division*, J. Symbolic Comput. **15** N°2 (1993), 169–180. [189, 190]

[Jeb 1993b] ———, *Improving the multiprecision Euclidean algorithm*, Design and Implementation of Symbolic Computation Systems – DISCO 1993, Lecture Notes in Comput. Sci., vol. 722, Springer-Verlag, Berlin, 1993, 45–58. [192]

[JoLe 2002] A. Joux & R. Lercier, *The function field sieve is quite special*, Algorithmic Number Theory Symposium – ANTS V, Lecture Notes in Comput. Sci., vol. 2369, Springer-Verlag, 2002, 431–445. [589]

[JoNg 2003] A. Joux & K. Nguyen, *Separating decision Diffie–Hellman from Diffie–Hellman in cryptographic groups*, J. Cryptology **16** (2003), 239–247. [574]

[JoQu 2001] M. Joye & J.-J. Quisquater, *Hessian elliptic curves and side-channel attacks*, Cryptographic Hardware and Embedded Systems – CHES 2001, Lecture Notes in Comput. Sci., vol. 2162, Springer-Verlag, Berlin, 2001, 402. [275, 276, 676, 696]

[JoQu+ 2002] M. Joye, J.-J. Quisquater, S.-M. Yen, & M. Yung, *Observability analysis – detecting when improved cryptosystems fail*, Topics in Cryptology – CT-RSA 2002, Lecture Notes in Comput. Sci., vol. 2271, Springer-Verlag, Berlin, 2002, 17–29. [708]

[JoTy 2002] M. Joye & C. Tymen, *Protections against differential analysis for elliptic curve cryptography – an algebraic approach*, Cryptographic Hardware and Embedded Systems – CHES 2001, Lecture Notes in Comput. Sci., vol. 2162, Springer-Verlag, Berlin, 2002, 377–390. [680, 700–702, 712]

[Jou 2000] A. Joux, *A one round protocol for tripartite Diffie–Hellman*, Algorithmic Number Theory Symposium – ANTS IV, Lecture Notes in Comput. Sci., vol. 1838, Springer-Verlag, 2000, 385–394. [13, 574, 583, 584]

[Jou 2004] ———, *A one round protocol for tripartite Diffie–Hellman*, J. Cryptology **17** (2004), 263–276. [574, 583]

[Joy 2004] M. Joye, *Smart-card implementation of elliptic curve cryptography and DPA-type attacks*, Smart Card Research and Advanced Application – CARDIS 2004, Kluwer Academic Publishers, 2004, 114–125. [680]

[Joy 2005] ———, *Defenses against side-channel analysis*, Advances in Elliptic Curve Cryptography (I. F. Blake, G. Seroussi, & N. P. Smart, eds.), Cambridge University Press, 2005. [687]

[JoYe 2000] M. Joye & S. M. Yen, *Optimal left-to-right binary signed-digit recoding*, IEEE Trans. on Computers **49** N°7 (2000), 740–748. [151, 152, 401, 676]

[JuMe+ 1990] D. Jungnickel, A. J. Menezes, & S. A. Vanstone, *On the number of self dual basis of GF(q^m) over GF(q)*, Proc. Amer. Math. Soc. **109** (1990), 23–29. [35]

[Jun 1993] D. Jungnickel, *Finite fields*, B.I.-Wissenschaftsverlag, Manheim, Leipzig, Wien, Zürich, 1993. [201, 230]

[JuVa 1996] M. Just & S. Vaudenay, *Authenticated multi-party key agreement*, Advances in Cryptology – Asiacrypt 1996, Lecture Notes in Comput. Sci., vol. 1163, Springer-Verlag, 1996, 36–49. [575]

[KaKi+ 2004] M. Katagi, I. Kitamura, T. Akishita, & T. Takagi, *Novel efficient implementations of hyperelliptic curve cryptosystems using degenerate divisors*, Workshop on Information Security Applications – WISA 2004, Lecture Notes in Comput. Sci., vol. 3325, Springer-Verlag, Berlin, 2004, 347–361. [675, 704]

[Kal 1986] B. S. Kaliski, Jr., *A pseudorandom bit generator based on elliptic logarithms*, Advances in Cryptology – Crypto 1986, Lecture Notes in Comput. Sci., vol. 293, Springer-Verlag, Berlin, 1986, 84–103. [735]

[Kal 1995] ———, *The Montgomery inverse and its applications*, IEEE Trans. on Computers **44** N°8 (1995), 1064–1065. [207, 646]

[KaLu 1982] G. C. Kato & S. Lubkin, *Zeta matrices of elliptic curves*, J. Number Theory **15** N°3 (1982), 318–330. [138, 423]

[Kam 1991] W. Kampkötter, *Explizite Gleichungen für Jacobische Varietäten hyperelliptischer Kurven*, PhD. Thesis, Universität Gesamthochschule Essen, 1991. [104, 422]

[KaMa 1997] A. H. Karp & P. Markstein, *High-precision division and square root*, ACM Trans. Math. Software **23** N°4 (1997), 561–589. [249]

[Kan 1993] G. Kanji, *100 statistical tests*, Sage Publications, 1993. [728]

[KaOf 1962] A. A. Karatsuba & Yu. Ofman, *Multiplication of multiplace numbers on automata*, Dokl. Acad. Nauk SSSR **145** N°2 (1962), 293–294. [176]

[KaOf 1963] ———, *Multiplication of multidigit numbers on automata*, Soviet Physics-Doklady **7** (1963), 595–596. [244]

[Kar 1995] A. A. Karatsuba, *The complexity of computations*, Trudy Mat. Inst. Steklov. *translated in* Proc. Steklov Inst. Math. **211** (1995), 186–202. [176]

[KaYu 2003] J. Katz & M. Yung, *Scalable protocols for authenticated group key exchange*, Advances in Cryptology – Crypto 2003, Lecture Notes in Comput. Sci., vol. 2729, Springer-Verlag, 2003, 110–125. [575]

[Ked 2001] K. S. Kedlaya, *Counting points on hyperelliptic curves using Monsky–Washnitzer cohomology*, J. Ramanujan Math. Soc. **16** (2001), 323–338. [138, 261, 433, 449, 452, 453, 567]

[Kin 2001] B. King, *An improved implementation of elliptic curves over GF(2) when using projective point arithmetic*, Selected Areas in Cryptography – SAC 2001, Lecture Notes in Comput. Sci., vol. 2259, Springer-Verlag, Berlin, 2001, 134–150. [221]

[KiPa+ 1999] A. Kipnis, J. Patarin, & L. Goubin, *Unbalanced oil and vinegar signature schemes*, Advances in Cryptology – Eurocrypt 1999, Lecture Notes in Comput. Sci., vol. 1592, Springer-Verlag, 1999, 206–222. Extended version: [KiPa+ 2003]. [15, 756]

[KiPa+ 2002] H. Y. Kim, J. Y. Park, J. H. Cheon, J. H. Park, J. H. Kim., & S. G. Hahn, *Fast elliptic curve point counting using Gaussian Normal Basis*, Algorithmic Number Theory Symposium – ANTS V, Lecture Notes in Comput. Sci., vol. 2369, Springer-Verlag, 2002, 292–307. [240, 433]

[KiPa+ 2003] A. Kipnis, J. Patarin, & L. Goubin, *Unbalanced oil and vinegar signature schemes*, extended version of [KiPa+ 1999], 2003. `http://citeseer.nj.nec.com/231623.html` [15, 756]

[Kno 1975] J. Knopfmacher, *Abstract analytic number theory*, North–Holland Mathematical Library, vol. 12, North–Holland, Amsterdam, 1975. [496]

[KnPa 1981] D. E. Knuth & C. H. Papadimitriou, *Duality in addition chains*, Bull. Eur. Assoc. Theoret. Comput. Sci. **13** (1981), 2–4. [159]

[Knu 1981] D. E. Knuth, *The art of computer programming. Vol. 2, Seminumerical algorithms*, second ed., Addison-Wesley Publishing Company, Reading, MA, 1981, Addison-Wesley Series in Computer Science and Information Processing. [165]

[Knu 1997] ———, *The art of computer programming. Vol. 2, Seminumerical algorithms*, third ed., Addison-Wesley Publishing Company, Reading, MA, 1997, Addison-Wesley Series in Computer Science and Information Processing. [146, 160, 162, 170, 177, 185, 226, 480, 484, 602, 716, 717, 720]

[Knu 1999] E. W. Knudsen, *Elliptic scalar multiplication using point halving*, Advances in Cryptology – Asiacrypt 1999, Lecture Notes in Comput. Sci., vol. 1716, Springer-Verlag, Berlin, 1999, 135–149. [229, 299, 300]

[KoAc 1998] Ç. K. Koç & T. Acar, *Montgomery multiplication in GF(2^k)*, Des. Codes Cryptogr. **14** N°1 (1998), 57–69. [218, 644]

[KoAc+ 1996] Ç. K. Koç, T. Acar, & B. S. Kaliski, Jr., *Analyzing and comparing Montgomery multiplication algorithms*, IEEE Micro **16** N°3 (1996), 26–33. [205, 639]

[Kob 1989] N. Koblitz, *Hyperelliptic cryptosystems*, J. Cryptology **1** (1989), 139–150. [308, 368]

[Kob 1992] ———, *CM-curves with good cryptographic properties*, Advances in Cryptology – Crypto 1991, Lecture Notes in Comput. Sci., vol. 576, Springer-Verlag, Berlin, 1992, 279–287. [356, 358, 375]

[Kob 1994] ———, *A course in Number Theory and Cryptography*, Graduate Texts in Mathematics, vol. 114, Springer-Verlag, 1994, second edition. [212]

[Koc 1996] P. Kocher, *Timings attacks on implementations of Diffie–Hellman, RSA, DSS and other systems*, Advances in Cryptology – Crypto 1996, Lecture Notes in Comput. Sci., vol. 1109, Springer-Verlag, Berlin, 1996, 104–113. [674, 705]

[Koe 2001] F. Koeune, *Careful design and integration of cryptographic primitives, with contribution to timing attack, padding schemes and random number generators*, PhD. Thesis, Katholieke Universiteit Leuven, 2001.
`http://www.dice.ucl.ac.be/~fkoeune/thesis.ps.gz` [674]

[Koh 2003] D. R. Kohel, *The AGM-$X_0(N)$ Heegner point lifting algorithm and elliptic curve point counting*, Advances in Cryptology Proceedings – Asiacrypt 2003, Lecture Notes in Comput. Sci., vol. 2894, Springer-Verlag, Berlin, 2003, 124–136. [442]

[KoJa+ 1999] P. Kocher, J. Jaffe, & B. Jun, *Differential power analysis*, Advances in Cryptology – Crypto 1999, Lecture Notes in Comput. Sci., vol. 1666, Springer-Verlag, Berlin, 1999, 388–397. [675, 680, 704]

[KöKu 1999] O. Kömmerling & M. G. Kuhn, *Design principles for tamper-resistant smartcard processors*, Proceedings of the 1999 USENIX Workshop on Smartcard Technology, 1999, 9–20. [670]

[KoLe+ 2000] K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. Kang, & C. Park, *New public key cryptosystem using braid groups*, Advances in Cryptology – Crypto 2000, Lecture Notes in Comput. Sci., vol. 1880, Springer-Verlag, Berlin, 2000, 166–183. [15]

[KoMo+ 1999] T. Kobayashi, H. Morita, K. Kobayashi, & F. Hoshino, *Fast elliptic curve algorithm combining Frobenius map and table reference to adapt to higher characteristic*, Theory and Application of Cryptographic Techniques, 1999, 176–189. [237]

[Kor 2002] I. Koren, *Computer arithmetic algorithms*, A. K. Peters, 2002. [618, 638]

[KoSh 2000] D. R. Kohel & I. E. Shparlinski, *Exponential sums and group generators for elliptic curves over finite fields*, Algorithmic Number Theory Symposium – ANTS IV, Lecture Notes in Comput. Sci., vol. 1838, Springer-Verlag, Berlin, 2000, 395–404. [732]

[KoSu 1998] Ç. K. Koç & B. Sunar, *Low-complexity bit-parallel canonical and normal basis multipliers for a class of finite fields*, IEEE Trans. on Computers **47** N°3 (1998), 353–356. [643]

[KoTs 1993] K. Koyama & Y. Tsuruoka, *Speeding up elliptic cryptosystems by using a signed binary window method*, Advances in Cryptology – Crypto 1992, Lecture Notes in Comput. Sci., vol. 740, Springer-Verlag, Berlin, 1993, 345–357. [152, 302]

[KoWe 2005] K. Koike & A. Weng, *Construction of CM-Picard curves*, Math. Comp. **74** N°249 (2005), 499–518. [473]

[Kra 1922] M. Kraitchik, *Théorie des nombres*, vol. 1, Gauthier-Villars, 1922. [495]

[Kra 1924] ———, *Recherches sur la théorie des nombres*, Gauthier-Villars, 1924. [495]

[Kri 1997] U. Krieger, *Anwendung hyperelliptischer Kurven in der Kryptographie*, Master's thesis, Universität Gesamthochschule Essen, 1997. [313]

[KrJe 1996] W. Krandick & T. Jebelean, *Bidirectional exact integer division*, J. Symbolic Comput. **21** N°4–6 (1996), 441–445. [190]

[KuGo+ 2002] J. Kuroki, M. Gonda, K. Matsuo, J. Chao, & S. Tsuji, *Fast genus three hyperelliptic curve cryptosystems*, Symposium on Cryptography and Information Security – SCIS 2002, 503–507.
`http://lab.iisec.ac.jp/~matsuo_lab/pub/pdf/8b-2_1244.pdf` [348]

[Küh 1902] H. Kühne, *Eine Wechselbeziehung zwischen Funktionen mehrerer Unbestimmten, die zu Reciprocitätsgesetzen führt*, J. Reine Angew. Math. **124** (1902), 121–133. [37]

[KuYa 1998] N. Kunihiro & H. Yamamoto, *Window and extended window methods for addition chain and addition-subtraction chain*, IEICE Trans. Fundamentals **E81-A** N°1 (1998), 72–81. [160]

[Lag 1973] J. L. Lagrange, *Œuvres*, Georg Olms Verlag, 1973, in French. [434]

[Lam 1996] R. J. Lambert, *Computational aspects of Discrete Logarithms*, PhD. Thesis, University of Waterloo, Ontario, Canada, 1996. [501]

[LaMi 2004] T. Lange & P. K. Mishra, *SCA resistant parallel explicit formula for addition and doubling of divisors in the Jacobian of hyperelliptic curves of genus* 2, preprint, 2004. [694]

[Lan 1973] S. Lang, *Elliptic functions*, Addison-Wesley Publishing Company, Reading, MA, 1973. [99, 123]

[Lan 1982] ———, *Introduction to algebraic and abelian functions*, 2nd edition ed., Springer-Verlag, Berlin, 1982. [100, 106]

[Lan 2001a] T. Lange, *Efficient arithmetic on hyperelliptic curves*, PhD. Thesis, Universität-Gesamthochschule Essen, 2001. [313, 314, 367, 374, 376, 383, 410, 712]

[Lan 2001b] ———, *Efficient arithmetic on hyperelliptic Koblitz curves*, Tech. Report 2-2001, Universität-Gesamthochschule Essen, 2001. [367]

[Lan 2001c] ———, *Hyperelliptic curves allowing fast arithmetic*, webpage, 2001.
`http://www.ruhr-uni-bochum.de/itsc/tanja/KoblitzC.html` [368, 371]

[Lan 2002a] S. Lang, *Algebra*, Graduate Texts in Mathematics, vol. 211, Springer-Verlag, Berlin, 2002, third edition. [19, 24, 92]

[Lan 2002b] T. Lange, *Efficient arithmetic on genus* 2 *hyperelliptic curves over finite fields via explicit formulae*, preprint, 2002.
`http://eprint.iacr.org/2002/121/` [314]

[Lan 2002c] ———, *Inversion-free arithmetic on genus* 2 *hyperelliptic curves*, preprint, 2002.
`http://eprint.iacr.org/2002/147/` [321]

[Lan 2002d] ———, *Weighted coordinates on genus* 2 *hyperelliptic curves*, preprint, 2002.
`http://eprint.iacr.org/2002/153/` [323, 324, 342]

[Lan 2004a] ———, *Montgomery addition for genus two curves*, Algorithmic Number Theory Symposium – ANTS VI, Lecture Notes in Comput. Sci., vol. 3076, Springer-Verlag, 2004, 309–317. [328, 329, 697]

[Lan 2004b] ———, *A note on López–Dahab coordinates*, preprint, 2004. http://eprint.iacr.org/2004/323/ [294]

[Lan 2004c] ———, *Trace zero subvarieties of genus 2 curves for cryptosystems*, J. Ramanujan Math. Soc. **19** N°1 (2004), 15–33. [131, 383, 385, 386]

[Lan 2005a] ———, *Arithmetic on binary genus 2 curves suitable for small devices*, preprint, 2005. [313, 346, 347]

[Lan 2005b] ———, *Formulae for arithmetic on genus 2 hyperelliptic curves*, Appl. Algebra Engrg. Comm. Comput. **15** N°5 (2005), 295–328. [339, 342, 346]

[Lan 2005c] ———, *Koblitz curve cryptosystems*, Finite Fields Appl. **11** N°2 (2005), 220–229. [367, 370, 376]

[LaRu 1985] H. Lange & W. Ruppert, *Complete systems of addition laws on abelian varieties*, Invent. Math. **79** (1985), 603–610. [56]

[LaSh 2005a] T. Lange & I. E. Shparlinski, *Certain exponential sums and random walks on elliptic curves*, Canad. J. Math. **57** (2005), 338–350. [733, 734]

[LaSh 2005b] ———, *Collisions in fast generation of ideal classes and points on hyperelliptic and elliptic curves*, Appl. Algebra Engrg. Comm. Comput. **15** N°5 (2005), 329–337. [376, 735]

[LaSt 2005] T. Lange & M. Stevens, *Efficient doubling for genus two curves over binary fields*, Selected Areas in Cryptography – SAC 2004, Lecture Notes in Comput. Sci., vol. 3357, Springer-Verlag, Berlin, 2005, 170–181. [334, 336, 337, 352]

[Lau 2004] A. G. B. Lauder, *Deformation theory and the computation of zeta functions*, Proc. London Math. Soc. (3) **88** N°3 (2004), 565–602. [138]

[LaWa 2002a] A. G. B. Lauder & D. Wan, *Computing zeta functions of Artin–Schreier curves over finite fields*, LMS J. Comput. Math. **5** (2002), 34–55 (electronic). [138, 453]

[LaWa 2002b] ———, *Counting points on varieties over finite fields of small characteristic*, Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography, Mathematical Sciences Research Institute Publications, 2002. Proceedings of an MSRI workshop. To appear. [138]

[LaWa 2004] ———, *Computing zeta functions of Artin-Schreier curves over finite fields II*, J. Complexity **20** N°2-3 (2004), 331–349. [138, 453]

[LaWi 2002] T. Lange & A. Winterhof, *Polynomial interpolation of the elliptic curve and XTR discrete logarithm*, Computing and Combinatorics – COCOON 2002, Lecture Notes in Comput. Sci., vol. 2387, Springer-Verlag, Berlin, 2002, 137–143. [554]

[LaWi 2003] ———, *Interpolation of the elliptic curve Diffie–Hellman mapping*, Applicable Algebra, Algebraic Algorithms and Error-Correcting Codes – AAECC 2003, Lecture Notes in Comput. Sci., Springer-Verlag, Berlin, 2003, 51–60. [554]

[Leh 1938] D. H. Lehmer, *Euclid's algorithm for large numbers*, Amer. Math. Monthly **45** (1938), 227–233. [192]

[LeLe 1990] A. K. Lenstra & H. W. Lenstra, Jr., *Algorithms in number theory*, Handbook of theoretical computer science, Volume A, algorithms and complexity (J. van Leeuwen, ed.), Elsevier, Amsterdam, 1990. [479]

[LeLe 1993] A. K. Lenstra & H. W. Lenstra, Jr. (eds.), *The development of the Number Field Sieve*, Lecture Notes in Math., vol. 1554, Springer-Verlag, Berlin, 1993. [508, 614]

[LeLe$^+$ 1982] A. K. Lenstra, H. W. Lenstra, Jr., & L. Lovász, *Factoring polynomials with rational coefficients.*, Math. Ann. **261** (1982), 513–534. [448]

[LeLe$^+$ 1990] A. K. Lenstra, H. W. Lenstra, Jr., M. S. Manasse, & J. M. Pollard, *The Number Field Sieve*, Symposium on the Theory of Computing – STOC 1990, ACM, 1990, 564–572. [614]

[LeLu 2003] R. Lercier & D. Lubicz, *Counting points on elliptic curves over finite fields of small characteristic in quasi quadratic time*, Advances in Cryptology – Eurocrypt 2003, Lecture Notes in Comput. Sci., vol. 2656, Springer-Verlag, 2003, 360–373. [253, 434]

[LeMa 1994] A. K. Lenstra & M. S. Manasse, *Factoring with two large primes*, Math. Comp. **63** (1994), 77–82. [508, 612]

[Len 1987] H. W. Lenstra, Jr., *Factoring integers with elliptic curves*, Ann. of Math. (2) **126** N°3 (1987), 649–673. [604, 605]

[Len 1999] A. K. Lenstra, *Efficient identity based parameter selection for elliptic curve cryptosystems*, Australasian Conference on Information Security and Privacy – ACISP 1999, Lecture Notes in Comput. Sci., vol. 1587, Springer-Verlag, 1999, 294–302. [382]

[Len 2002] ———, *Computational methods in public key cryptology*, 2002. `http://www.win.tue.nl/~klenstra/notes.ps` [205, 610, 612]

[Ler 1996] R. Lercier, *Computing isogenies in GF(2^n)*, Algorithmic Number Theory Symposium – ANTS II, Lecture Notes in Comput. Sci., vol. 1122, Springer-Verlag, 1996, 197–212. [421]

[Ler 1997] ———, *Algorithmique des courbes elliptiques dans les corps finis*, PhD. Thesis, École polytechnique, 1997. `http://www.medicis.polytechnique.fr/~lercier/preprints/these.pdf` [190, 192, 195, 277, 421]

[LeSc 1984] H. W. Lenstra, Jr. & C. P. Schnorr, *A Monte Carlo factoring algorithm with linear storage*, Math. Comp. **43** N°167 (1984), 289–311. [486]

[LeVe 2000] A. K. Lenstra & E. R. Verheul, *The XTR public key system*, Advances in Cryptology – Crypto 2000, Lecture Notes in Comput. Sci., vol. 1880, Springer-Verlag, Berlin, 2000, 1–19. [8]

[LeZi 1978] A. Lempel & J. Ziv, *Compression of individual sequences via variable rate coding*, IEEE Trans. Inform. Theory **IT-24** N°5 (1978), 530–536. [160]

[Lic 1969] S. Lichtenbaum, *Duality theorems for curves over p-adic fields*, Invent. Math. **7** (1969), 120–136. [120]

[LiDe$^+$ 1994] Y. X. Li, R. H. Deng, & X. M. Wang, *On the equivalence of McEliece's and Niederreiter's public-key cryptosystems*, IEEE Trans. Inform. Theory **40** N°1 (1994), 271–273. [15]

[Lidia] Lidia, *A* `C++` *library for computational number theory, version 2.1.3*, 2004. `http://www.informatik.tu-darmstadt.de/TI/LiDIA/` [201]

[LiLe 1994] C. H. Lim & P. J. Lee, *More flexible exponentiation with precomputation*, Advances in Cryptology – Crypto 1994, Lecture Notes in Comput. Sci., vol. 839, Springer-Verlag, Berlin, 1994, 95–107. [166]

[LiLe 1997] ———, *A key recovery attack on discrete log-based schemes using a prime order subgroup*, Advances in Cryptology – Crypto 1997, Lecture Notes in Comput. Sci., vol. 1294, Springer-Verlag, 1997, 249–263. [706]

[LiNi 1997] R. Lidl & H. Niederreiter, *Finite fields*, second ed., Cambridge University Press, 1997. [19, 31, 201]

[LiQu 2003] B. Libert & J.-J. Quisquater, *Efficient revocation and threshold pairing based cryptosystems*, Principles of Distributed Computing – PODC 2003, ACM, 2003, 163–171. [578]

[LiSm 2001] P.-Y. Liardet & N. P. Smart, *Preventing SPA/DPA in ECC systems using the Jacobi form*, Cryptographic Hardware and Embedded Systems – CHES 2001, Lecture Notes in Comput. Sci., vol. 2162, Springer-Verlag, Berlin, 2001, 391. [275, 676, 696, 699]

[LóDa 1998] J. López & R. Dahab, *Improved algorithms for elliptic curve arithmetic in GF(2^n)*, Tech. Report IC-98-39, Relatório Técnico, October 1998. [267, 293, 294]

[LóDa 1999] ———, *Fast multiplication on elliptic curves over GF(2^m) without precomputation*, Cryptographic Hardware and Embedded Systems – CHES 1999), Lecture Notes in Comput. Sci., vol. 1717, Springer-Verlag, Berlin, 1999, 316–327. [267, 298]

[LóDa 2000a] ———, *High-speed software multiplication in* $\mathbb{F}_{2^m}$, Progress in Cryptology – Indocrypt 2000, Lecture Notes in Comput. Sci., vol. 1977, Springer-Verlag, Berlin, 2000, 203–212. [218]

[LóDa 2000b] ———, *An overview of elliptic curve cryptography*, Tech. Report IC-00-10, Relatório Técnico, May 2000. [295]

[Lor 1996] D. Lorenzini, *An invitation to arithmetic geometry*, Graduate studies in mathematics, vol. 9, AMS, 1996. [45]

[Lub 1968] S. Lubkin, *A p-adic proof of Weil's conjectures*, Ann. of Math. (2), 105-194; ibid. (2) **87** (1968), 195–255. [136]

[Lubicz] D. Lubicz, *homepage*, Sur les tests statistiques de générateurs aléatoires. `http://www.math.u-bordeaux.fr/~lubicz/` [715, 725, 726]

[LuSe+ 1964] J. Lubin, J.-P. Serre, & J. Tate, *Elliptic curves and formal groups*, July 1964. Lecture notes prepared in connection with the seminars held at the Summer Institute on Algebraic Geometry, Whitney State, Woods Hole, Massachusets. `http://ma.utexas.edu/users/voloch/lst.html` [138, 423]

[LuSh 2005] F. Luca & I. E. Shparlinski, *On the exponent of the group of points on elliptic curves in extension fields*, Intern. Math. Research Notices **23** (2005), 1391–1409. [586]

[MaCh+ 2001] K. Matsuo, J. Chao, & S. Tsujii, *Fast genus two hyperelliptic curve cryptosysytems*, Tech. Report ISEC2001-23, IEICE, 2001. [314]

[MaCh+ 2002] ———, *An improved baby-step giant-step algorithm for point counting of hyperelliptic curves over finite fields*, Algorithmic Number Theory Symposium – ANTS V, Lecture Notes in Comput. Sci., vol. 2369, Springer-Verlag, 2002, 461–474. [411, 685]

[Mad 2003] M. S. Madsen, *A general framework for p-adic point counting and application to elliptic curves in Legendre form*, preprint, 2003. [442]

[Magma] *The Magma computational algebra system for algebra, number theory and geometry, version 2.11-14*, April 2005. `http://magma.maths.usyd.edu.au/magma/` [201, 267]

[MaIm 1988] T. Matsumoto & H. Imai, *Public quadratic polynomial-tuples for efficient signature verification and message-encryption*, Advances in Cryptology – Eurocrypt 1988, Lecture Notes in Comput. Sci., vol. 330, Springer-Verlag, 1988, 419–445. [15]

[MaMe+ 2002] U. M. Maurer, A. J. Menezes, & E. Teske, *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. [531, 536]

[Man 1961] Ju. I. Manin, *The Hasse-Witt matrix of an algebraic curve*, Izv. Akad. Nauk. SSSR Ser. Mat. **25** (1961), 153–172. [411]

[Man 1962] ———, *On the theory of Abelian varieties over a field of finite characteristic*, Izv. Akad. Nauk. SSSR Ser. Mat. **26** (1962), 281–292. [412]

[MaNa 2002] D. Maisner & E. Nart, *Abelian surfaces over finite fields as Jacobians*, Experiment. Math. **11** (2002), 321–337, with an appendix by E. Howe. [113]

[Mar] G. Marsaglia, *The diehard battery of stringent statistical randomness tests*. `http://random.com.hr/products/random/manual/html/Diehard.html` [729]

[Mas 1969] J. L. Massey, *Shift–register synthesis and BCH decoding*, IEEE Trans. Inform. Theory **IT-15** (1969), 122–127. [501]

[Mau 1992] U. M. Maurer, *A universal statistical test for random number generators*, J. Cryptology **5** N°2 (1992), 89–105. [723, 725]

[MaWo 1998] U. M. Maurer & S. Wolf, *Lower bounds on generic algorithms in groups*, Advances in Cryptology – Eurocrypt 1998, Lecture Notes in Comput. Sci., vol. 1403, Springer-Verlag, Berlin, 1998, 72–84. [478]

[MaWo 1999] ———, *The relationship between breaking the Diffie–Hellman protocol and computing Discrete Logarithms*, SIAM J. Comput. **28** N°5 (1999), 1689–1721. [10]

[McC 1990] K. S. McCurley, *The discrete logarithm problem*, Cryptography and computational number theory (C. Pomerance, ed.), Proc. Symp. Appl. Math., vol. 42, AMS, 1990, 49–74. [495]

[McE 1969] R. J. McEliece, *Factorization of polynomials over finite fields*, Math. Comp. **23** (1969), 861–867. [507]

[McE 1978] ———, *A public-key cryptosystem based on algebraic coding theory*, Deep Space Network Progress Report 42-44, Jet Propulsion Lab., California Institute of Technology (1978), 114–116. [15]

[MeBu+ 2004] G. Meurice de Dormale, P. Bulens, & J.-J. Quisquater, *Efficient modular division implementation: ECC over GF(p) affine coordinates application*, Field-Programmable Logic and Applications – FPL 2004, Lecture Notes in Comput. Sci., vol. 3203, Springer-Verlag, Berlin, 2004, 231–240. [206]

[MeOk+ 1993] A. J. Menezes, T. Okamoto, & S. A. Vanstone, *Reducing elliptic curve logarithms to a finite field*, IEEE Trans. on Inform. Theory **39** (1993), 1639–1646. [395, 530, 580]

[MeOo+ 1996] A. J. Menezes, P. van Oorschot, & S. A. Vanstone, *The Handbook of Applied Cryptography*, CRC Press, Inc., 1996.
http://www.cacr.math.uwaterloo.ca/hac/ [xxix, 5, 10, 12, 13, 146, 170, 180, 183, 197, 720, 728, 729, 731]

[MeQu 2001] A. J. Menezes & M. Qu, *Analysis of the Weil descent attack of Gaudry, Hess and Smart*, Topics in cryptology – CT-RSA 2001, Lecture Notes in Comput. Sci., vol. 2020, Springer-Verlag, Berlin, 2001, 308–318. [531, 534, 535]

[Mes 1991] J.-F. Mestre, *Construction des courbes de genre* 2 *à partir de leurs modules*, Prog. Math., Birkhäuser **94** (1991), 313–334. [102]

[Mes 2000a] T. S. Messerges, *Using second order power analysis to attack DPA resistant software*, Cryptographic Hardware and Embedded Systems – CHES 2000, Lecture Notes in Comput. Sci., vol. 1965, Springer-Verlag, Berlin, 2000, 238–251. [680, 704]

[Mes 2000b] J.-F. Mestre, *Lettre adressée à Gaudry et Harley*, December 2000. In French.
http://www.math.jussieu.fr/~mestre/ [138, 433, 434]

[Mes 2002] ———, *Applications de l'AGM au calcul du nombre de points d'une courbe de genre* 1 *ou* 2 *sur* $\mathbb{F}_{2^n}$. Talk given to the Séminaire de Cryptographie de l'Université de Rennes, March 2002.
http://www.maths.univ-rennes1.fr/crypto/2001-02/Mestre2203.html [434, 442]

[MeSt 1993] W. Meier & O. Staffelbach, *Efficient multiplication on certain nonsupersingular elliptic curves*, Advances in Cryptology – Crypto 1992, Lecture Notes in Comput. Sci., vol. 740, Springer-Verlag, Berlin, 1993, 333–344. [359, 360, 362]

[MeTe+ 2004] A. J. Menezes, E. Teske, & A. Weng, *Weak fields for ECC*, Topics in Cryptology – CT-RSA 2004, Lecture Notes in Comput. Sci., vol. 2964, Springer-Verlag, 2004, 366–386. [536]

[MeVa 1990] A. J. Menezes & S. A. Vanstone, *The implementation of elliptic curve cryptosystems*, Advances in Cryptology – Auscrypt 1990, Lecture Notes in Comput. Sci., vol. 453, Springer-Verlag, Berlin, 1990, 2–13. [356, 581]

[MFA 2004] Microelectronics Failure Analysis Desk Reference Fifth Edition EDFAS (Electronic Device Failure Analysis Society) and ASM International editors, 2004. [670]

[MiAv 2003] P. Mihăilescu & R. M. Avanzi, *Efficient "quasi"-deterministic primality test improving AKS*, preprint, March 2003. [601]

[MiDo+ 2002] Y. Miyamoto, H. Doi, K. Matsuo, J. Chao, & S. Tsuji, *A fast addition algorithm of genus two hyperelliptic curve*, Symposium on Cryptography and Information Security – SCIS 2002, 497–502. In Japanese. [314, 321]

[Mih 1997] P. Mihăilescu, *Optimal Galois field bases which are not normal*, 1997. Presented at the Workshop on Fast Software Encryption in Haifa. [229]

[MIH 2000] ———, *Medium Galois fields, their bases and arithmetic*, 2000. Preprint. [231]
http://grouper.ieee.org/groups/1363/P1363a/contributions/Medium.pdf

[MIL 1986] V. S. MILLER, *Short programs for functions on curves*, 1986. IBM, Thomas J. Watson Research Center. [122, 392]
http://crypto.stanford.edu/miller/

[MIL 2004] ———, *The Weil pairing, and its efficient calculation*, J. Cryptology **17** (2004), 235–261. [122, 392]

[MINA+ 2001] A. MIYAJI, M. NAKABAYASHI, & S. TAKANO, *New explicit conditions of elliptic curve traces for FR-reduction*, IEICE Trans. Fundamentals **E84-A** Nº5 (2001), 1234–1243. [586]

[MIS 2004a] P. K. MISHRA, *Pipelined computation of scalar multiplication in elliptic curve cryptosystems*, Cryptographic Hardware and Embedded Systems – CHES 2004, Lecture Notes in Comput. Sci., vol. 3156, Springer-Verlag, Berlin, 2004, 328–342. [302, 692]

[MIS 2004b] ———, *Scalar multiplication in elliptic curve cryptosystems: Pipelining with precomputations*, preprint, 2004. [694]
http://eprint.iacr.org/2004/191/

[MOBO 1972] R. T. MOENCK & A. B. BORODIN, *Fast modular transforms via division*, Conf. Record, IEEE 13th Annual Symp. on Switching and Automata Theory, IEEE Press, 1972, 90–96. [184]

[MOBR 1975] M. A. MORRISON & J. BRILLHART, *A method of factorization and the factorization of F_7*, Math. Comp. **29** (1975), 183–205. [508, 607]

[MOE 1973] R. T. MOENCK, *Fast computation of GCDs*, Proceedings of the 5th Annual ACM Symposium on the Theory of Computing, 1973, 142–151. [263]

[MOJO] Z. MO & J. P. JONES, *A new primality test using Lucas sequences*, preprint. [595]

[MÖL 2001a] B. MÖLLER, *Securing elliptic curve point multiplication against Side-Channel Attacks*, Information Security Conference – ISC 2001, Lecture Notes in Comput. Sci., vol. 2200, Springer-Verlag, 2001, 324–334. See also [MÖL 2001b]. [690, 699]

[MÖL 2001b] ———, *Securing elliptic curve point multiplication against Side-Channel Attacks*, Tech. report, TU Darmstadt, 2001, Addendum "Efficiency Improvement" added 2001-08-27/2001-08-29. Errata added 2001-12-21. [690, 763]
http://www.informatik.tu-darmstadt.de/TI/Mitarbeiter/moeller/

[MÖL 2003] ———, *Improved techniques for fast exponentiation*, Information Security and Cryptology – ICISC 2002, Lecture Notes in Comput. Sci., vol. 2587, Springer-Verlag, 2003, 298–312. [154]

[MON 1968] P. MONSKY, *Formal cohomology. II: the cohomology sequence of a pair*, Ann. of Math. (2) **88** (1968), 218–238. [136, 139]

[MON 1970] ———, *p-adic analysis and zeta functions*, Lectures in Mathematics, Department of Mathematics Kyoto University, vol. 4, Kinokuniya Book-Store Co. Ltd., Tokyo, 1970. [139]

[MON 1971] ———, *Formal cohomology. III: fixed point theorems*, Ann. of Math. (2) **93** (1971), 315–343. [136, 139]

[MON 1985] P. L. MONTGOMERY, *Modular multiplication without trial division*, Math. Comp. **44** Nº170 (1985), 519–521. [180, 207]

[MON 1987] ———, *Speeding the Pollard and elliptic curve methods of factorization*, Math. Comp. **48** Nº177 (1987), 243–264. [285, 603]

[MON 1994] ———, *A survey of modern integer factorization algorithms*, CWI Quarterly **7** Nº4 (1994), 337–366. [610]

[MON 1995] ———, *A block Lanczos algorithm for finding dependencies over GF(2)*, Advances in Cryptology – Eurocrypt 1995, Lecture Notes in Comput. Sci., no. 921, Springer-Verlag, 1995, 106–120. [503]

[MoOl 1990] F. Morain & J. Olivos, *Speeding up the computations on an elliptic curve using addition-subtraction chains*, Inform. Theory Appl. **24** (1990), 531–543. [151, 153]

[Mor 1995] F. Morain, *Calcul du nombre de points sur une courbe elliptique dans un corps fini : aspects algorithmiques*, J. Théor. Nombres Bordeaux **7** (1995), 255–282. [416, 420]

[Morain] ———, *homepage*. `http://www.lix.polytechnique.fr/~morain/` [601]

[MoWa 1968] P. Monsky & G. Washnitzer, *Formal cohomology. I*, Ann. of Math. (2) **88** (1968), 181–217. [136, 139]

[Mül 1995] V. Müller, *Ein Algorithmus zur Bestimmung der Punktanzahl elliptisher Kurven über endlichen Körpen der Charakteristik größer drei*, PhD. Thesis, Technische Fakultät der Universität des Saarlandes, February 1995. [416, 420]

[Mül 1998] ———, *Fast multiplication on elliptic curves over small fields of characteristic two*, J. Cryptology **11** (1998), 219–234. [367, 370]

[Mum 1966] D. Mumford, *On the equations defining Abelian varieties I-III*, Invent. Math. **1** (1966), 287–354. [56]

[Mum 1974] ———, *Abelian varieties*, Oxford University Press, New York, 1974. [59, 60, 62, 63, 92, 93, 111, 115]

[MuOn+ 1989] R. C. Mullin, I. M. Onyszchuk, S. A. Vanstone, & R. M. Wilson, *Optimal normal bases in GF(p^n)*, Discrete Appl. Math. **22** (1989), 149–161. [217, 221]

[MuSm+ 2004] A. Muzereau, N. P. Smart, & F. Vercauteren, *The equivalence between the DHP and DLP for elliptic curves used in practical applications*, LMS J. Comp. Math. **7** (2004), 50–72. [10]

[MuSt 2004] J. A. Muir & D. R. Stinson, *Minimality and other properties of the width-w nonadjacent form*, Combinatorics and Optimization Research Report CORR 2004-08, University of Waterloo, 2004. `http://www.cacr.math.uwaterloo.ca/techreports/2004/corr2004-08.ps` [153]

[MuSt 2005] ———, *New minimal weight representations for left-to-right window methods*, Topics in cryptology – CT-RSA 2005, Lecture Notes in Comput. Sci., vol. 3376, Springer-Verlag, Berlin, 2005, 366–383. [154]

[Nag 2004] K.-I. Nagao, *Improvement of Thériault algorithm of index calculus for Jacobian of hyperelliptic curves of small genus*, preprint, 2004. `http://eprint.iacr.org/2004/161/` [525]

[NaSt+ 2004] D. Naccache, J. Stern, & N. P. Smart, *Projective coordinates leak*, Advances in Cryptology – Eurocrypt 2004, Lecture Notes in Comput. Sci., vol. 3027, Springer-Verlag, Berlin, 2004, 257–267. [700]

[Nau 1999] N. Naumann, *Weil-Restriktion abelscher Varietäten*, Master's thesis, University Essen, 1999. [383, 386]

[Nec 1994] V. I. Nechaev, *On the complexity of a deterministic algorithm for a discrete logarithm*, Mat. Zametki **55** N°2 (1994), 91–101, 189, Russian. Translation in Math. Notes 55 (1994), no. 1-2, 165–172. [478, 480]

[NeMa 2002] N. Nedjah & L. de Macedo Mourelle, *Minimal addition chain for efficient modular exponentiation using genetic algorithms*, Proceedings of the 2002 Industrial and Engineering, Applications of Artificial Intelligence and Expert Systems Conference, Lecture Notes in Comput. Sci., vol. 2358, Springer-Verlag, Berlin, 2002, 88–98. [163]

[NgSh 2003] P. Q. Nguyen & I. E. Shparlinski, *The insecurity of the elliptic curve digital signature algorithm with partially known nonces*, Des. Codes Cryptogr. **30** (2003), 201–217. [376, 477, 698]

[NgSt 1999] P. Q. Nguyen & J. Stern, *The hardness of the hidden subset sum problem and its cryptographic implications*, Advances in Cryptology – Crypto 1999, Lecture Notes in Comput. Sci., vol. 1666, Springer-Verlag, Berlin, 1999, 31–46. [376]

[Ngu 1998] P. Q. Nguyen, *A Montgomery-like square root for the Number Field Sieve*, Algorithmic Number Theory Symposium – ANTS III, Lecture Notes in Comput. Sci., vol. 1423, Springer-Verlag, Berlin, 1998, 151–168. [614]

[Ngu 2001] K. Nguyen, *Explicit arithmetic of Brauer groups, ray class fields and index calculus*, PhD. Thesis, Universität Gesamthochschule Essen, 2001. [119, 121, 507]

[Nie 1986] H. Niederreiter, *Knapsack-type cryptosystems and algebraic coding theory*, Prob. Contr. Inform. Theory **15** N°2 (1986), 157–166. [15]

[Nie 2003] ———, *Linear complexity and related complexity measures for sequences*, Progress in Cryptology – Indocrypt 2003, Lecture Notes in Comput. Sci., vol. 2904, Springer-Verlag, 2003, 1–17. [730]

[NiSh 1999] H. Niederreiter & I. E. Shparlinski, *On the distribution and lattice structure of nonlinear congruential pseudorandom numbers*, Finite Fields Appl. **5** (1999), 246–253. [731]

[NIST] National Institute of Standard and Technology, *Recommended elliptic curves for federal government use*, 1999.
`http://www.csrc.nist.gov/encryption/` [286]

[Niv 2004] G. Nivash, *Cycle detection using a stack*, Inform. Process. Lett. **90** N°3 (2004), 135–140. [487, 490]

[NiXi 2001] H. Niederreiter & C. Xing, *Rational points on curves over finite fields. Theory and Applications*, London Mathematical Society Lecture Note Series, vol. 285, Cambridge University Press, 2001. [730]

[Nöc 1996] M. Nöcker, *Exponentiation in finite fields: theory and practice*, Diplomarbeit im Fach Informatik, Universität Paderborn, 1996. [224, 226]

[Nöc 2001] ———, *Data structures for parallel exponentiation in finite fields*, PhD. Thesis, Universität Paderborn, 2001. [35]

[NSA] NSA Tempest Series.
`http://cryptome.org/nsa-tempest.htm` [682]

[NTL] V. Shoup, *NTL: A Library for doing Number Theory, version 5.4*, 2005.
`http://www.shoup.net/` [201]

[NTRU] NTRU Cryptolab.
`http://www.ntru.com/cryptolab/index.htm` [14]

[O'Co 2001] L. J. O'Connor, *On string replacement exponentiation*, Des. Codes Cryptogr. **23** (2001), 173–183. [160]

[Odl 1985] A. M. Odlyzko, *Discrete logarithms in finite fields and their cryptographic significance*, Advances in Cryptology – Eurocrypt 1984, Lecture Notes in Comput. Sci., vol. 209, Springer-Verlag, Berlin, 1985, 224–314. [215, 495, 506, 508]

[Odl 1990] ———, *The rise and fall of knapsack cryptosystems*, Cryptology and computational number theory (Boulder, CO, 1989) (Providence, RI), Amer. Math. Soc., 1990, 75–88. [14]

[OkPo 2001] T. Okamoto & D. Pointcheval, *The gap-problems: a new class of problems for the security of cryptographic schemes*, Public Key Cryptography – PKC 2001, Lecture Notes in Comput. Sci., vol. 1992, Springer-Verlag, 2001, 104–118. [578]

[OkSa 2000] K. Okeya & K. Sakurai, *Power analysis breaks elliptic curve cryptosystems even secure against the timing attack*, Progress in Cryptology – Indocrypt 2000, Lecture Notes in Comput. Sci., vol. 1977, Springer-Verlag, Berlin, 2000, 178–190. [699]

[OkSa 2001] ———, *Efficient elliptic curve cryptosystems from a scalar multiplication algorithm with recovery of the y-coordinate on a Montgomery-form elliptic curve*, Cryptographic Hardware and Embedded Systems – CHES 2001, Lecture Notes in Comput. Sci., vol. 2162, Springer-Verlag, Berlin, 2001, 126–141. [286, 298]

[OkSa 2002] ———, *On insecurity of the Side Channel Attack countermeasure using addition-subtraction chains under distinguishability between addition and doubling*, Australasian Conference on Information Security and Privacy – ACISP 2002, Lecture Notes in Comput. Sci., vol. 2384, Springer-Verlag, Berlin, 2002, 420–435. [699]

[OkSa 2003] ———, *A simple power attack on a randomized addition-subtraction chains method for elliptic curve cryptosystems*, IEICE Transactions **E86-A** (2003), 1171–1180. [699]

[OkTa 2003] K. Okeya & T. Takagi, *The width-w NAF method provides small memory and fast elliptic scalar multiplication secure against side channel attacks*, Topics in Cryptology – CT-RSA 2003, Lecture Notes in Comput. Sci., vol. 2612, Springer-Verlag, Berlin, 2003, 328–342. [690]

[Oli 1981] J. Olivos, *On vectorial addition chains*, Journal of algorithms **2** (1981), 13–21. [159]

[Ols 2004] L. D. Olson, *Side-Channel Attacks in ECC: A general technique for varying the parametrization of the elliptic curve*, Cryptographic Hardware and Embedded Systems – CHES 2004, Lecture Notes in Comput. Sci., vol. 3156, Springer-Verlag, Berlin, 2004, 220–229. [696]

[OmMa 1986] J. Omura & J. L. Massey, *Computational method and apparatus for finite field arithmetic*, United States Patent $4,587,627$, Date: May 6th 1986. [35, 220]

[OoTs 1986] F. Oort & S. Tsutomu, *The canonical lifting of an ordinary Jacobian variety need not be a Jacobian variety*, J. Math. Soc. Japan **38** N°3 (1986), 427–437. [139]

[OoWi 1999] P. van Oorschot & M. J. Wiener, *Parallel collision search with cryptanalytic applications*, J. Cryptology **12** (1999), 1–28. [489, 490, 492, 493]

[OsAi 2001] E. Oswald & M. Aigner, *Randomized addition-subtraction chains as a countermeasure against power attacks*, Cryptographic Hardware and Embedded Systems – CHES 2001, Lecture Notes in Comput. Sci., vol. 2162, Springer-Verlag, Berlin, 2001, 39–50. [699]

[PaJe+ 2002a] Y.-H. Park, S. Jeong, C. Kim, & J. Lim, *An alternate decomposition of an integer for faster point multiplication on certain elliptic curves*, Public Key Cryptography – PKC 2002, Lecture Notes in Comput. Sci., vol. 2274, Springer-Verlag, Berlin, 2002, 323–334. [380]

[PaJe+ 2002b] Y.-H. Park, S. Jeong, & J. Lim, *Speeding up point multiplication on hyperelliptic curves with efficiently-computable endomorphisms*, Advances in Cryptology – Eurocrypt 2002, Lecture Notes in Comput. Sci., vol. 2332, Springer-Verlag, 2002, 197–208. [380]

[PaMi 1998] S. K. Park & K. W. Miller, *Random number generators: Good ones are hard to find*, Comm. ACM **31** N°10 (1998), 1192–1201. [720, 721]

[Pap 1994] C. H. Papadimitriou, *Computational complexity*, Addison-Wesley Publishing Company, Reading, MA, 1994. [2]

[Par 2000] B. Parhami, *Computer arithmetic – algorithms and hardware design*, Oxford University Press, New York, 2000. [618]

[Pari] The PARI Group, Bordeaux, *PARI/GP, version 2.1.6*, 2004. `http://pari.math.u-bordeaux.fr/` [267, 467]

[PaSm+ 2004] D. Page, N. P. Smart, & F. Vercauteren, *A comparison of MNT curves and supersingular curves*, preprint, 2004. `http://eprint.iacr.org/2004/165/` [589]

[PaSt 1973] M. S. Paterson & L. J. Stockmeyer, *On the number of nonscalar multiplications necessary to evaluate polynomials*, SIAM J. Comput. **2** (1973), 60–66. [251, 253, 260, 261]

[Pat 1996] J. Patarin, *Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of asymmetric algorithms*, Advances in Cryptology – Eurocrypt 1996, Lecture Notes in Comput. Sci., vol. 1070, Springer-Verlag, Berlin, 1996, 33–48. [15]

[Pel 2002] J. Pelzl, *Fast hyperelliptic curve cryptosystems for embedded processors*, Master's thesis, Ruhr-University of Bochum, 2002. [348]

[PeWo+ 2004] J. Pelzl, T. Wollinger, & C. Paar, *Special hyperelliptic curve cryptosystems of genus two: Efficient arithmetic and fast implementation*, Embedded Cryptographic Hardware: Design and Security, Nova Science Publishers, 2004. [334]

[Pil 1990] J. Pila, *Frobenius maps of abelian varieties and finding roots of unity in finite fields*, Math. Comp. **55** N°192 (1990), 745–763. [137, 422]

[Pinch] R. Pinch, *homepage*. `http://www.chalcedon.demon.co.uk/rgep.html` [593]

[Pip 1979] N. Pippenger, *The minimum number of edges in graphs with prescribed paths*, Math. Systems Theory **12** (1979), 325–346. [166]

[Pip 1980] ———, *On the evaluation of powers and monomials*, SIAM J. Comput. **9** (1980), 230–250. [166]

[PKCS] Public Key Cryptography Standards, *PKCS #1 v1.5: RSA encryption standard*, 1993. `http://www.rsasecurity.com/rsalabs/pkcs` [1]

[PoHe 1978] S. Pohlig & M. Hellmann, *An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance*, IEEE Trans. Inform. Theory **IT-24** (1978), 106–110. [479]

[Pol 1974] J. M. Pollard, *Theorems on factorization and primality testing*, Proceedings of the Cambridge philosophical society **76** (1974), 521–528. [603]

[Pol 1978] ———, *Monte Carlo methods for index computation (mod p)*, Math. Comp. **32** (1978), 918–924. [483, 488, 492]

[Pol 2000] ———, *Kangaroos, monopoly and discrete logarithms*, J. Cryptology **13** (2000), 437–447. [492–494]

[Pom 1983] C. Pomerance, *Analysis and comparison of some integer factoring algorithms*, Computational methods in number theory (H. W. Lenstra, Jr. & R. Tijdeman, eds.), Math. Centre Tracts, no. 154, 155, Mathematisch Centrum, Amsterdam, 1983, 89–139. [609, 610]

[Pom 1984] ———, *Are there counter-examples to the Baillie-PSW primality test?*, Dopo Le Parole aangeboden aan Dr. A.K. Lenstra (H. W. Lenstra, Jr., J. K. Lenstra, & P. van Emde Boas, eds.), Amsterdam, 1984. `http://www.pseudoprime.com/dopo.ps` [596]

[Pom 1985] ———, *The quadratic sieve factoring algorithm*, Advances in Cryptology – Eurocrypt 1984, Lecture Notes in Comput. Sci., vol. 209, Springer-Verlag, Berlin, 1985, 169–182. [609]

[Pom 1990] ———, *Factoring*, Cryptology and Computational Number Theory, Proceedings of Symposia in Applied Mathematics, vol. 42, American Mathematical Society, 1990, 27–47. [594]

[PoSe+ 1980] C. Pomerance, J. L. Selfridge, & S. S. Wagstaff, Jr., *The pseudoprimes to $25 \cdot 10^9$*, Math. Comp. **35** N°151 (1980), 1003–1026. [593, 594, 596]

[PoSm 1992] C. Pomerance & J. W. Smith, *Reduction of huge, sparse matrices over finite fields via created catastrophes*, Experiment. Math. **1** N°2 (1992), 89–94. [504]

[PRIMO] M. Martin, *PRIMO – Primality Proving*. `http://www.ellipsa.net` [596]

[Put 1986] M. van der Put, *The cohomology of Monsky and Washnitzer*, Mém. Soc. Math. France **23** (1986), 33–60. [139]

[QuDe 1990] J.-J. Quisquater & J.-P. Delescaille, *How easy is collision search? Application to DES*, Advances in Cryptology – Eurocrypt 1989, Lecture Notes in Comput. Sci., no. 434, Springer-Verlag, 1990, 429–434. [489]

[Qui 1990] J.-J. Quisquater, *Procédé de codage selon la méthode dite RSA, par un microcontrôleur et dispositifs utilisant ce procédé*, Demande de brevet français. N° de dépôt 90 02274, Date: Feb. 23rd 1990. [187, 203]

[Qui 1992] ———, *Encoding system according to the so-called RSA method, by means of a microcontroller and arrangement implementing this system*, U.S. Patent # 5,166,978, Date: Nov. 24th 1992. [187, 203]

[QuWa+ 1991] J.-J. Quisquater, D. de Waleffe, & J.-P. Bournas, *A chip with fast RSA capability*, Proceedings of Smart Card 2000, Elsevier Science Publishers, Amsterdam, 1991, 199–205. [204]

[Rab 1980] M. O. Rabin, *Probabilistic algorithms in finite fields*, SIAM J. Comput. N°9 (1980), 273–280. [214]

[RaEf 2000] W. Rankl & W. Effing, *Smart card handbook*, 2nd ed., John Wiley & Sons, Ltd., 2000. [653, 660, 661]

[Rei 1962] G. Reitwiesner, *Binary arithmetic*, Adv. Comput. **1** (1962), 231–308. [151]

[Rib 1996] P. Ribenboim, *Lucas pseudoprimes*, p. 129, Springer, 1996. [595]

[RiSh+ 1978] R. L. Rivest, A. Shamir, & L. Adleman, *A method for obtaining digital signatures and public key cryptosystems*, Comm. ACM **21** (1978), 120–126. [7]

[RiSi 1997] R. L. Rivest & R. D. Silverman, *Are "strong" primes needed for RSA?*, preprint, 1997.
`http://eprint.iacr.org/2001/007/` [585, 604]

[Rit] T. Ritter, *Random number machines: A literature survey*.
`http://www.ciphersbyritter.com/RES/RNGMACH.HTM` [718]

[Roo 1995] P. de Rooij, *Efficient exponentiation using precomputation and vector addition chains*, Advances in Cryptology – Eurocrypt 1994, Lecture Notes in Comput. Sci., vol. 950, Springer-Verlag, Berlin, 1995, 389–399. [166]

[RSA] *The new RSA factoring challenge*.
`http://www.rsasecurity.com/rsalabs/node.asp?id=2092` [7]

[Rück 1999] H.-G. Rück, *On the discrete logarithm problem in the divisor class group of curves*, Math. Comp. **68** (1999), 805–806. [77, 529]

[Ruk 2001] A. Rukhin, *Testing randomness: A suite of statistical procedures*, Theory Probab. Appl. **45** N°1 (2001), 111–132. [720]

[RuSo+] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, & S. Vo, *A statistical test suite for random and pseudorandom number generators for cryptographic Applications*, NIST Special Publication 800-22.
`http://csrc.nist.gov/rng/` [729]

[SaAr 1998] T. Satoh & K. Araki, *Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves*, Comm. Math. Univ. Sancti Pauli **47** (1998), 81–92. [529]

[Sah 1975] S. Sahni, *Approximate algorithms for the 0/1 knapsack problem*, J. ACM **22** (1975), 115–124. [14]

[SaKo 2002] E. Savaş & Ç. K. Koç, *Architectures for unified field inversion with applications in elliptic curve cryptography*, International Conference on Electronics, Circuits and Systems – ICECS 2002, vol. 2, 2002, 1155–1158. [646]

[SaSc 1985] J. Sattler & C. P. Schnorr, *Generating random walks in groups*, Ann. Univ. Sci. Budapest. Sect. Comput. **6** (1985), 65–79. [489]

[SaSc+ 2004] H. Sato, D. Schepers, & T. Takagi, *Exact analysis of Montgomery multiplication*, Progress in Cryptology – Indocrypt 2004, vol. 3348, Springer-Verlag, Berlin, 2004, 290–304. [705]

[SaSk+ 2003] T. Satoh, B. Skjernaa, & Y. Taguchi, *Fast computation of canonical lifts of elliptic curves and its application to point counting*, Finite Fields Appl. **9** (2003), 89–101. [258, 262, 433]

[Sat 2000] T. Satoh, *The canonical lift of an ordinary elliptic curve over a finite field and its point counting*, J. Ramanujan Math. Soc. **15** N°4 (2000), 247–270. [138, 423, 428, 429]

[SaTe+ 2000] E. Savaş, A. F. Tenca, & Ç. K. Koç, *A scalable and unified multiplier architecture for finite fields GF(p) and GF(2^m)*, Cryptographic Hardware and Embedded Systems – CHES 2000, Lecture Notes in Comput. Sci., vol. 1965, Springer-Verlag, Berlin, 2000, 277–292. [644]

[SCA Lounge] Ecrypt-Vampire, *The side-channel cryptanalysis lounge*. `http://www.crypto.ruhr-uni-bochum.de/en_sclounge.html` [687]

[ScBa 2004] M. Scott & P. S. L. M. Barreto, *Compressed pairings*, Advances in Cryptology – Crypto 2004, Lecture Notes in Comput. Sci., vol. 3152, Springer-Verlag, Berlin, 2004, 140–156. [401, 586, 588]

[Sch 1927] F. K. Schmidt, *Zur Zahlentheorie in Körpern der Charakteristik p. (Vorläufige Mitteilung.)*, Sitz.-Ber. phys. med. Soz. Erlangen **58/59** (1926/1927), 159–172. [37]

[Sch 1974] B. Schoeneberg, *Elliptic modular functions*, Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen, vol. 203, Springer-Verlag, 1974. [416, 417]

[Sch 1975] A. Schönhage, *A lower bound on the length of addition chains*, Theoret. Comput. Sci. **1** (1975), 1–12. [158]

[Sch 1985] R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Math. Comp. **44** (1985), 483–494. [413]

[Sch 1987] ———, *Nonsingular plane cubic curves*, J. Combin. Theory Ser. A **46** N°2 (1987), 183–211. [605]

[Sch 1995] ———, *Counting points on elliptic curves over finite fields*, J. Théor. Nombres Bordeaux **7** (1995), 219–254. [419, 420]

[Sch 1996] B. Schneier, *Applied cryptography: protocols, algorithms and source code in C*, John Wiley & Sons, Ltd., New York, 1996, second edition. [5]

[Sch 2000a] W. Schindler, *A timing attack against RSA with the Chinese Remainder Theorem*, Cryptographic Hardware and Embedded Systems – CHES 2000, Lecture Notes in Comput. Sci., vol. 1965, Springer-Verlag, Berlin, 2000, 109–124. [705]

[Sch 2000b] O. Schirokauer, *Using number fields to compute logarithms in finite fields*, Math. Comp. **69** N°231 (2000), 1267–1283. [507]

[Sch 2000c] R. Schroeppel, *Elliptic curves: Twice as fast!*, 2000. Presentation at the Crypto 2000 Rump Session. [299]

[Sch 2000d] E. Schulte-Geers, *Collision search in a random mapping: some asymptotic results*, Talk at ECC 2000, the fourth Workshop on Elliptic Curve Cryptography, Essen, Germany, 2000. `http://www.cacr.math.uwaterloo.ca/conferences/2000/ecc2000/` [490]

[ScOr+ 1995] R. Schroeppel, H. Orman, & S. O'Malley, *Fast key exchange with elliptic curve systems*, Tech. report, Department of Computer Science. The University of Arizona, 1995. [214]

[ScSt 1971] A. Schönhage & V. Strassen, *Schnelle Multiplikation grosser Zahlen*, Computing (Arch. Elektron. Rechnen) **7** (1971), 281–292. [244]

[ScWe+ 1996] O. Schirokauer, D. Weber, & Th. F. Denny, *Discrete logarithms: the effectiveness of the index calculus method*, Algorithmic Number Theory Symposium – ANTS II, Lecture Notes in Comput. Sci., vol. 1122, Springer-Verlag, Berlin, 1996, 337–361. [507]

[Sec] Standards for Efficient Cryptography, *Elliptic curve cryptography Ver.0.5*, 1999. `http://www.secg.org/drafts.htm` [286]

[SeLe 1980] G. Seroussi & A. Lempel, *Factorization of symmetric matrices and trace-orthogonal bases in finite fields*, SIAM J. Comput. **9** N°4 (1980), 758–767. [35]

[Sem 1983] I. Semba, *Systematic method for determining the number of multiplications required to compute x^m, where m is a positive integer*, J. Inform. Process. **6** N°1 (1983), 31–33. [166]

[Sem 1998] I. Semaev, *Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p*, Math. Comp. **67** (1998), 353–356. [529]

[Sem 2004] ———, *Summation polynomials and the discrete logarithm problem on elliptic curves*, preprint, 2004.
`http://eprint.iacr.org/2004/031/` [541]

[Ser 1958] J.-P. Serre, *Sur la topologie des variétés algébriques en caractéristique p*, Symposium internacional de topología algebraica – International symposium on algebraic topology (México City 1956), Universidad Nacional Autónoma de México and UNESCO, 1958, 24–53. [76]

[Ser 1970] ———, *Cours d'arithmétique*, Presses Universitaires de France, 1970. [416]

[Ser 1979] ———, *Local Fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, 1979. [39]

[Ser 1998] G. Seroussi, *Table of low-weight binary irreducible polynomials*, Tech. Report HPL-98-135, Hewlett–Packard, August 1998.
`http://www.hpl.hp.com/techreports/98/HPL-98-135.pdf` [214, 217]

[SeSm 1991] A. S. Sedra & K. C. Smith, *Microelectronic circuits*, Oxford University Press, New York, 1991. [653]

[SeSz$^+$ 1982] R. Sedgewick, T. G. Szymanski, & A. C. Yao, *The complexity of finding cycles in periodic functions*, SIAM J. Comput. **11** N°2 (1982), 376–390. [486]

[SGA 4] *Théorie des topos et cohomologie étale des schémas.*, Springer-Verlag, Berlin, 1973, Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4), Dirigé par M. Artin, A. Grothendieck et J. L. Verdier. Lecture Notes in Math., Vol. 269, 270, 305. [136]

[Sha 1971] D. Shanks, *Class number, a theory of factorization and genera*, Proc. Symp. Pure Math. **20** (1971), 415–440. [480]

[Sha 1984] A. Shamir, *Identity-based cryptosystems and signature schemes*, Advances in Cryptology – Crypto 1984, Lecture Notes in Comput. Sci., vol. 196, Springer-Verlag, 1984, 47–53. [576]

[Sha 1999] ———, *Method and apparatus for protecting public key schemes from timing and fault attacks*, United States Patent 5991415, 1999. [708]

[Shi 1967] T. Shioda, *On the graded ring of invariants of binary octavics*, Amer. J. Math. **89** (1967), 1022–1046. [101]

[Shi 1998] G. Shimura, *Abelian Varieties with complex multiplication and modular functions*, revised ed., Princeton University Press, 1998. [107]

[Sho] V. Shoup, *A computational introduction to number theory and algebra*.
`http://www.shoup.net/ntb/ntb-b5.pdf` [201]

[Sho 1990] ———, *On the deterministic complexity of factoring polynomials over finite fields*, Inform. Process. Lett. **33** N°5 (1990), 261–267. [507]

[Sho 1991] ———, *A fast deterministic algorithm for factoring polynomials over finite fields of small characteristic*, International Symposium on Symbolic and Algebraic Computations – ISSAC 1991, ACM Press, Bonn, 1991, 14–21. [507]

[Sho 1994a] ———, *Exponentiation in GF(2^n) using fewer polynomial multiplications*, preprint, 1994. [226]

[Sho 1994b] ———, *Fast construction of irreducible polynomials over finite fields*, J. Symbolic Comput. **17** N°5 (1994), 371–391. [214]

[Sho 1997] ———, *Lower bounds for discrete logarithms and related problems*, Advances in Cryptology – Eurocrypt 1997, Lecture Notes in Comput. Sci., vol. 1233, Springer-Verlag, Berlin, 1997, 256–266. [478]

[Shp 1999] I. E. Shparlinski, *Finite fields: Theory and computation*, Kluwer Academic Publishers, Dordrecht/Boston/London, 1999. [35, 201]

[Shp 2000] ———, *On the Naor–Reingold pseudo-random function from elliptic curves*, Appl. Algebra Engrg. Comm. Comput. **11** (2000), 27–34. [734]

[Shp 2003] ———, *Cryptographic applications of analytic number theory*, Progress in Computer Science and Applied Logic, vol. 22, Birkhäuser Verlag, Basel, 2003, Complexity lower bounds and pseudorandomness. [4]

[ShTa 1961] G. Shimura & Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, Publications of the Mathematical Society of Japan, vol. 6, the Mathematical Society of Japan, Tokyo, 1961. [104, 105]

[SiCi+ 2002] F. Sica, M. Ciet, & J.-J. Quisquater, *Analysis of the Gallant-Lambert-Vanstone method based on efficient endomorphisms: Elliptic and hyperelliptic curves*, Selected Areas in Cryptography – SAC 2002, Lecture Notes in Comput. Sci., vol. 2595, Springer-Verlag, 2002, 21–36. [377, 379, 380]

[Sid 1994] V. M. Sidel'nikov, *A public-key cryptosystem based on Reed–Muller codes*, Discr. Math. Appli. **4** N°3 (1994), 191–207. [15]

[Sil 1986] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, Berlin, 1986. [45, 72, 95, 96, 99, 115, 424, 432]

[Sil 1994] ———, *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, Berlin, 1994. [98, 416]

[Sil 1999] ———, *Fast multiplication in finite fields GF*(2^n), Cryptographic Hardware and Embedded Systems – CHES 1999, Lecture Notes in Comput. Sci., vol. 1717, Springer-Verlag, Berlin, 1999, 122–134. [217]

[Simath] *Simath, a computer algebra system for number theoretic applications*. `http://tnt.math.metro-u.ac.jp/simath` [267]

[SiRu 2004] A. Silverberg & K. Rubin, *Algebraic tori in cryptography*, High Primes and Misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, Fields Institute Communications, AMS, 2004. [56]

[SiSh 2001] J. H. Silverman & I. E. Shparlinski, *On the linear complexity of the Naor–Reingold pseudo-random function from elliptic curves*, Des. Codes Cryptogr. **243** (2001), 279–289. [734, 735]

[SkAn 2003] S. P. Skorobogatov & R. J. Anderson, *Optical fault induction attacks*, Cryptographic Hardware and Embedded Systems – CHES 2002, Lecture Notes in Comput. Sci., vol. 2523, Springer-Verlag, Berlin, 2003, 281–290. [684]

[Skj 2003] B. Skjernaa, *Satoh's algorithm in characteristic* 2, Math. Comp. **72** N°241 (2003), 477–487. [432]

[Sma 1998] N. P. Smart, *The algorithmic resolution of Diophantine equations*, London Mathematical Society Student Texts, vol. 41, Cambridge University Press, 1998. [587]

[Sma 1999a] ———, *The Discrete Logarithm problem on elliptic curves of trace one*, J. Cryptology **12** (1999), 193–196. [529]

[Sma 1999b] ———, *Elliptic curve cryptosystems over small fields of odd characteristic*, J. Cryptology **12** (1999), 141–151. [367, 370]

[Sma 2001] ———, *The Hessian form of an elliptic curve*, Cryptographic Hardware and Embedded Systems – CHES 2001, Lecture Notes in Comput. Sci., vol. 2162, Springer-Verlag, 2001, 118–125. [275, 276, 288, 696]

[Sma 2003] ———, *An analysis of Goubin refined power analysis attack*, Cryptographic Hardware and Embedded Systems – CHES 2003, Lecture Notes in Comput. Sci., vol. 2779, Springer-Verlag, Berlin, 2003, 281–290. [682, 703]

[SmGe 2003] E. Smith & C. Gebotys, *SCA countermeasures for ECC over binary fields on a VLIW DSP core*, Combinatorics and Optimization Research Report CORR 2003-06, University of Waterloo, 2003. http://www.cacr.math.uwaterloo.ca/techreports/2003/cacr2003-06.pdf [709, 711, 712]

[SmSk 1995] P. Smith & C. Skinner, *A public key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms*, Advances in Cryptology – Asiacrypt 1994, Lecture Notes in Comput. Sci., vol. 917, Springer-Verlag, Berlin, 1995, 357–364. [8]

[Sol 1997] J. A. Solinas, *An improved algorithm for arithmetic on a family of elliptic curves*, Advances in Cryptology – Crypto 1997, Lecture Notes in Comput. Sci., vol. 1294, Springer-Verlag, Berlin, 1997, 357–371. [295, 358, 772]

[Sol 1999a] ———, *Generalized Mersenne numbers*, Combinatorics and Optimization Research Report CORR 99-39, University of Waterloo, 1999. http://www.cacr.math.uwaterloo.ca/techreports/1999/corr99-39.ps [183, 393]

[Sol 1999b] ———, *Improved algorithms for arithmetic on anomalous binary curves*, Combinatorics and Optimization Research Report CORR 99-46, University of Waterloo, 1999, updated and corrected version of [Sol 1997]. http://www.cacr.math.uwaterloo.ca/techreports/1999/corr99-46.ps [356, 359, 360, 362, 363]

[Sol 2000] ———, *Efficient arithmetic on Koblitz curves*, Des. Codes Cryptogr. **19** (2000), 195–249. [356, 363, 373]

[Sol 2001] ———, *Low-weight binary representations for pairs of integers*, Combinatorics and Optimization Research Report CORR 2001-41, University of Waterloo, 2001. http://www.cacr.math.uwaterloo.ca/techreports/2001/corr2001-41.ps [155, 156]

[Spa 1994] A. M. Spallek, *Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen*, PhD. Thesis, Universität Gesamthochschule Essen, 1994. [101, 313, 459, 464]

[Sta 2003] M. Stam, *Speeding up subgroup cryptosystems*, PhD. Thesis, Technische Universiteit Eindhoven, 2003. [146, 159, 491]

[Sta 2004] C. Stahlke, *Point compression on Jacobians of hyperelliptic curves over $\mathbb{F}_q$*, preprint, 2004. http://eprint.iacr.org/2004/030/ [311]

[Ste 1910] E. Steinitz, *Algebraische Theorie der Körper*, J. Reine Angew. Math. **137** (1910), 167–309. [27]

[Sti 1979] H. Stichtenoth, *Die Hasse–Witt–Invariante eines Kongruenzfunktionenkörpers*, Arch. Math. (Basel) **33** No 4 (1979/80), 357–360. [135]

[Sti 1993] ———, *Algebraic function fields and codes*, Springer-Verlag, Berlin, 1993. [45, 51, 67, 68, 73, 75, 110–112]

[Sti 1995] D. Stinson, *Cryptography – theory and practice*, CRC Press, Inc., 1995. [5]

[StLe 2003] M. Stam & A. K. Lenstra, *Efficient subgroup exponentiation in quadratic and sixth degree extensions*, Cryptographic Hardware and Embedded Systems – CHES 2002, Lecture Notes in Comput. Sci., vol. 2523, Springer-Verlag, 2003, 317–332. [491]

[StPo+ 2002] J. Stern, D. Pointcheval, J. Malone-Lee, & N. P. Smart, *Flaws in applying proof methodologies to signature schemes*, Advances in Cryptology – Crypto 2002, Lecture Notes in Comput. Sci., vol. 2442, Springer-Verlag, Berlin, 2002, 93–110. [571]

[Str 1964] E. G. Straus, *Addition chains of vectors (problem 5125)*, Amer. Math. Monthly **70** (1964), 806–808. [154]

[StXi 1995] H. Stichtenoth & C. P. Xing, *On the structure of the divisor class group of a class of curves over finite fields*, Arch. Math. (Basel) **65** No 2 (1995), 141–150. [135]

[SuMa+ 2002] H. Sugizaki, K. Matsuo, J. Chao, & S. Tsujii, *An Extension of Harley algorithm addition algorithm for hyperelliptic curves over finite fields of characteristic two*, Tech. Report ISEC2002-9(2002-5), IEICE, 2002. [314, 317]

[Swa 1962] R. G. Swan, *Factorization of polynomials over finite fields*, Pacific J. Math. **12** (1962), 1099–1106. [214]

[Tak 1998] N. Takagi, *A VLSI algorithm for modular division based on the binary GCD algorithm*, IEICE Trans. Fundamentals **E81-A** N°5 (1998), 724–728. [206]

[Tak 2002] M. Takahashi, *Improving Harley algorithms for Jacobians of genus 2 hyperelliptic curves*, Symposium on Cryptography and Information Security – SCIS 2002. In Japanese. [314, 317]

[Tak 2004] K. Takashima, *New families of hyperelliptic curves with efficient Gallant-Lambert-Vanstone method*, Preproceedings ICISC 2004. [381]

[Tat 1958] J. Tate, *WC-groups over $\mathfrak{p}$-adic fields*, Séminaire Bourbaki; 10e année: 1957/1958. Textes des conférences; Exposés 152 à 168; 2e éd. corrigée, Exposé 156, vol. 13, Secrétariat mathématique, Paris, 1958. [118]

[Tat 1966] ———, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144. [112, 448]

[Ter 2000] D. C. Terr, *A modification of Shanks' baby-step giant-step algorithm*, Math. Comp. **69** N°230 (2000), 767–773. [481]

[Tes 1998a] E. Teske, *A space efficient algorithm for group structure computation*, Math. Comp. **67** N°224 (1998), 1637–1663. [486]

[Tes 1998b] ———, *Speeding up Pollard's rho method for computing discrete logarithms*, Algorithmic Number Theory Symposium – ANTS III, Lecture Notes in Comput. Sci., no. 1423, Springer-Verlag, Berlin, 1998, 541–554. [489]

[Tes 2001a] ———, *On random walks for Pollard's rho method*, Math. Comp. **70** N°234 (2001), 809–825. [489]

[Tes 2001b] ———, *Square-root algorithms for the Discrete Logarithm Problem (a survey)*, Public-Key Cryptography and Computational Number Theory, Walter de Gruyter, 2001, 283–301. [477]

[Tes 2003] ———, *Computing discrete logarithms with the parallelized kangaroo method*, Discrete Appl. Math. **130** N°3 (2003), 61–82. [493]

[Thé 2003a] N. Thériault, *Index calculus attack for hyperelliptic curves of small genus*, Advances in Cryptology – Asiacrypt 2003, Lecture Notes in Comput. Sci., vol. 2894, Springer-Verlag, Berlin, 2003, 75–92. [518, 521, 554]

[Thé 2003b] ———, *Weil descent attack for Artin–Schreier curves*, preprint, 2003. `http://www.cacr.math.uwaterloo.ca/~ntheriault/weildescent.pdf` [531, 534–537]

[Thé 2003c] ———, *Weil descent attack for Kummer extensions*, J. Ramanujan Math. Soc. **18** (2003), 281–312. [536]

[ThKe+ 1986] J. J. Thomas, J. M. Keller, & G. N. Larsen, *The calculation of multiplicative inverses over GF(p) efficiently where p is a Mersenne prime*, IEEE Trans. on Computers **35** N°5 (1986), 478–482. [206]

[Tho 2001] E. Thomé, *Computation of Discrete Logarithms in $\mathbb{F}_{2^{607}}$*, Advances in Cryptology – Asiacrypt 2001, Lecture Notes in Comput. Sci., vol. 2248, Springer-Verlag, 2001, 107–124. [501]

[Tho 2003] ———, *Algorithmes de calcul des Logarithmes Discrets dans les corps finis*, PhD. Thesis, École Polytechnique, Palaiseau, September 2003. [501, 507, 508]

[Thu 1999] E. G. Thurber, *Efficient generation of minimal length addition chains*, SIAM J. Comput. **28** N°4 (1999), 1247–1263. [158]

[TrZh+ 1997] J. Tromp, L. Zhang, & Y. Zhao, *Small weight bases for Hamming codes*, Theoret. Comput. Sci. **181** N°2 (1997), 337–345. [217]

[Tun 1968] B. P. Tunstall, *Synthesis of noiseless compression codes*, PhD. Thesis, Georgia Inst. Tech. Atlanta, 1968. [160]

[USB] USB, Universal serial bus specification revision 2.0, April 27 2000. http://www.usb.org [664]

[VÉL 1971] J. VÉLU, *Isogénies entre courbes elliptiques*, C. R. Acad. Sci. Paris Sér. A-B **273** (1971), A238–A241. [415, 427]

[VEPR+ 2001] F. VERCAUTEREN, B. PRENEEL, & J. VANDEWALLE, *A memory efficient version of Satoh's algorithm*, Advances in Cryptology – Eurocrypt 2001, Lecture Notes in Comput. Sci., vol. 2045, Springer-Verlag, Berlin, 2001, 1–13. [433, 437]

[VER 2001] E. VERHEUL, *Evidence that XTR is more secure than supersingular elliptic curves cryptosystems*, Advances in Cryptology – Eurocrypt 2001, Lecture Notes in Comput. Sci., vol. 2045, Springer-Verlag, Berlin, 2001, 195–210. [582]

[VER 2004] ———, *Evidence that XTR is more secure than supersingular elliptic curves cryptosystems*, J. Cryptology **17** (2004), 277–296. [582]

[WAL 2001] C. D. WALTER, *MIST: An efficient, randomized exponentiation algorithm for resisting power analysis*, Topics in Cryptology – CT-RSA 2002, Lecture Notes in Comput. Sci., vol. 2271, Springer-Verlag, Berlin, 2001, 53–66. [699]

[WAL 2002a] ———, *Breaking the Liardet–Smart randomized exponentiation algorithm*, Smart Card Research and Advanced Applications – CARDIS 2002, Usenix Association, 2002, 59–68. [699]

[WAL 2002b] ———, *Some security aspects of the MIST randomized exponentiation algorithm*, Cryptographic Hardware and Embedded Systems – CHES 2002, Lecture Notes in Comput. Sci., vol. 2523, Springer-Verlag, Berlin, 2002, 276–290. [699]

[WAL 2003] ———, *Seeing through MIST given a small fraction of an RSA private key*, Topics in Cryptology – CT-RSA 2003, Lecture Notes in Comput. Sci., vol. 2612, Springer-Verlag, Berlin, 2003, 391–402. [699]

[WAL 2004] ———, *Security constraints on the Oswald–Aigner exponentiation algorithm*, Topics in Cryptology – CT-RSA 2004, Lecture Notes in Comput. Sci., vol. 2964, Springer-Verlag, Berlin, 2004, 208–221. [699]

[WAT 1969] W. WATERHOUSE, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. 4^{e} série **2** (1969), 521–560. [278, 605]

[WEB 1997] H. J. WEBER, *Hyperelliptic simple factors of $J_0(N)$ with dimension at least* 3, Experiment. Math. **6** (1997), 273–287. [104, 470, 472]

[WEI 1948] A. WEIL, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Publ. Inst. Math. Univ. Strasbourg **7** (1945), Hermann et Cie., Paris, 1948. [135]

[WEI 1949] ———, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497–508. [134]

[WEI 1957] ———, *Zum Beweis des Torellischen Satzes*, Nachr. Akad. Wiss. Göttingen, Math. Phys. Klasse (1957), 33–53. [101]

[WEI 2001] A. WEIMERSKIRCH, *The application of the Mordell–Weil group to cryptographic systems*, Master's thesis, Worchester polytechnic institute, 2001. [383]

[WEI 2005] E. W. WEISSTEIN, *RSA-200 factored*, 2005. http://mathworld.wolfram.com/news/2005-05-10/rsa-200/ [7]

[WEN 2001a] A. WENG, *Hyperelliptic CM-curves of genus* 3, J. Ramanujan Math. Soc. **16** (2001), 339–372. [104, 108, 472, 473]

[WEN 2001b] ———, *Konstruktion kryptographisch geeigneter Kurven mit komplexer Multiplikation*, PhD. Thesis, Universität Gesamthochschule Essen, 2001. [106, 459, 471, 564]

[WEN 2003] ———, *Constructing hyperelliptic curves of genus* 2 *suitable for cryptography*, Math. Comp. **72** N°241 (2003), 435–458. [101, 465, 467, 468]

[WENG] ———, *A table of class polynomials covering all CM-curves up to discriminant* 422500. http://www.exp-math.uni-essen.de/zahlentheorie/classpol/class.html [457, 458, 460, 567]

[Wie 1986] D. H. Wiedemann, *Solving sparse linear equations over finite fields*, IEEE Trans. Inform. Theory **IT-32** N°1 (1986), 54–62. [501]

[Wil 1982] H. C. Williams, *A $p+1$ method of factoring*, Math. Comp. **39** N°159 (1982), 225–234. [604]

[WiZu 1998] M. Wiener & R. Zuccherato, *Faster attacks on elliptic curve cryptosystems*, Selected Areas in Cryptography – SAC 1998, Lecture Notes in Comput. Sci., vol. 1556, Springer-Verlag, Berlin, 1998, 190–200. [491]

[WoBa+ 2000] A. Woodbury, D. Bailey, & C. Paar, *Elliptic curve cryptography on smart cards without coprocessor*, Smart Card Research and Advanced Application – CARDIS 2000, IFIP Conference Proceedings, vol. 180, Kluwer Academic Publishers, 2000, 71–92. [229, 646]

[Wol 2004] T. Wollinger, *Software and hardware implementation of hyperelliptic curve cryptosystems*, PhD. Thesis, Ruhr-University of Bochum, 2004. [348, 352]

[WuHa+ 2002] H. Wu, M. A. Hasan, I. F. Blake, & S. Gao, *Finite field multiplier using redundant representation*, IEEE Trans. on Computers **51** N°11 (2002), 1306–1316. [217]

[WuWu+ 2004] C.-H. Wu, C.-M. Wu, M.-D. Shieh, & Y.-T. Hwang, *High-speed, low-complexity systolic designs of novel iterative division algorithms in GF($2m$)*, IEEE Trans. on Computers **53** N°3 (2004), 375–380. [223]

[Yac 1998] Y. Yacobi, *Fast exponentiation using data compression*, SIAM J. Comput. **28** N°2 (1998), 700–703. [160]

[Yan 2001] T. Yanik, *New methods for finite field arithmetic*, PhD. Thesis, Oregon State University, 2001.
`http://islab.oregonstate.edu/papers/01Yanik.pdf` [202]

[Yao 1976] A. C. Yao, *On the evaluation of powers*, SIAM J. Comput. **5** (1976), 100–103. [158, 165]

[YaSa+ 2002] T. Yanik, E. Savaş, & Ç. K. Koç, *Incomplete reduction in modular arithmetic*, IEEE Micro **149** N°2 (2002), 46–52. [202, 640]

[Zag 1981] D. Zagier, *Zetafunktionen und quadratische Zahlkörper*, Springer-Verlag, Berlin, 1981, Eine Einführung in die höhere Zahlentheorie. [An introduction to higher number theory], Hochschultext. [University Text]. [457]

[ZaSa 1976] O. Zariski & P. Samuel, *Commutative algebra. vol. II.*, Springer, 1976. [45, 48, 67, 75, 78]

[Zen] F. Chabaud & R. Lercier, *ZEN, version 3.0*, 2001.
`http://zenfact.sourceforge.net/` [201]

[Zha 2002] Z. Zhang, *A one-parameter quadratic-base version of the Baillie-PSW probable prime test*, Math. Comp. **71** N°240 (2002), 1669–1734. [596]

[ZiLe 1977] J. Ziv & A. Lempel, *A universal algorithm for data compression*, IEEE Trans. Inform. Theory **IT-23** (1977), 337–343. [160]

[Zim 2001] P. Zimmermann, *Arithmétique en précision arbitraire*, Tech. Report 4272, INRIA Lorraine, September 2001.
`http://www.loria.fr/~zimmerma/papers/RR4272.ps.gz` [172, 187]