Bibliography

[1] M. Abdalla, M. Bellare, and P. Rogaway, *DHIES: An encryption scheme based on the Diffie-Hellman problem*, Preprint, 2001.

[2] L. M. Adleman and J. DeMarrais, *A subexponential algorithm for discrete logarithms over all finite fields*, Math. Comp. **61** (1993), no. 203, 1–15.

[3] L. M. Adleman, K. L. Manders, and G. L. Miller, *On taking roots in finite fields*, Foundations of Computer Science (FOCS), IEEE, 1977, pp. 175–178.

[4] L.M. Adleman, J. DeMarrais, and M.-D. Huang, *A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields*, ANTS I (L. M. Adleman and M.-D. Huang, eds.), LNCS, vol. 877, Springer, 1994, pp. 28–40.

[5] G. B. Agnew, R. C. Mullin, I. M. Onyszchuk, and S. A. Vanstone, *An implementation for a fast public-key cryptosystem*, J. Crypt. **3** (1991), no. 2, 63–79.

[6] M. Agrawal, N. Kayal, and N. Saxena, *PRIMES is in P*, Ann. of Math **160** (2004), no. 2, 781–793.

[7] E. Agrell, T. Eriksson, A. Vardy, and K. Zeger, *Closest point search in lattices*, IEEE Trans. Inf. Theory **48** (2002), no. 8, 2201–2214.

[8] A. Akavia, *Solving hidden number problem with one bit oracle and advice*, CRYPTO 2009 (S. Halevi, ed.), LNCS, vol. 5677, Springer, 2009, pp. 337–354.

[9] W. Alexi, B. Chor, O. Goldreich, and C.-P. Schnorr, *RSA and Rabin functions: Certain parts are as hard as the whole*, SIAM J. Comput. **17** (1988), no. 2, 194–209.

[10] W. R. Alford, A. Granville, and C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math. **139** (1994), no. 3, 703–722.

[11] A. Antipa, D. R. L. Brown, R. P. Gallant, R. J. Lambert, R. Struik, and S. A. Vanstone, *Accelerated verification of ECDSA signatures*, SAC 2005 (B. Preneel and S. E. Tavares, eds.), LNCS, vol. 3897, Springer, 2006, pp. 307–318.

[12] C. Arène, T. Lange, M. Naehrig, and C. Ritzenthaler, *Faster computation of the Tate pairing*, J. Number Theory **131** (2011), no. 5, 842–857.

[13] J. Arney and E. D. Bender, *Random mappings with constraints on coalescence and number of origins*, Pacific J. Math. **103** (1982), 269–294.

[14] E. Artin, *Galois theory*, 2nd ed., Notre Dame, 1959.

[15] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley, 1969.

[16] R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, and F. Vercauteren, *Handbook of elliptic and hyperelliptic cryptography*, Chapman and Hall/CRC, 2006.

[17] R. M. Avanzi, *A note on the signed sliding window integer recoding and a left-to-right analogue*, SAC 2004 (H. Handschuh and M. A. Hasan, eds.), LNCS, vol. 3357, Springer, 2004, pp. 130–143.

[18] L. Babai, *On Lovász lattice reduction and the nearest lattice point problem*, Combinatorica **6** (1986), no. 1, 1–13.

[19] L. Babai and E. Szemerédi, *On the complexity of matrix group problems I*, Foundations of Computer Science (FOCS) (1996), 229–240.

[20] E. Bach, *Bounds for primality testing and related problems*, Math. Comp. **55** (1990), no. 191, 355–380.

[21] ———, *Toward a theory of Pollard's rho method*, Inf. Comput. **90** (1991), no. 2, 139–155.

[22] E. Bach and J. Shallit, *Algorithmic number theory*, MIT press, 1996.

[23] E. Bach and J. Sorenson, *Sieve algorithms for perfect power testing*, Algorithmica **9** (1993), 313–328.

[24] S. Bai and R. P. Brent, *On the efficiency of Pollard's rho method for discrete logarithms*, CATS 2008 (J. Harland and P. Manyem, eds.), Australian Computer Society, 2008, pp. 125–131.

[25] D. V. Bailey, L. Batina, D. J. Bernstein, P. Birkner, J. W. Bos, H.-C. Chen, C.-M. Cheng, G. van Damme, G. de Meulenaer, L. Julian Dominguez Perez, J. Fan, T. Güneysu, F. Gurkaynak, T. Kleinjung, T. Lange, N. Mentens, R. Niederhagen, C. Paar, F. Regazzoni, P. Schwabe, L. Uhsadel, A. Van Herrewege, and B.-Y. Yang, *Breaking ECC2K-130*, Cryptology ePrint Archive, Report 2009/541, 2009.

[26] R. Balasubramanian and N. Koblitz, *The improbability that an elliptic curve has sub-exponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm*, J. Crypt. **11** (1998), no. 2, 141–145.

[27] W. D. Banks and I. E. Shparlinski, *Sato-Tate, cyclicity, and divisibility statistics on average for elliptic curves of small height*, Israel J. Math. **173** (2009), 253–277.

[28] P. S. L. M. Barreto, S. D. Galbraith, C. Ó hÉigeartaigh, and M. Scott, *Efficient pairing computation on supersingular abelian varieties*, Des. Codes Crypt. **42** (2007), no. 3, 239–271.

[29] P. S. L. M. Barreto, H. Y. Kim, B. Lynn, and M. Scott, *Efficient algorithms for pairing-based cryptosystems*, CRYPTO 2002 (M. Yung, ed.), LNCS, vol. 2442, Springer, 2002, pp. 354–369.

[30] P. S. L. M. Barreto and M. Naehrig, *Pairing-friendly elliptic curves of prime order*, SAC 2005 (B. Preneel and S. E. Tavares, eds.), LNCS, vol. 3897, Springer, 2006, pp. 319–331.

[31] A. Bauer, *Vers une généralisation rigoureuse des méthodes de Coppersmith pour la recherche de petites racines de polynômes*, Ph.D. thesis, Université de Versailles Saint-Quentin-en-Yvelines, 2008.

[32] M. Bellare, R. Canetti, and H. Krawczyk, *A modular approach to the design and analysis of authentication and key exchange protocols*, Symposium on the Theory of Computing (STOC), ACM, 1998, pp. 419–428.

[33] M. Bellare, J. A. Garay, and T. Rabin, *Fast batch verification for modular exponentiation and digital signatures*, EUROCRYPT 1998 (K. Nyberg, ed.), LNCS, vol. 1403, Springer, 1998, pp. 236–250.

[34] M. Bellare, S. Goldwasser, and D. Micciancio, *"Pseudo-Random" number generation within cryptographic algorithms: The DSS case*, CRYPTO 1997 (B. S. Kaliski Jr., ed.), LNCS, vol. 1294, Springer, 1997, pp. 277–291.

[35] M. Bellare, C. Namprempre, and G. Neven, *Security proofs for identity-based identification and signature schemes*, J. Crypt. **22** (2009), no. 1, 1–61.

[36] M. Bellare and G. Neven, *Multi-signatures in the plain public-key model and a general forking lemma*, CCS 2006 (A. Juels, R. N. Wright, and S. De Capitani di Vimercati, eds.), ACM, 2006, pp. 390–399.

[37] M. Bellare, D. Pointcheval, and P. Rogaway, *Authenticated key exchange secure against dictionary attacks*, EUROCRYPT 2000 (B. Preneel, ed.), LNCS, vol. 1807, Springer, 2000, pp. 139–155.

[38] M. Bellare and P. Rogaway, *Random oracles are practical: A paradigm for designing efficient protocols*, CCS 1993, ACM, 1993, pp. 62–73.

[39] ______, *Entity authentication and key distribution*, CRYPTO 1993 (D. R. Stinson, ed.), LNCS, vol. 773, Springer, 1994, pp. 232–249.

[40] ______, *Optimal asymmetric encryption - How to encrypt with RSA*, EUROCRYPT 1994 (A. De Santis, ed.), LNCS, vol. 950, Springer, 1995, pp. 92–111.

[41] ______, *The exact security of digital signatures – how to sign with RSA and Rabin*, EUROCRYPT 1996 (U. M. Maurer, ed.), LNCS, vol. 1070, Springer, 1996, pp. 399–416.

[42] K. Bentahar, *The equivalence between the DHP and DLP for elliptic curves used in practical applications, revisited*, IMA Cryptography and Coding (N. P. Smart, ed.), LNCS, vol. 3796, Springer, 2005, pp. 376–391.

[43] ______, *Theoretical and practical efficiency aspects in cryptography*, Ph.D. thesis, University of Bristol, 2008.

[44] D. J. Bernstein, *Faster square roots in annoying finite fields*, Preprint, 2001.

[45] ______, *Pippenger's exponentiation algorithm*, Preprint, 2002.

[46] ______, *Curve 25519: New Diffie-Hellman speed records*, PKC 2006 (M. Yung, Y. Dodis, A. Kiayias, and T. Malkin, eds.), LNCS, vol. 3958, Springer, 2006, pp. 207–228.

[47] ———, *Proving tight security for Rabin-Williams signatures*, EUROCRYPT 2008 (N. P. Smart, ed.), LNCS, vol. 4965, Springer, 2008, pp. 70–87.

[48] D. J. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters, *Twisted Edwards curves*, Africacrypt 2008 (S. Vaudenay, ed.), LNCS, vol. 5023, Springer, 2008, pp. 389–405.

[49] D. J. Bernstein, P. Birkner, T. Lange, and C. Peters, *ECM using Edwards curves*, Cryptology ePrint Archive, Report 2008/016, 2008.

[50] D. J. Bernstein, J. Buchmann, and E. Dahmen, *Post quantum cryptography*, Springer, 2008.

[51] D. J. Bernstein and T. Lange, *Explicit formulas database*, 2007.

[52] ———, *Faster addition and doubling on elliptic curves*, ASIACRYPT 2007 (K. Kurosawa, ed.), LNCS, vol. 4833, Springer, 2007, pp. 29–50.

[53] ———, *Analysis and optimization of elliptic-curve single-scalar multiplication*, Contemporary Mathematics **461** (2008), 1–19.

[54] ———, *Type-II optimal polynomial bases*, WAIFI 2010 (M. A. Hasan and T. Helleseth, eds.), LNCS, vol. 6087, Springer, 2010, pp. 41–61.

[55] D. J. Bernstein, T. Lange, and R. R. Farashahi, *Binary Edwards curves*, CHES 2008, (E. Oswald and P. Rohatgi, eds.), LNCS, vol. 5154, Springer, 2008, pp. 244–265.

[56] D. J. Bernstein, T. Lange, and P. Schwabe, *On the correct use of the negation map in the Pollard rho method*, PKC 2011 (D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, eds.), LNCS, vol. 6571, Springer, 2011, pp. 128–146.

[57] E. Biham, D. Boneh, and O. Reingold, *Breaking generalized Diffie-Hellman modulo a composite is no easier than factoring*, Inf. Process. Lett. **70** (1999), no. 2, 83–87.

[58] G. Bisson and A. V. Sutherland, *Computing the endomorphism ring of an ordinary elliptic curve over a finite field*, J. Number Theory **131** (2011), no. 5, 815–831.

[59] S. R. Blackburn and S. Murphy, *The number of partitions in Pollard rho*, unpublished manuscript, 1998.

[60] S. R. Blackburn and E. Teske, *Baby-step giant-step algorithms for non-uniform distributions*, ANTS IV (W. Bosma, ed.), LNCS, vol. 1838, Springer, 2000, pp. 153–168.

[61] I. F. Blake, R. Fuji-Hara, R. C. Mullin, and S. A. Vanstone, *Computing logarithms in finite fields of characteristic two*, SIAM J. Algebraic and Discrete Methods **5** (1984), no. 2, 272–285.

[62] I. F. Blake and T. Garefalakis, *On the complexity of the discrete logarithm and Diffie-Hellman problems*, J. Complexity **20** (2004), no. 2-3, 148–170.

[63] I. F. Blake, T. Garefalakis, and I. E. Shparlinski, *On the bit security of the Diffie-Hellman key*, Appl. Algebra Eng. Commun. Comput. **16** (2006), no. 6, 397–404.

[64] I. F. Blake, G. Seroussi, and N. P. Smart, *Elliptic curves in cryptography*, Cambridge, 1999.

[65] ———, *Advances in elliptic curve cryptography*, Cambridge, 2005.

[66] D. Bleichenbacher, *Generating ElGamal signatures without knowing the secret key*, EUROCRYPT 1996 (U. M. Maurer, ed.), LNCS, vol. 1070, Springer, 1996, pp. 10–18.

[67] ———, *Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1*, CRYPTO 1998 (H. Krawczyk, ed.), LNCS, vol. 1462, Springer, 1998, pp. 1–12.

[68] ———, *Compressing Rabin signatures*, CT-RSA 2004 (T. Okamoto, ed.), LNCS, vol. 2964, Springer, 2004, pp. 126–128.

[69] D. Bleichenbacher and A. May, *New attacks on RSA with small secret CRT-exponents*, PKC 2006 (M. Yung, Y. Dodis, A. Kiayias, and T. Malkin, eds.), LNCS, vol. 3958, Springer, 2006, pp. 1–13.

[70] D. Bleichenbacher and P. Q. Nguyen, *Noisy polynomial interpolation and noisy Chinese remaindering*, EUROCRYPT 2000 (B. Preneel, ed.), LNCS, vol. 1807, Springer, 2000, pp. 53–69.

[71] J. Blömer and A. May, *Low secret exponent RSA revisited*, Cryptography and Lattices (CaLC) (J. H. Silverman, ed.), LNCS, vol. 2146, Springer, 2001, pp. 4–19.

[72] J. Blömer and A. May, *A tool kit for finding small roots of bivariate polynomials over the integers*, EUROCRYPT 2005 (R. Cramer, ed.), LNCS, vol. 3494, Springer, 2005, pp. 251–267.

[73] M. Blum and S. Micali, *How to generate cryptographically strong sequences of pseudo-random bits*, SIAM J. Comput. **13** (1984), no. 4, 850–864.

[74] D. Boneh, *Simplified OAEP for the RSA and Rabin functions*, CRYPTO 2001 (J. Kilian, ed.), LNCS, vol. 2139, Springer, 2001, pp. 275–291.

[75] ———, *Finding smooth integers in short intervals using CRT decoding*, J. Comput. Syst. Sci. **64** (2002), no. 4, 768–784.

[76] D. Boneh and X. Boyen, *Short signatures without random oracles*, EUROCRYPT 2004 (C. Cachin and J. Camenisch, eds.), LNCS, vol. 3027, Springer, 2004, pp. 56–73.

[77] ———, *Short signatures without random oracles and the SDH assumption in bilinear groups*, J. Crypt. **21** (2008), no. 2, 149–177.

[78] D. Boneh and G. Durfee, *Cryptanalysis of RSA with private key d less than $N^{0.292}$*, IEEE Trans. Inf. Theory **46** (2000), no. 4, 1339–1349.

[79] D. Boneh, G. Durfee, and N. Howgrave-Graham, *Factoring $N = p^r q$ for large r*, CRYPTO 1999 (M. J. Wiener, ed.), LNCS, vol. 1666, Springer, 1999, pp. 326–337.

[80] D. Boneh and M. K. Franklin, *Identity based encryption from the Weil pairing*, CRYPTO 2001 (J. Kilian, ed.), LNCS, vol. 2139, Springer, 2001, pp. 213–229.

[81] ———, *Identity based encryption from the Weil pairing*, SIAM J. Comput. **32** (2003), no. 3, 586–615.

[82] D. Boneh, A. Joux, and P. Nguyen, *Why textbook ElGamal and RSA encryption are insecure*, ASIACRYPT 2000 (T. Okamoto, ed.), LNCS, vol. 1976, Springer, 2000, pp. 30–43.

[83] D. Boneh and R. J. Lipton, *Algorithms for black-box fields and their application to cryptography*, CRYPTO 1996 (N. Koblitz, ed.), LNCS, vol. 1109, Springer, 1996, pp. 283–297.

[84] D. Boneh and I. E. Shparlinski, *On the unpredictability of bits of the elliptic curve Diffie-Hellman scheme*, CRYPTO 2001 (J. Kilian, ed.), LNCS, vol. 2139, Springer, 2001, pp. 201–212.

[85] D. Boneh and R. Venkatesan, *Hardness of computing the most significant bits of secret keys in Diffie-Hellman and related schemes*, CRYPTO 1996 (N. Koblitz, ed.), LNCS, vol. 1109, Springer, 1996, pp. 129–142.

[86] ______, *Rounding in lattices and its cryptographic applications*, Symposium on Discrete Algorithms (SODA), ACM/SIAM, 1997, pp. 675–681.

[87] ______, *Breaking RSA may not be equivalent to factoring*, EUROCRYPT 1998 (K. Nyberg, ed.), LNCS, vol. 1403, Springer, 1998, pp. 59–71.

[88] A. Borodin and I. Munro, *The computational complexity of algebraic and numeric problems*, Elsevier, 1975.

[89] J. W. Bos, M. E. Kaihara, and T. Kleinjung, *Pollard rho on elliptic curves*, Preprint, 2009.

[90] J. W. Bos, M. E. Kaihara, and P. L. Montgomery, *Pollard rho on the playstation 3*, Handouts of SHARCS 2009, 2009, pp. 35–50.

[91] J. W. Bos, T. Kleinjung, and A. K. Lenstra, *On the use of the negation map in the Pollard Rho method*, ANTS IX (G. Hanrot, F. Morain, and E. Thomé, eds.), LNCS, vol. 6197, Springer, 2010, pp. 66–82.

[92] W. Bosma and H. W. Lenstra Jr., *Complete systems of two addition laws for elliptic curves*, J. Number Theory **53** (1995), 229–240.

[93] A. Bostan, F. Morain, B. Salvy, and E. Schost, *Fast algorithms for computing isogenies between elliptic curves*, Math. Comp. **77** (2008), no. 263, 1755–1778.

[94] C. Boyd and A. Mathuria, *Protocols for authentication and key establishment*, Information Security and Cryptography, Springer, 2003.

[95] X. Boyen, *The uber-assumption family*, Pairing 2008 (S. D. Galbraith and K. G. Paterson, eds.), LNCS, vol. 5209, Springer, 2008, pp. 39–56.

[96] V. Boyko, M. Peinado, and R. Venkatesan, *Speeding up discrete log and factoring based schemes via precomputations*, EUROCRYPT 1998 (K. Nyberg, ed.), LNCS, vol. 1403, Springer, 1998, pp. 221–235.

[97] S. Brands, *An efficient off-line electronic cash system based on the representation problem*, Tech. report, CWI Amsterdam, 1993, CS-R9323.

[98] R. P. Brent, *An improved Monte Carlo factorization algorithm*, BIT (1980), 176–184.

[99] R. P. Brent and J. M. Pollard, *Factorization of the eighth Fermat number*, Math. Comp. **36** (1981), no. 154, 627–630.

[100] R. P. Brent and P. Zimmermann, *Modern computer arithmetic*, Cambridge, 2010.

[101] ———, *An $O(M(n)logn)$ algorithm for the Jacobi symbol*, ANTS IX (G. Hanrot, F. Morain, and E. Thomé, eds.), LNCS, vol. 6197, Springer, 2010, pp. 83–95.

[102] E. Bresson, Y. Lakhnech, L. Mazaré, and B. Warinschi, *A generalization of DDH with applications to protocol analysis and computational soundness*, CRYPTO 2007 (A. J. Menezes, ed.), LNCS, vol. 4622, Springer, 2007, pp. 482–499.

[103] E. F. Brickell, *Breaking iterated knapsacks*, CRYPTO 1984 (G. R. Blakley and D. Chaum, eds.), LNCS, vol. 196, Springer, 1985, pp. 342–358.

[104] E. F. Brickell and A. M. Odlyzko, *Cryptanalysis: A survey of recent results*, Contemporary Cryptology (G. J. Simmons, ed.), IEEE, 1991, pp. 501–540.

[105] E. F. Brickell, D. Pointcheval, S. Vaudenay, and M. Yung, *Design validations for discrete logarithm based signature schemes*, PKC 2000 (H. Imai and Y. Zheng, eds.), LNCS, vol. 1751, Springer, 2000, pp. 276–292.

[106] E. Brier, C. Clavier, and D. Naccache, *Cryptanalysis of RSA signatures with fixed-pattern padding*, CRYPTO 2001 (J. Kilian, ed.), LNCS, vol. 2139, Springer, 2001, pp. 433–439.

[107] R. Bröker, *Constructing supersingular elliptic curves*, J. Comb. Number Theory **1** (2009), no. 3, 269–273.

[108] R. Bröker, D. X. Charles, and K. Lauter, *Evaluating large degree isogenies and applications to pairing based cryptography*, Pairing 2008 (S. D. Galbraith and K. G. Paterson, eds.), LNCS, vol. 5209, Springer, 2008, pp. 100–112.

[109] R. Bröker, K. Lauter, and A. V. Sutherland, *Modular polynomials via isogeny volcanoes*, Math. Comp. **81** (2012), no. 278, 1201–1231.

[110] R. Bröker and A. V. Sutherland, *An explicit height bound for the classical modular polynomial*, The Ramanujan Journal **22** (2010), no. 3, 293–313.

[111] D. R. L. Brown and R. P. Gallant, *The static Diffie-Hellman problem*, Cryptology ePrint Archive, Report 2004/306, 2004.

[112] B. B. Brumley and K. U. Järvinen, *Koblitz curves and integer equivalents of Frobenius expansions*, SAC 2007 (C. M. Adams, A. Miri, and M. J. Wiener, eds.), LNCS, vol. 4876, Springer, 2007, pp. 126–137.

[113] J. P. Buhler and P. Stevenhagen, *Algorithmic number theory*, MSRI publications, Cambridge, 2008.

[114] M. Burmester and Y. Desmedt, *A secure and efficient conference key distribution system*, EUROCRYPT 1994 (A. De Santis, ed.), LNCS, vol. 950, Springer, 1995, pp. 267–275.

[115] R. Canetti, O. Goldreich, and S. Halevi, *The random oracle model, revisited*, Symposium on the Theory of Computing (STOC), ACM, 1998, pp. 209–218.

[116] R. Canetti and H. Krawczyk, *Analysis of key-exchange protocols and their use for building secure channels*, EUROCRYPT 2001 (B. Pfitzmann, ed.), LNCS, vol. 2045, Springer, 2001, pp. 453–474.

[117] E. R. Canfield, P. Erdös, and C. Pomerance, *On a problem of Oppenheim concerning "factorisatio numerorum"*, J. Number Theory **17** (1983), no. 1, 1–28.

[118] D. G. Cantor, *Computing in the Jacobian of an hyperelliptic curve*, Math. Comp. **48** (1987), no. 177, 95–101.

[119] ______, *On the analogue of the division polynomials for hyperelliptic curves*, J. Reine Angew. Math. **447** (1994), 91–145.

[120] D. Cash, E. Kiltz, and V. Shoup, *The twin Diffie-Hellman problem and applications*, EUROCRYPT 2008 (N. P. Smart, ed.), LNCS, vol. 4965, Springer, 2008, pp. 127–145.

[121] J. W. S. Cassels, *An introduction to the geometry of numbers*, Springer, 1959.

[122] ______, *Lectures on elliptic curves*, Cambridge, 1991.

[123] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus 2*, Cambridge, 1996.

[124] J. W. S. Cassels and A. Frölich, *Algebraic number theory*, Academic Press, 1967.

[125] D. Catalano, R. Gennaro, N. Howgrave-Graham, and P. Q. Nguyen, *Paillier's cryptosystem revisited*, CCS 2001, ACM, 2001, pp. 206–214.

[126] L. S. Charlap and R. Coley, *An elementary introduction to elliptic curves II*, CCR Expository Report 34, Institute for Defense Analysis, 1990.

[127] L. S. Charlap and D. P. Robbins, *An elementary introduction to elliptic curves*, CRD Expository Report 31, 1988.

[128] D. X. Charles, K. E. Lauter, and E. Z. Goren, *Cryptographic hash functions from expander graphs*, J. Crypt. **22** (2009), no. 1, 93–113.

[129] M. Chateauneuf, A. C. H. Ling, and D. R. Stinson, *Slope packings and coverings, and generic algorithms for the discrete logarithm problem*, Journal of Combinatorial Designs **11** (2003), no. 1, 36–50.

[130] D. Chaum, E. van Heijst, and B. Pfitzmann, *Cryptographically strong undeniable signatures, unconditionally secure for the signer*, CRYPTO 1991 (J. Feigenbaum, ed.), LNCS, vol. 576, Springer, 1992, pp. 470–484.

[131] J.-H. Cheon, *Security analysis of the strong Diffie-Hellman problem*, EUROCRYPT 2006 (S. Vaudenay, ed.), LNCS, vol. 4004, Springer, 2006, pp. 1–11.

[132] ______, *Discrete logarithm problem with auxiliary inputs*, J. Crypt. **23** (2010), no. 3, 457–476.

[133] J. H. Cheon, J. Hong, and M. Kim, *Speeding up the Pollard rho method on prime fields*, ASIACRYPT 2008 (J. Pieprzyk, ed.), LNCS, vol. 5350, Springer, 2008, pp. 471–488.

[134] J. H. Cheon and H.-T. Kim, *Analysis of low Hamming weight products*, Discrete Applied Mathematics **156** (2008), no. 12, 2264–2269.

[135] M. A. Cherepnev, *On the connection between the discrete logarithms and the Diffie-Hellman problem*, Discr. Math. Appl. **6** (1996), no. 4, 341–349.

[136] H. Cohen, *A course in computational algebraic number theory*, GTM 138, Springer, 1993.

[137] ______, *Analysis of the sliding window powering algorithm*, J. Crypt. **18** (2005), no. 1, 63–76.

[138] P. Cohen, *On the coefficients of the transformation polynomials for the elliptic modular function*, Math. Proc. Cambridge Philos. Soc. **95** (1984), no. 3, 389–402.

[139] S. A. Cook, *An overview of computational complexity*, Commun. ACM **26** (1983), no. 6, 400–408.

[140] D. Coppersmith, *Fast evaluation of logarithms in fields of characteristic 2*, IEEE Trans. Inf. Theory **30** (1984), no. 4, 587–594.

[141] ______, *Small solutions to polynomial equations, and low exponent RSA vulnerabilities*, J. Crypt. **10** (1997), no. 4, 233–260.

[142] ______, *Finding small solutions to small degree polynomials*, Cryptography and Lattices (CaLC) (J. H. Silverman, ed.), LNCS, vol. 2146, Springer, 2001, pp. 20–31.

[143] D. Coppersmith, J.-S. Coron, F. Grieu, S. Halevi, C. Jutla, D. Naccache, and J. P. Stern, *Cryptanalysis of ISO/IEC 9796-1*, J. Crypt. **21** (2008), no. 1, 27–51.

[144] D. Coppersmith, M. K. Franklin, J. Patarin, and M. K. Reiter, *Low-exponent RSA with related messages*, EUROCRYPT 1996 (U. M. Maurer, ed.), LNCS, vol. 1070, Springer, 1996, pp. 1–9.

[145] D. Coppersmith, A. M. Odlzyko, and R. Schroeppel, *Discrete logarithms in GF(p)*, Algorithmica **1** (1986), no. 1-4, 1–15.

[146] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to algorithms*, 2nd ed., MIT press, 2001.

[147] G. Cornelissen, *Two-torsion in the Jacobian of hyperelliptic curves over finite fields*, Arch. Math. **77** (2001), no. 3, 241–246.

[148] J.-S. Coron, *On the exact security of full domain hash*, CRYPTO 2000 (M. Bellare, ed.), LNCS, vol. 1880, Springer, 2000, pp. 229–235.

[149] ______, *Optimal security proofs for PSS and other signature schemes*, EUROCRYPT 2002 (L. R. Knudsen, ed.), LNCS, vol. 2332, Springer, 2002, pp. 272–287.

[150] ______, *Finding small roots of bivariate integer polynomial equations: A direct approach*, CRYPTO 2007 (A. Menezes, ed.), LNCS, vol. 4622, Springer, 2007, pp. 379–394.

[151] J.-S. Coron and A. May, *Deterministic polynomial-time equivalence of computing the RSA secret key and factoring*, J. Crypt. **20** (2007), no. 1, 39–50.

[152] J.-S. Coron, D. M'Raïhi, and C. Tymen, *Fast generation of pairs* $(k, [k]P)$ *for Koblitz elliptic curves*, SAC 2001 (S. Vaudenay and A. M. Youssef, eds.), LNCS, vol. 2259, Springer, 2001, pp. 151–164.

[153] J.-S. Coron, D. Naccache, M. Tibouchi, and R.-P. Weinmann, *Practical cryptanalysis of ISO/IEC 9796-2 and EMV signatures*, CRYPTO 2009 (S. Halevi, ed.), LNCS, vol. 5677, Springer, 2009, pp. 428–444.

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

[155] J.-M. Couveignes, *Computing* l*-isogenies with the* p*-torsion*, ANTS II (H. Cohen, ed.), LNCS, vol. 1122, Springer, 1996, pp. 59–65.

[156] J.-M. Couveignes, L. Dewaghe, and F. Morain, *Isogeny cycles and the Schoof-Elkies-Atkin algorithm*, Research Report LIX/RR/96/03, 1996.

[157] D. A. Cox, *Primes of the form* $x^2 + ny^2$, Wiley, 1989.

[158] D. A. Cox, J. Little, and D. O'Shea, *Ideals, varieties and algorithms: An introduction to computational algebraic geometry and commutative algebra*, 2nd ed., Springer, 1997.

[159] R. Cramer and V. Shoup, *A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack*, CRYPTO 1998 (H. Krawczyk, ed.), LNCS, vol. 1462, Springer, 1998, pp. 13–25.

[160] ———, *Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption*, EUROCRYPT 2002 (L. R. Knudsen, ed.), LNCS, vol. 2332, Springer, 2002, pp. 45–64.

[161] ———, *Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack*, SIAM J. Comput. **33** (2003), no. 1, 167–226.

[162] R. Crandall and C. Pomerance, *Prime numbers: A computational perspective*, 2nd ed., Springer, 2005.

[163] C. W. Curtis, *Linear algebra: An introductory approach*, Undergraduate Texts in Mathematics, Springer, 1984.

[164] I. Damgård, *On the randomness of Legendre and Jacobi sequences*, CRYPTO 1988 (S. Goldwasser, ed.), LNCS, vol. 403, Springer, 1990, pp. 163–172.

[165] I. Damgård and M. Jurik, *A generalisation, a simplification and some applications of Paillier's probabilistic public-key system*, PKC 2001 (K. Kim, ed.), LNCS, vol. 1992, Springer, 2001, pp. 119–136.

[166] G. Davidoff, P. Sarnak, and A. Valette, *Elementary number theory, group theory, and Ramanujan graphs*, Cambridge, 2003.

[167] M. Davis and E. J. Weyuker, *Computability, complexity and languages*, Academic Press, 1983.

[168] P. de Rooij, *On Schnorr's preprocessing for digital signature schemes*, J. Crypt. **10** (1997), no. 1, 1–16.

[169] B. den Boer, *Diffie-Hellman is as strong as discrete log for certain primes*, CRYPTO 1988 (S. Goldwasser, ed.), LNCS, vol. 403, Springer, 1990, pp. 530–539.

[170] Y. Desmedt and A. M. Odlyzko, *A chosen text attack on the RSA cryptosystem and some discrete logarithm schemes*, CRYPTO 1985 (H. C. Williams, ed.), LNCS, vol. 218, Springer, 1986, pp. 516–522.

[171] L. Dewaghe, *Un corollaire aux formules de Vélu*, Preprint, 1995.

[172] C. Diem, *The GHS-attack in odd characteristic*, J. Ramanujan Math. Soc. **18** (2003), no. 1, 1–32.

[173] ———, *On the discrete logarithm problem in elliptic curves over non-prime finite fields*, Lecture at ECC 2004, 2004.

[174] ———, *An index calculus algorithm for non-singular plane curves of high genus*, Talk at ECC 2006, 2006.

[175] ———, *An index calculus algorithm for plane curves of small degree*, ANTS VII (F. Hess, S. Pauli, and M. E. Pohst, eds.), LNCS, vol. 4076, Springer, 2006, pp. 543–557.

[176] ———, *On the discrete logarithm problem in class groups of curves*, Math. Comp. **80** (2011), no. 273, 443–475.

[177] ———, *On the discrete logarithm problem in elliptic curves*, Compositio Math. **147** (2011), 75–104.

[178] C. Diem and E. Thomé, *Index calculus in class groups of non-hyperelliptic curves of genus three*, J. Crypt. **21** (2008), no. 4, 593–611.

[179] W. Diffie and M. E. Hellman, *New directions in cryptography*, IEEE Trans. Inf. Theory **22** (1976), 644–654.

[180] V. S. Dimitrov, K. U. Järvinen, M. J. Jacobson, W. F. Chan, and Z. Huang, *Provably sublinear point multiplication on Koblitz curves and its hardware implementation*, IEEE Trans. Computers **57** (2008), no. 11, 1469–1481.

[181] V. S. Dimitrov, G. A. Jullien, and W. C. Miller, *Theory and applications of the double-base number system*, IEEE Trans. Computers **48** (1999), no. 10, 1098–1106.

[182] S. A. DiPippo and E. W. Howe, *Real polynomials with all roots on the unit circle and abelian varieties over finite fields*, J. Number Theory **73** (1998), no. 2, 426–450.

[183] C. Doche, T. Icart, and D. R. Kohel, *Efficient scalar multiplication by isogeny decompositions*, PKC 2006 (M. Yung, Y. Dodis, A. Kiayias, and T. Malkin, eds.), LNCS, vol. 3958, Springer, 2006, pp. 191–206.

[184] A. Dujella, *A variant of Wiener's attack on RSA*, Computing **85** (2009), no. 1-2, 77–83.

[185] I. M. Duursma, *Class numbers for some hyperelliptic curves*, Arithmetic, Geometry and Coding Theory (R. Pellikaan, M. Perret, and S.G. Vladut, eds.), Walter de Gruyter, 1996, pp. 45–52.

[186] I. M. Duursma, P. Gaudry, and F. Morain, *Speeding up the discrete log computation on curves with automorphisms*, ASIACRYPT 1999 (K.Y. Lam, E. Okamoto, and C. Xing, eds.), LNCS, vol. 1716, Springer, 1999, pp. 103–121.

[187] I. M. Duursma and H.-S. Lee, *Tate pairing implementation for hyperelliptic curves* $y^2 = x^p - x + d$, ASIACRYPT 2003 (C.-S. Laih, ed.), LNCS, vol. 2894, Springer, 2003, pp. 111–123.

[188] P. N. J. Eagle, S. D. Galbraith, and J. Ong, *Point compression for Koblitz elliptic curves*, Advances in Mathematics of Communication **5** (2011), no. 1, 1–10.

[189] S. Edixhoven, *Le couplage Weil: de la géométrie à l'arithmétique*, Notes from a seminar in Rennes, 2002.

[190] H. M. Edwards, *A normal form for elliptic curves*, Bulletin of the AMS **44** (2007), 393–422.

[191] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, GTM, vol. 150, Springer, 1999.

[192] T. ElGamal, *A public key cryptosystem and a signature scheme based on discrete logarithms*, CRYPTO 1984 (G. R. Blakley and D. Chaum, eds.), LNCS, vol. 196, Springer, 1985, pp. 10–18.

[193] N. D. Elkies, *Elliptic and modular curves over finite fields and related computational issues*, Computational Perspectives on Number Theory (D. A. Buell and J. T. Teitelbaum, eds.), Studies in Advanced Mathematics, AMS, 1998, pp. 21–76.

[194] A. Enge, *Computing modular polynomials in quasi-linear time*, Math. Comp. **78** (2009), no. 267, 1809–1824.

[195] A. Enge and P. Gaudry, *A general framework for subexponential discrete logarithm algorithms*, Acta Arith. **102** (2002), 83–103.

[196] ———, *An $L(1/3 + \epsilon)$ algorithm for the discrete logarithm problem for low degree curves*, EUROCRYPT 2007 (M. Naor, ed.), LNCS, vol. 4515, Springer, 2007, pp. 379–393.

[197] A. Enge, P. Gaudry, and E. Thomé, *An $L(1/3)$ discrete logarithm algorithm for low degree curves*, J. Crypt. **24** (2011), no. 1, 24–41.

[198] A. Enge and A. Stein, *Smooth ideals in hyperelliptic function fields*, Math. Comp. **71** (2002), no. 239, 1219–1230.

[199] S. Erickson, M. J. Jacobson Jr., N. Shang, S. Shen, and A. Stein, *Explicit formulas for real hyperelliptic curves of genus 2 in affine representation*, WAIFI 2007 (C. Carlet and B. Sunar, eds.), LNCS, vol. 4547, Springer, 2007, pp. 202–218.

[200] H. M. Farkas and I. Kra, *Riemann surfaces*, GTM, vol. 71, Springer, 1980.

[201] U. Feige, A. Fiat, and A. Shamir, *Zero-knowledge proofs of identity*, J. Crypt. **1** (1988), no. 2, 77–94.

[202] L. De Feo, *Fast algorithms for towers of finite fields and isogenies*, Ph.D. thesis, L'École Polytechnique, 2010.

[203] R. Fischlin and C.-P. Schnorr, *Stronger security proofs for RSA and Rabin bits*, J. Crypt. **13** (2000), no. 2, 221–244.

[204] P. Flajolet and A. M. Odlyzko, *Random mapping statistics*, EUROCRYPT 1989 (J.-J.Quisquater and J. Vandewalle, eds.), LNCS, vol. 434, Springer, 1990, pp. 329–354.

[205] P. Flajolet and R. Sedgewick, *Analytic combinatorics*, Cambridge, 2009.

[206] R. Flassenberg and S. Paulus, *Sieving in function fields*, Experiment. Math. **8** (1999), no. 4, 339–349.

[207] K. Fong, D. Hankerson, J. López, and A. J. Menezes, *Field inversion and point halving revisited*, IEEE Trans. Computers **53** (2004), no. 8, 1047–1059.

[208] C. Fontaine and F. Galand, *A survey of homomorphic encryption for nonspecialists*, EURASIP Journal on Information Security **2007** (2007), no. 15, 1–10.

[209] M. Fouquet and F. Morain, *Isogeny volcanoes and the SEA algorithm*, ANTS V (C. Fieker and D. R. Kohel, eds.), LNCS, vol. 2369, Springer, 2002, pp. 276–291.

[210] D. Freeman, M. Scott, and E. Teske, *A taxonomy of pairing-friendly elliptic curves*, J. Crypt. **23** (2010), no. 2, 224–280.

[211] D. M. Freeman, O. Goldreich, E. Kiltz, A. Rosen, and G. Segev, *More constructions of lossy and correlation-secure trapdoor functions*, PKC 2010 (P. Q. Nguyen and D. Pointcheval, eds.), LNCS, vol. 6056, Springer, 2010, pp. 279–295.

[212] G. Frey, *How to disguise an elliptic curve*, Talk at ECC 1998, Waterloo, 1998.

[213] G. Frey and H.-G. Rück, *A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves*, Math. Comp. **62** (1994), no. 206, 865–874.

[214] M. D. Fried and M. Jarden, *Field arithmetic*, 3rd ed., Springer, 2008.

[215] E. Fujisaki, T. Okamoto, D. Pointcheval, and J. Stern, *RSA-OAEP is secure under the RSA assumption*, J. Crypt. **17** (2004), no. 2, 81–104.

[216] W. Fulton, *Algebraic curves*, Addison-Wesley, 1989, Out of print, but freely available here: `http://www.math.lsa.umich.edu/~wfulton/`.

[217] S. D. Galbraith, *Constructing isogenies between elliptic curves over finite fields*, LMS J. Comput. Math. **2** (1999), 118–138.

[218] ______, *Supersingular curves in cryptography*, ASIACRYPT 2001 (C. Boyd, ed.), LNCS, vol. 2248, Springer, 2001, pp. 495–513.

[219] S. D. Galbraith, M. Harrison, and D. J. Mireles Morales, *Efficient hyperelliptic arithmetic using balanced representation for divisors*, ANTS VIII (A. J. van der Poorten and A. Stein, eds.), LNCS, vol. 5011, Springer, 2008, pp. 342–356.

[220] S. D. Galbraith, C. Heneghan, and J. F. McKee, *Tunable balancing of RSA*, ACISP 2005 (C. Boyd and J. M. González Nieto, eds.), LNCS, vol. 3574, Springer, 2005, pp. 280–292.

[221] S. D. Galbraith, F. Hess, and N. P. Smart, *Extending the GHS Weil descent attack*, EUROCRYPT 2002 (L. R. Knudsen, ed.), LNCS, vol. 2332, Springer, 2002, pp. 29–44.

[222] S. D. Galbraith, F. Hess, and F. Vercauteren, *Aspects of pairing inversion*, IEEE Trans. Inf. Theory **54** (2008), no. 12, 5719–5728.

[223] S. D. Galbraith and M. Holmes, *A non-uniform birthday problem with applications to discrete logarithms*, Cryptology ePrint Archive, Report 2010/616, 2010.

[224] S. D. Galbraith, X. Lin, and M. Scott, *Endomorphisms for faster elliptic curve cryptography on a large class of curves*, EUROCRYPT 2009 (A. Joux, ed.), LNCS, vol. 5479, Springer, 2009, pp. 518–535.

[225] S. D. Galbraith and J. F. McKee, *The probability that the number of points on an elliptic curve over a finite field is prime*, Journal of the Lond. Math. Soc. **62** (2000), no. 3, 671–684.

[226] S. D. Galbraith, J. M. Pollard, and R. S. Ruprai, *Computing discrete logarithms in an interval*, 2013, pp. 1181–1195.

[227] S. D. Galbraith and R. S. Ruprai, *An improvement to the Gaudry-Schost algorithm for multidimensional discrete logarithm problems*, IMA Cryptography and Coding (M. G. Parker, ed.), LNCS, vol. 5921, Springer, 2009, pp. 368–382.

[228] ______, *Using equivalence classes to accelerate solving the discrete logarithm problem in a short interval*, PKC 2010 (P. Q. Nguyen and D. Pointcheval, eds.), LNCS, vol. 6056, Springer, 2010, pp. 368–383.

[229] S. D. Galbraith and N. P. Smart, *A cryptographic application of Weil descent*, IMA Cryptography and Coding (M. Walker, ed.), LNCS, vol. 1746, Springer, 1999, pp. 191–200.

[230] S. D. Galbraith and A. Stolbunov, *Improved algorithm for the isogeny problem for ordinary elliptic curves*, Applicable Algebra in Engineering, Communication and Computing **24** (2013), no. 2, 107–131.

[231] S. D. Galbraith and E. R. Verheul, *An analysis of the vector decomposition problem*, PKC 2008 (R. Cramer, ed.), LNCS, vol. 4939, Springer, 2008, pp. 308–327.

[232] R. P. Gallant, R. J. Lambert, and S. A. Vanstone, *Improving the parallelized Pollard lambda search on binary anomalous curves*, Math. Comp. **69** (2000), no. 232, 1699–1705.

[233] ______, *Faster point multiplication on elliptic curves with efficient endomorphisms*, CRYPTO 2001 (J. Kilian, ed.), LNCS, vol. 2139, Springer, 2001, pp. 190–200.

[234] N. Gama, N. Howgrave-Graham, and P. Q. Nguyen, *Symplectic lattice reduction and NTRU*, EUROCRYPT 2006 (S. Vaudenay, ed.), LNCS, vol. 4004, Springer, 2006, pp. 233–253.

[235] N. Gama, P. Q. Nguyen, and O. Regev, *Lattice enumeration using extreme pruning*, EUROCRYPT 2010 (H. Gilbert, ed.), LNCS, vol. 6110, Springer, 2010, pp. 257–278.

[236] S. Gao, *Normal bases over finite fields*, Ph.D. thesis, Waterloo, 1993.

[237] T. Garefalakis, *The generalised Weil pairing and the discrete logarithm problem on elliptic curves*, Theor. Comput. Sci. **321** (2004), no. 1, 59–72.

[238] J. von zur Gathen and J. Gerhard, *Modern computer algebra*, Cambridge, 1999.

[239] J. von zur Gathen and M. Giesbrecht, *Constructing normal bases in finite fields*, J. Symb. Comput. **10** (1990), no. 6, 547–570.

[240] J. von zur Gathen, I. E. Shparlinski, and A. Sinclair, *Finding points on curves over finite fields*, SIAM J. Comput. **32** (2003), no. 6, 1436–1448.

[241] P. Gaudry, *Courbes hyperelliptiques et cryptologie*, MSc thesis, L'École Polytechnique, 1995.

[242] ———, *An algorithm for solving the discrete log problem on hyperelliptic curves*, EUROCRYPT 2000 (B. Preneel, ed.), LNCS, vol. 1807, Springer, 2000, pp. 19–34.

[243] ———, *Algorithmique des courbes hyperelliptiques et applications à la cryptologie*, Ph.D. thesis, L'École Polytechnique, 2000.

[244] ———, *Fast genus 2 arithmetic based on theta functions*, J. Math. Crypt. **1** (2007), no. 3, 243–265.

[245] ———, *Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem*, Journal of Symbolic Computation **44** (2009), no. 12, 1690–1702.

[246] P. Gaudry, F. Hess, and N. P. Smart, *Constructive and destructive facets of Weil descent on elliptic curves*, J. Crypt. **15** (2002), no. 1, 19–46.

[247] P. Gaudry and D. Lubicz, *The arithmetic of characteristic 2 Kummer surfaces and of elliptic Kummer lines*, Finite Fields Appl. **15** (2009), no. 2, 246–260.

[248] P. Gaudry and É. Schost, *Construction of secure random curves of genus 2 over prime fields*, EUROCRYPT 2004 (C. Cachin and J. Camenisch, eds.), LNCS, vol. 3027, Springer, 2004, pp. 239–256.

[249] ———, *A low-memory parallel version of Matsuo, Chao, and Tsujii's algorithm*, ANTS VI (D. A. Buell, ed.), LNCS, vol. 3076, Springer, 2004, pp. 208–222.

[250] P. Gaudry, E. Thomé, N. Thériault, and C. Diem, *A double large prime variation for small genus hyperelliptic index calculus*, Math. Comp. **76** (2007), no. 257, 475–492.

[251] C. Gentry, *Key recovery and message attacks on NTRU-composite*, EUROCRYPT 2001 (B. Pfitzmann, ed.), LNCS, vol. 2045, Springer, 2001, pp. 182–194.

[252] ———, *The geometry of provable security: Some proofs of security in which lattices make a surprise appearance*, The LLL Algorithm (P. Q. Nguyen and B. Vallée, eds.), Springer, 2010, pp. 391–426.

[253] C. Gentry, C. Peikert, and V. Vaikuntanathan, *Trapdoors for hard lattices and new cryptographic constructions*, Symposium on the Theory of Computing (STOC) (R. E. Ladner and C. Dwork, eds.), ACM, 2008, pp. 197–206.

[254] M. Girault, *An identity-based identification scheme based on discrete logarithms modulo a composite number*, EUROCRYPT 1990 (I. Damgård, ed.), LNCS, vol. 473, Springer, 1991, pp. 481–486.

[255] M. Girault, G. Poupard, and J. Stern, *On the fly authentication and signature schemes based on groups of unknown order*, J. Crypt. **19** (2006), no. 4, 463–487.

[256] O. Goldreich, S. Goldwasser, and S. Halevi, *Public-key cryptosystems from lattice reduction problems*, CRYPTO 1997 (B. S. Kaliski Jr., ed.), LNCS, vol. 1294, Springer, 1997, pp. 112–131.

[257] O. Goldreich, D. Ron, and M. Sudan, *Chinese remaindering with errors*, IEEE Trans. Inf. Theory **46** (2000), no. 4, 1330–1338.

[258] S. Goldwasser, S. Micali, and R. L. Rivest, *A digital signature scheme secure against adaptive chosen-message attacks*, SIAM J. Comput. **17** (1988), no. 2, 281–308.

[259] G. Gong and L. Harn, *Public-key cryptosystems based on cubic finite field extensions*, IEEE Trans. Inf. Theory **45** (1999), no. 7, 2601–2605.

[260] M. I. González Vasco, M. Näslund, and I. E. Shparlinski, *New results on the hardness of Diffie-Hellman bits*, PKC 2004 (F. Bao, R. H. Deng, and J. Zhou, eds.), LNCS, vol. 2947, Springer, 2004, pp. 159–172.

[261] M. I. González Vasco and I. E. Shparlinski, *On the security of Diffie-Hellman bits*, Cryptography and Computational Number Theory (H. Wang K. Y. Lam, I. E. Shparlinski and C. Xing, eds.), Progress in Computer Science and Applied Logic, Birkhäuser, 2001, pp. 257–268.

[262] D. M. Gordon, *On the number of elliptic pseudoprimes*, Math. Comp. **52** (1989), no. 185, 231–245.

[263] D. M. Gordon and K. S. McCurley, *Massively parallel computation of discrete logarithms*, CRYPTO 1992 (E. F. Brickell, ed.), LNCS, vol. 740, Springer, 1993, pp. 312–323.

[264] J. Gordon, *Strong primes are easy to find*, EUROCRYPT 1984 (T. Beth, N. Cot, and I. Ingemarsson, eds.), LNCS, vol. 209, Springer, 1985, pp. 216–223.

[265] R. Granger, F. Hess, R. Oyono, N. Thériault, and F. Vercauteren, *Ate pairing on hyperelliptic curves*, EUROCRYPT 2007 (M. Naor, ed.), LNCS, vol. 4515, Springer, 2007, pp. 430–447.

[266] R. Granger and F. Vercauteren, *On the discrete logarithm problem on algebraic tori*, CRYPTO 2005 (V. Shoup, ed.), LNCS, vol. 3621, Springer, 2005, pp. 66–85.

[267] A. Granville, *Smooth numbers: Computational number theory and beyond*, Algorithmic number theory (J. P. Buhler and P. Stevenhagen, eds.), MSRI Proceedings, vol. 44, Cambridge, 2008, pp. 267–323.

[268] B. H. Gross, *Heights and the special values of L-series*, Number theory, CMS Conf. Proc., vol. 7, AMS, 1987, pp. 115–187.

[269] M. Grötschel, L. Lovász, and A. Schrijver, *Geometric algorithms and combinatorial optimization*, Springer, 1993.

[270] J. Guarjardo and C. Paar, *Itoh-Tsujii inversion in standard basis and its application in cryptography and codes*, Des. Codes Crypt. **25** (2002), no. 2, 207–216.

[271] L. C. Guillou and J.-J. Quisquater, *A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory*, EUROCRYPT 1988 (C. G. Günther, ed.), LNCS, vol. 330, Springer, 1988, pp. 123–128.

[272] R. K. Guy, *Unsolved problems in number theory*, 2nd ed., Springer, 1994.

[273] J. L. Hafner and K. S. McCurley, *Asymptotically fast triangularization of matrices over rings*, SIAM J. Comput. **20** (1991), no. 6, 1068–1083.

[274] D. Hankerson, A. Menezes, and S. Vanstone, *Guide to elliptic curve cryptography*, Springer, 2004.

[275] G. Hanrot and D. Stehlé, *Improved analysis of Kannan's shortest lattice vector algorithm*, CRYPTO 2007 (A. Menezes, ed.), LNCS, vol. 4622, Springer, 2007, pp. 170–186.

[276] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th ed., Oxford, 1980.

[277] R. Harley, *Fast arithmetic on genus two curves*, Preprint, 2000.

[278] R. Hartshorne, *Algebraic geometry*, GTM, vol. 52, Springer, 1977.

[279] J. Håstad and M. Näslund, *The security of all RSA and discrete log bits*, J. ACM **51** (2004), no. 2, 187–230.

[280] G. Havas, B. S. Majewski, and K. R. Matthews, *Extended GCD and Hermite normal form algorithms via lattice basis reduction*, Experimental Math. **7** (1998), no. 2, 125–136.

[281] B. Helfrich, *Algorithms to construct Minkowski reduced and Hermite reduced lattice bases*, Theor. Comput. Sci. **41** (1985), 125–139.

[282] F. Hess, *A note on the Tate pairing of curves over finite fields*, Arch. Math. **82** (2004), 28–32.

[283] ______, *Pairing lattices*, Pairing 2008 (S. D. Galbraith and K. G. Paterson, eds.), LNCS, vol. 5209, Springer, 2008, pp. 18–38.

[284] F. Hess, N. Smart, and F. Vercauteren, *The eta pairing revisited*, IEEE Trans. Inf. Theory **52** (2006), no. 10, 4595–4602.

[285] N. J. Higham, *Accuracy and stability of numerical algorithms*, 2nd ed., SIAM, 2002.

[286] H. Hisil, K. K.-H. Wong, G. Carter, and E. Dawson, *Jacobi quartic curves revisited*, ACISP 2009 (C. Boyd and J. M. González Nieto, eds.), LNCS, vol. 5594, Springer, 2009, pp. 452–468.

[287] Y. Hitchcock, P. Montague, G. Carter, and E. Dawson, *The efficiency of solving multiple discrete logarithm problems and the implications for the security of fixed elliptic curves*, Int. J. Inf. Secur. **3** (2004), 86–98.

[288] J. Hoffstein, J. Pipher, and J. H. Silverman, *NTRU: A ring-based public key cryptosystem*, ANTS III (J. Buhler, ed.), LNCS, vol. 1423, Springer, 1998, pp. 267–288.

[289] ______, *An introduction to mathematical cryptography*, Springer, 2008.

[290] J. Hoffstein and J. H. Silverman, *Random small Hamming weight products with applications to cryptography*, Discrete Applied Mathematics **130** (2003), no. 1, 37–49.

[291] D. Hofheinz and E. Kiltz, *The group of signed quadratic residues and applications*, CRYPTO 2009 (S. Halevi, ed.), LNCS, vol. 5677, Springer, 2009, pp. 637–653.

[292] S. Hohenberger and B. Waters, *Short and stateless signatures from the RSA assumption*, CRYPTO 2009 (S. Halevi, ed.), LNCS, vol. 5677, Springer, 2009, pp. 654–670.

[293] J. E. Hopcroft and J. D. Ullman, *Introduction to automata theory, languages and computation*, Addison-Wesley, 1979.

[294] J. Horwitz and R. Venkatesan, *Random Cayley digraphs and the discrete logarithm*, ANTS V (C. Fieker and D. R. Kohel, eds.), LNCS, vol. 2369, Springer, 2002, pp. 416–430.

[295] E. W. Howe, *On the group orders of elliptic curves over finite fields*, Compositio Mathematica **85** (1993), 229–247.

[296] N. Howgrave-Graham, *Finding small roots of univariate modular equations revisited*, IMA Cryptography and Coding (M. Darnell, ed.), LNCS, vol. 1355, Springer, 1997, pp. 131–142.

[297] ______, *Approximate integer common divisors*, Cryptography and Lattices (CaLC) (J. H. Silverman, ed.), LNCS, vol. 2146, Springer, 2001, pp. 51–66.

[298] N. Howgrave-Graham, P. Q. Nguyen, D. Pointcheval, J. Proos, J. H. Silverman, A. Singer, and W. Whyte, *The impact of decryption failures on the security of NTRU encryption*, CRYPTO 2003 (D. Boneh, ed.), LNCS, vol. 2729, Springer, 2003, pp. 226–246.

[299] N. Howgrave-Graham and N. P. Smart, *Lattice attacks on digital signature schemes*, Des. Codes Crypt. **23** (2001), 283–290.

[300] N. A. Howgrave-Graham and A. Joux, *New generic algorithms for hard knapsacks*, Eurocrypt 2010 (H. Gilbert, ed.), LNCS, vol. 6110, Springer, 2010, pp. 235–256.

[301] T. W. Hungerford, *Algebra*, GTM 73, Springer, 1974.

[302] D. Husemöller, *Elliptic curves*, 2nd ed., GTM, vol. 111, Springer, 2004.

[303] T. Icart, *How to hash into elliptic curves*, CRYPTO 2009 (S. Halevi, ed.), LNCS, vol. 5677, Springer, 2009, pp. 303–316.

[304] J.-I. Igusa, *Arithmetic variety of moduli for genus two*, Ann. of Math. **72** (1960), no. 3, 612–649.

[305] T. Iijima, K. Matsuo, J. Chao, and S. Tsujii, *Construction of Frobenius maps of twist elliptic curves and its application to elliptic scalar multiplication*, Symposium on Cryptography and Information Security (SCIS) 2002, IEICE Japan, 2002, pp. 699–702.

[306] A. Islam, *Products of three pairwise coprime integers in short intervals*, LMS J. Comput. Math. **15** (2012), 59–70.

[307] T. Itoh and S. Tsujii, *A fast algorithm for computing multiplicative inverses in GF(2^m) using normal bases*, Information and Computation **78** (1988), no. 3, 171–177.

[308] T. Jager and J. Schwenk, *On the equivalence of generic group models*, ProvSec 2008 (K. Chen J. Baek, F. Bao and X. Lai, eds.), LNCS, vol. 5324, Springer, 2008, pp. 200–209.

[309] D. Jao, D. Jetchev, and R. Venkatesan, *On the bits of elliptic curve Diffie-Hellman keys*, INDOCRYPT 2007 (K. Srinathan, C. Pandu Rangan, and M. Yung, eds.), LNCS, vol. 4859, Springer, 2007, pp. 33–47.

[310] D. Jao, S. D. Miller, and R. Venkatesan, *Do all elliptic curves of the same order have the same difficulty of discrete log?*, ASIACRYPT 2005 (B. K. Roy, ed.), LNCS, vol. 3788, Springer, 2005, pp. 21–40.

[311] ______, *Expander graphs based on GRH with an application to elliptic curve cryptography*, J. Number Theory **129** (2009), no. 6, 1491–1504.

[312] D. Jao and V. Soukharev, *A subexponential algorithm for evaluating large degree isogenies*, ANTS IX (G. Hanrot, F. Morain, and E. Thomé, eds.), LNCS, vol. 6197, Springer, 2010, pp. 219–233.

[313] D. Jao and K. Yoshida, *Boneh-Boyen signatures and the strong Diffie-Hellman problem*, Pairing 2009 (H. Shacham and B. Waters, eds.), LNCS, vol. 5671, Springer, 2009, pp. 1–16.

[314] D. Jetchev and R. Venkatesan, *Bits security of the elliptic curve Diffie-Hellman secret keys*, CRYPTO 2008 (D. Wagner, ed.), LNCS, vol. 5157, Springer, 2008, pp. 75–92.

[315] Z.-T. Jiang, W.-L. Xu, and Y.-M. Wang, *Polynomial analysis of DH secrete key and bit security*, Wuhan University Journal of Natural Sciences **10** (2005), no. 1, 239–242.

[316] A. Joux, *A one round protocol for tripartite Diffie-Hellman*, ANTS IV (W. Bosma, ed.), LNCS, vol. 1838, Springer, 2000, pp. 385–393.

[317] ______, *Algorithmic cryptanalysis*, Chapman & Hall/CRC, 2009.

[318] A. Joux and R. Lercier, *The function field sieve in the medium prime case*, EUROCRYPT 2006 (S. Vaudenay, ed.), LNCS, vol. 4004, Springer, 2006, pp. 254–270.

[319] A. Joux, R. Lercier, N. P. Smart, and F. Vercauteren, *The number field sieve in the medium prime case*, CRYPTO 2006 (C. Dwork, ed.), LNCS, vol. 4117, Springer, 2006, pp. 326–344.

[320] M. Joye and G. Neven, *Identity-based cryptography*, Cryptology and Information Security, vol. 2, IOS Press, 2008.

[321] M. Joye and S.-M. Yen, *Optimal left-to-right binary signed-digit recoding*, IEEE Trans. Computers **49** (2000), no. 7, 740–748.

[322] M. J. Jacobson Jr., N. Koblitz, J. H. Silverman, A. Stein, and E. Teske, *Analysis of the Xedni calculus attack*, Des. Codes Crypt. **20** (2000), no. 1, 41–64.

[323] M. J. Jacobson Jr. and A. J. van der Poorten, *Computational aspects of NUCOMP*, ANTS V (C. Fieker and D. R. Kohel, eds.), LNCS, vol. 2369, Springer, 2002, pp. 120–133.

[324] C. S. Jutla, *On finding small solutions of modular multivariate polynomial equations*, EUROCRYPT 1998 (K. Nyberg, ed.), LNCS, vol. 1403, Springer, 1998, pp. 158–170.

[325] M. Kaib and H. Ritter, *Block reduction for arbitrary norms*, Technical Report, Universität Frankfurt am Main, 1994.

[326] M. Kaib and C.-P. Schnorr, *The generalized Gauss reduction algorithm*, Journal of Algorithms **21** (1996), no. 3, 565–578.

[327] B. S. Kaliski Jr., *Elliptic curves and cryptography: A pseudorandom bit generator and other tools*, Ph.D. thesis, MIT, 1988.

[328] W. van der Kallen, *Complexity of the Havas, Majewski, Matthews LLL Hermite normal form algorithm*, Journal of Symbolic Computation **30** (2000), no. 3, 329–337.

[329] R. Kannan, *Improved algorithms for integer programming and related lattice problems*, Symposium on the Theory of Computing (STOC), ACM, 1983, pp. 193–206.

[330] ______, *Minkowski's convex body theorem and integer programming*, Mathematics of Operations Research **12** (1987), no. 3, 415–440.

[331] R. Kannan and A. Bachem, *Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix*, SIAM J. Comput. **8** (1979), 499–507.

[332] M. Katagi, T. Akishita, I. Kitamura, and T. Takagi, *Some improved algorithms for hyperelliptic curve cryptosystems using degenerate divisors*, ICISC 2004 (C. Park and S. Chee, eds.), LNCS, vol. 3506, Springer, 2004, pp. 296–312.

[333] M. Katagi, I. Kitamura, T. Akishita, and T. Takagi, *Novel efficient implementations of hyperelliptic curve cryptosystems using degenerate divisors*, WISA 2004 (C.-H. Lim and M. Yung, eds.), LNCS, vol. 3325, Springer, 2004, pp. 345–359.

[334] J. Katz and Y. Lindell, *Introduction to modern cryptography*, Chapman & Hall/CRC, 2008.

[335] E. Kiltz and G. Neven, *Identity-based signatures*, Identity-Based Cryptography (M. Joye and G. Neven, eds.), Cryptology and Information Security Series, vol. 2, IOS Press, 2008, pp. 31–44.

[336] J. H. Kim, R. Montenegro, Y. Peres, and P. Tetali, *A birthday paradox for Markov chains, with an optimal bound for collision in the Pollard rho algorithm for discrete logarithm*, ANTS VIII (A. J. van der Poorten and A. Stein, eds.), LNCS, vol. 5011, Springer, 2008, pp. 402–415.

[337] J. H. Kim, R. Montenegro, and P. Tetali, *Near optimal bounds for collision in Pollard rho for discrete log*, Foundations of Computer Science (FOCS), IEEE, 2007, pp. 215–223.

[338] S. Kim and J.-H. Cheon, *A parameterized splitting system and its application to the discrete logarithm problem with low Hamming weight product exponents*, PKC 2008 (R. Cramer, ed.), LNCS, vol. 4939, Springer, 2008, pp. 328–343.

[339] B. King, *A point compression method for elliptic curves defined over GF(2^n)*, PKC 2004 (F. Bao, R. H. Deng, and J. Zhou, eds.), LNCS, vol. 2947, Springer, 2004, pp. 333–345.

[340] J. F. C. Kingman and S. J. Taylor, *Introduction to measure theory and probability*, Cambridge, 1966.

[341] P. N. Klein, *Finding the closest lattice vector when it's unusually close*, Symposium on Discrete Algorithms (SODA), ACM/SIAM, 2000, pp. 937–941.

[342] E. W. Knudsen, *Elliptic scalar multiplication using point halving*, ASIACRYPT 1999 (K.-Y. Lam, E. Okamoto, and C. Xing, eds.), LNCS, vol. 1716, Springer, 1999, pp. 135–149.

[343] D. E. Knuth, *Art of computer programming, Volume 2: semi-numerical algorithms*, 3rd ed., Addison-Wesley, 1997.

[344] N. Koblitz, *Elliptic curve cryptosystems*, Math. Comp. **48** (1987), no. 177, 203–209.

[345] ______, *Primality of the number of points on an elliptic curve over a finite field*, Pacific J. Math. **131** (1988), no. 1, 157–165.

[346] ______, *Hyperelliptic cryptosystems*, J. Crypt. **1** (1989), 139–150.

[347] ______, *CM curves with good cryptographic properties*, CRYPTO 1991 (J. Feigenbaum, ed.), LNCS, vol. 576, Springer, 1992, pp. 279–287.

[348] ______, *A course in number theory and cryptography*, 2nd ed., GTM 114, Springer, 1994.

[349] C. K. Koç and T. Acar, *Montgomery multplication in GF(2^k)*, Des. Codes Crypt. **14** (1998), no. 1, 57–69.

[350] D. R. Kohel, *Endomorphism rings of elliptic curves over finite fields*, Ph.D. thesis, University of California, Berkeley, 1996.

[351] ______, *Constructive and destructive facets of torus-based cryptography*, Preprint, 2004.

[352] D. R. Kohel and I. E. Shparlinski, *On exponential sums and group generators for elliptic curves over finite fields*, ANTS IV (W. Bosma, ed.), LNCS, vol. 1838, Springer, 2000, pp. 395–404.

[353] S. Kozaki, T. Kutsuma, and K. Matsuo, *Remarks on Cheon's algorithms for pairing-related problems*, Pairing 2007 (T. Takagi, T. Okamoto, E. Okamoto, and T. Okamoto, eds.), LNCS, vol. 4575, Springer, 2007, pp. 302–316.

[354] M. Kraitchik, *Théorie des nombres, Vol. 1*, Gauthier-Villars, Paris, 1922.

[355] F. Kuhn and R. Struik, *Random walks revisited: Extensions of Pollard's rho algorithm for computing multiple discrete logarithms*, SAC 2001 (S. Vaudenay and A. M. Youssef, eds.), LNCS, vol. 2259, Springer, 2001, pp. 212–229.

[356] R. M. Kuhn, *Curves of genus 2 with split Jacobian*, Trans. Amer. Math. Soc. **307** (1988), no. 1, 41–49.

[357] R. Kumar and D. Sivakumar, *Complexity of SVP – a reader's digest*, SIGACT News Complexity Theory Column 32 (2001), 13.

[358] N. Kunihiro and K. Koyama, *Equivalence of counting the number of points on elliptic curve over the ring Z_n and factoring n*, EUROCRYPT 1998 (K. Nyberg, ed.), LNCS, vol. 1403, Springer, 1998, pp. 47–58.

[359] K. Kurosawa and Y. Desmedt, *A new paradigm of hybrid encryption scheme*, CRYPTO 2004 (M. K. Franklin, ed.), LNCS, vol. 3152, Springer, 2004, pp. 426–442.

[360] J. C. Lagarias, *Knapsack public key cryptosystems and diophantine approximation*, CRYPTO 1983 (D. Chaum, ed.), Plenum Press, 1984, pp. 3–23.

[361] J. C. Lagarias, H. W. Lenstra Jr., and C.-P. Schnorr, *Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice*, Combinatorica **10** (1990), no. 4, 333–348.

[362] J. C. Lagarias and A. M. Odlyzko, *Solving low-density subset sum problems*, J. ACM **32** (1985), no. 1, 229–246.

[363] C. Lanczos, *Solution of systems of linear equations by minimized iterations*, J. Res. Nat. Bureau of Standards **49** (1952), 33–53.

[364] S. Lang, *Introduction to algebraic geometry*, Wiley, 1964.

[365] ______, *Algebraic number theory*, GTM, vol. 110, Springer, 1986.

[366] ______, *Elliptic functions*, 2nd ed., GTM, vol. 112, Springer, 1987.

[367] ______, *Algebra*, 3rd ed., Addison-Wesley, 1993.

[368] T. Lange, *Koblitz curve cryptosystems*, Finite Fields Appl. **11** (2005), no. 2, 200–229.

[369] E. Lee, H.-S. Lee, and C.-M. Park, *Efficient and generalized pairing computation on abelian varieties*, IEEE Trans. Information Theory **55** (2009), no. 4, 1793–1803.

[370] A. K. Lenstra, *Factorization of polynomials*, Computational methods in number theory (H. W. Lenstra Jr. and R. Tijdeman, eds.), Mathematical Center Tracts 154, Mathematisch Centrum Amsterdam, 1984, pp. 169–198.

[371] ______, *Integer factoring*, Des. Codes Crypt. **19** (2000), no. 2/3, 101–128.

[372] A. K. Lenstra and H. W. Lenstra Jr., *The development of the number field sieve*, LNM, vol. 1554, Springer, 1993.

[373] A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515–534.

[374] A. K. Lenstra and I. E. Shparlinski, *Selective forgery of RSA signatures with fixed-pattern padding*, PKC 2002 (D. Naccache and P. Paillier, eds.), LNCS, vol. 2274, Springer, 2002, pp. 228–236.

[375] A. K. Lenstra and E. R. Verheul, *The XTR public key system*, CRYPTO 2000 (M. Bellare, ed.), LNCS, vol. 1880, Springer, 2000, pp. 1–19.

[376] ———, *Fast irreducibility and subgroup membership testing in XTR*, PKC 2001 (K. Kim, ed.), LNCS, vol. 1992, Springer, 2001, pp. 73–86.

[377] H. W. Lenstra Jr., *Factoring integers with elliptic curves*, Annals of Mathematics **126** (1987), no. 3, 649–673.

[378] ———, *Elliptic curves and number theoretic algorithms*, Proc. International Congr. Math., Berkeley 1986, AMS, 1988, pp. 99–120.

[379] ———, *Finding isomorphisms between finite fields*, Math. Comp. **56** (1991), no. 193, 329–347.

[380] H. W. Lenstra Jr., J. Pila, and C. Pomerance, *A hyperelliptic smoothness test I*, Phil. Trans. R. Soc. Lond. A **345** (1993), 397–408.

[381] H. W. Lenstra Jr. and C. Pomerance, *A rigorous time bound for factoring integers*, J. Amer. Math. Soc. **5** (1992), no. 3, 483–516.

[382] R. Lercier, *Computing isogenies in F_{2^n}*, ANTS II (H. Cohen, ed.), LNCS, vol. 1122, Springer, 1996, pp. 197–212.

[383] R. Lercier and F. Morain, *Algorithms for computing isogenies between elliptic curves*, Computational Perspectives on Number Theory (D. A. Buell and J. T. Teitelbaum, eds.), Studies in Advanced Mathematics, vol. 7, AMS, 1998, pp. 77–96.

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

[385] G. Leurent and P. Q. Nguyen, *How risky is the random oracle model?*, CRYPTO 2009 (S. Halevi, ed.), LNCS, vol. 5677, Springer, 2009, pp. 445–464.

[386] K.-Z. Li and F. Oort, *Moduli of supersingular abelian varieties*, LNM, vol. 1680, Springer, 1998.

[387] W.-C. Li, M. Näslund, and I. E. Shparlinski, *Hidden number problem with the trace and bit security of XTR and LUC*, CRYPTO 2002 (M. Yung, ed.), LNCS, vol. 2442, Springer, 2002, pp. 433–448.

[388] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge, 1994.

[389] ———, *Finite fields*, Cambridge, 1997.

[390] R. Lindner and C. Peikert, *Better key sizes (and attacks) for LWE-based encryption*, CT-RSA 2011 (A. Kiayias, ed.), LNCS, vol. 6558, Springer, 2011, pp. 1–23.

[391] J. H. van Lint, *Introduction to coding theory*, 3rd ed., GTM, vol. 86, Springer, 1999.

[392] P. Lockhart, *On the discriminant of a hyperelliptic curve*, Trans. Amer. Math. Soc. **342** (1994), no. 2, 729–752.

[393] D. L. Long and A. Wigderson, *The discrete logarithm hides O(log n) bits*, SIAM J. Comput. **17** (1988), no. 2, 363–372.

[394] D. Lorenzini, *An invitation to arithmetic geometry*, Graduate Studies in Mathematics, vol. 106, AMS, 1993.

[395] L. Lovász, *An algorithmic theory of numbers, graphs and convexity*, SIAM, 1986.

[396] L. Lovász and H. E. Scarf, *The generalized basis reduction algorithm*, Mathematics of Operations Research **17** (1992), no. 3, 751–764.

[397] R. Lovorn Bender and C. Pomerance, *Rigorous discrete logarithm computations in finite fields via smooth polynomials*, Computational Perspectives on Number Theory (D. A. Buell and J. T. Teitelbaum, eds.), Studies in Advanced Mathematics, vol. 7, AMS, 1998, pp. 221–232.

[398] M. Luby, *Pseudorandomness and cryptographic applications*, Princeton, 1996.

[399] H. Lüneburg, *On a little but useful algorithm*, AAECC-3, 1985 (J. Calmet, ed.), LNCS, vol. 229, Springer, 1986, pp. 296–301.

[400] S. Martín Molleví, P. Morillo, and J. L. Villar, *Computing the order of points on an elliptic curve modulo N is as difficult as factoring N*, Appl. Math. Lett. **14** (2001), no. 3, 341–346.

[401] C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences I: Measure of pseudorandomness, the Legendre symbol*, Acta Arith. **82** (1997), 365–377.

[402] U. M. Maurer, *Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms*, CRYPTO 1994 (Y. Desmedt, ed.), LNCS, vol. 839, Springer, 1994, pp. 271–281.

[403] ______, *Fast generation of prime numbers and secure public-key cryptographic parameters*, J. Crypt. **8** (1995), no. 3, 123–155.

[404] ______, *Abstract models of computation in cryptography*, IMA Int. Conf. (N. P. Smart, ed.), LNCS, vol. 3796, Springer, 2005, pp. 1–12.

[405] U. M. Maurer and S. Wolf, *Diffie-Hellman oracles*, CRYPTO 1996 (N. Koblitz, ed.), LNCS, vol. 1109, Springer, 1996, pp. 268–282.

[406] ______, *On the complexity of breaking the Diffie-Hellman protocol*, Technical Report 244, Institute for Theoretical Computer Science, ETH Zurich, 1996.

[407] ______, *Lower bounds on generic algorithms in groups*, EUROCRYPT 1998 (K. Nyberg, ed.), LNCS, vol. 1403, Springer, 1998, pp. 72–84.

[408] ______, *The relationship between breaking the Diffie-Hellman protocol and computing discrete logarithms*, SIAM J. Comput. **28** (1999), no. 5, 1689–1721.

[409] ______, *The Diffie-Hellman protocol*, Des. Codes Crypt. **19** (2000), no. 2/3, 147–171.

[410] A. May, *New RSA vulnerabilities using lattice reduction methods*, Ph.D. thesis, Paderborn, 2003.

[411] ______, *Using LLL-reduction for solving RSA and factorization problems: A survey*, The LLL Algorithm (P. Q. Nguyen and B. Vallée, eds.), Springer, 2010, pp. 315–348.

[412] A. May and J. H. Silverman, *Dimension reduction methods for convolution modular lattices*, Cryptography and Lattices (CaLC) (J. H. Silverman, ed.), LNCS, Springer, 2001, pp. 110–125.

[413] J. F. McKee, *Subtleties in the distribution of the numbers of points on elliptic curves over a finite prime field*, J. London Math. Soc. **59** (1999), no. 2, 448–460.

[414] J. F. McKee and R. G. E. Pinch, *Further attacks on server-aided RSA cryptosystems*, unpublished manuscript, 1998.

[415] W. Meier and O. Staffelbach, *Efficient multiplication on certain non-supersingular elliptic curves*, CRYPTO 1992 (E. F. Brickell, ed.), LNCS, vol. 740, Springer, 1993, pp. 333–344.

[416] A. Menezes and S. A. Vanstone, *The implementation of elliptic curve cryptosystems*, AUSCRYPT 1990 (J. Seberry and J. Pieprzyk, eds.), LNCS, vol. 453, Springer, 1990, pp. 2–13.

[417] A. J. Menezes, T. Okamoto, and S. A. Vanstone, *Reducing elliptic curve logarithms to a finite field*, IEEE Trans. Inf. Theory **39** (1993), no. 5, 1639–1646.

[418] A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone, *Handbook of applied cryptography*, CRC Press, 1996.

[419] J.-F. Mestre, *La méthode des graphes. exemples et applications*, Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata, 1986), Nagoya Univ., 1986, pp. 217–242.

[420] J.-F. Mestre, *Construction de courbes de genre 2 à partir de leurs modules*, Effective methods in algebraic geometry (T. Mora and C. Traverso, eds.), Progress in Mathematics, Birkhäuser, 1991, pp. 313–334.

[421] D. Micciancio, *Improving lattice based cryptosystems using the Hermite normal form*, Cryptography and Lattices (CaLC) (J. H. Silverman, ed.), LNCS, vol. 2146, Springer, 2001, pp. 126–145.

[422] D. Micciancio and S. Goldwasser, *Complexity of lattice problems: A cryptographic perspective*, Kluwer, 2002.

[423] D. Micciancio and O. Regev, *Lattice-based cryptography*, Post Quantum Cryptography (D. J. Bernstein, J. Buchmann, and E. Dahmen, eds.), Springer, 2009, pp. 147–191.

[424] D. Micciancio and P. Voulgaris, *Faster exponential time algorithms for the shortest vector problem*, SODA (M. Charikar, ed.), SIAM, 2010, pp. 1468–1480.

[425] D. Micciancio and B. Warinschi, *A linear space algorithm for computing the Hermite normal form*, ISSAC, 2001, pp. 231–236.

[426] S. D. Miller and R. Venkatesan, *Spectral analysis of Pollard rho collisions*, ANTS VII (F. Hess, S. Pauli, and M. E. Pohst, eds.), LNCS, vol. 4076, Springer, 2006, pp. 573–581.

[427] V. S. Miller, *Short programs for functions on curves*, Unpublished manuscript, 1986.

[428] ———, *Use of elliptic curves in cryptography*, CRYPTO 1985 (H. C. Williams, ed.), LNCS, vol. 218, Springer, 1986, pp. 417–426.

[429] ———, *The Weil pairing, and its efficient calculation*, J. Crypt. **17** (2004), no. 4, 235–261.

[430] A. Miyaji, T. Ono, and H. Cohen, *Efficient elliptic curve exponentiation*, ICICS 1997 (Y. Han, T. Okamoto, and S. Qing, eds.), LNCS, vol. 1334, Springer, 1997, pp. 282–291.

[431] B. Möller, *Algorithms for multi-exponentiation*, SAC 2001 (S. Vaudenay and A. M. Youssef, eds.), LNCS, vol. 2259, Springer, 2001, pp. 165–180.

[432] ______, *Improved techniques for fast exponentiation*, ICISC 2002 (P.-J. Lee and C.-H. Lim, eds.), LNCS, vol. 2587, Springer, 2003, pp. 298–312.

[433] ______, *Fractional windows revisited: Improved signed-digit representations for efficient exponentiation*, ICISC 2004 (C. Park and S. Chee, eds.), LNCS, vol. 3506, Springer, 2005, pp. 137–153.

[434] R. Montenegro and P. Tetali, *How long does it take to catch a wild kangaroo?*, Symposium on Theory of Computing (STOC), 2009, pp. 553–559.

[435] P. L. Montgomery, *Modular multiplication without trial division*, Math. Comp. **44** (1985), no. 170, 519–521.

[436] ______, *Speeding the Pollard and elliptic curve methods of factorization*, Math. Comp. **48** (1987), no. 177, 243–264.

[437] F. Morain and J.-L. Nicolas, *On Cornacchia's algorithm for solving the Diophantine equation $u^2 + dv^2 = m$*, Preprint, 1990.

[438] F. Morain and J. Olivos, *Speeding up the computations on an elliptic curve using addition-subtraction chains*, Theoretical Informatics and Applications, vol. 24, 1990, pp. 531–543.

[439] C. J. Moreno, *Algebraic curves over finite fields*, Cambridge, 1991.

[440] W. H. Mow, *Universal lattice decoding: principle and recent advances*, Wireless Communications and Mobile Computing **3** (2003), no. 5, 553–569.

[441] J. A. Muir and D. R. Stinson, *New minimal weight representations for left-to-right window methods*, CT-RSA 2005 (A. Menezes, ed.), LNCS, vol. 3376, Springer, 2005, pp. 366–383.

[442] ______, *Minimality and other properties of the width-w nonadjacent form*, Math. Comp. **75** (2006), no. 253, 369–384.

[443] V. Müller, *Fast multiplication on elliptic curves over small fields of characteristic two*, J. Crypt. **11** (1998), no. 4, 219–234.

[444] D. Mumford, *Abelian varieties*, Oxford, 1970.

[445] ______, *Tata lectures on theta II*, Progess in Mathematics, vol. 43, Birkhäuser, 1984.

[446] M. R. Murty, *Ramanujan graphs*, J. Ramanujan Math. Soc. **18** (2003), no. 1, 1–20.

[447] R. Murty and I. E. Shparlinski, *Group structure of elliptic curves over finite fields and applications*, Topics in Geometry, Coding Theory and Cryptography (A. Garcia and H. Stichtenoth, eds.), Springer-Verlag, 2006, pp. 167–194.

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

[449] D. Naccache, D. M'Raïhi, S. Vaudenay, and D. Raphaeli, *Can D.S.A. be improved? Complexity trade-offs with the digital signature standard*, EUROCRYPT 1994 (A. De Santis, ed.), LNCS, vol. 950, Springer, 1995, pp. 77–85.

[450] D. Naccache and I. E. Shparlinski, *Divisibility, smoothness and cryptographic applications*, Algebraic Aspects of Digital Communications (T. Shaska and E. Hasimaj, eds.), NATO Science for Peace and Security Series, vol. 24, IOS Press, 2009, pp. 115–173.

[451] N.Courtois, M. Finiasz, and N. Sendrier, *How to achieve a McEliece-based digital signature scheme*, ASIACRYPT 2001 (C. Boyd, ed.), LNCS, vol. 2248, Springer, 2001, pp. 157–174.

[452] V. I. Nechaev, *Complexity of a determinate algorithm for the discrete logarithm*, Mathematical Notes **55** (1994), no. 2, 165–172.

[453] G. Neven, N. P. Smart, and B. Warinschi, *Hash function requirements for Schnorr signatures*, J. Math. Crypt. **3** (2009), no. 1, 69–87.

[454] P. Nguyen and D. Stehlé, *Floating-point LLL revisited*, EUROCRYPT 2005 (R. Cramer, ed.), LNCS, vol. 3494, Springer, 2005, pp. 215–233.

[455] ———, *Low-dimensional lattice basis reduction revisited*, ACM Transactions on Algorithms **5** (2009), no. 4:46, 1–48.

[456] P. Q. Nguyen, *Public key cryptanalysis*, Recent Trends in Cryptography (I. Luengo, ed.), AMS, 2009, pp. 67–119.

[457] P. Q. Nguyen and O. Regev, *Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures*, EUROCRYPT 2006 (S. Vaudenay, ed.), LNCS, vol. 4004, Springer, 2006, pp. 271–288.

[458] ———, *Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures*, J. Crypt. **22** (2009), no. 2, 139–160.

[459] P. Q. Nguyen and I. E. Shparlinski, *The insecurity of the digital signature algorithm with partially known nonces*, J. Crypt. **15** (2002), no. 3, 151–176.

[460] ———, *The insecurity of the elliptic curve digital signature algorithm with partially known nonces*, Des. Codes Crypt. **30** (2003), no. 2, 201–217.

[461] P. Q. Nguyen and D. Stehlé, *Low-dimensional lattice basis reduction revisited*, ANTS VI (D. A. Buell, ed.), LNCS, vol. 3076, Springer, 2004, pp. 338–357.

[462] P. Q. Nguyen and J. Stern, *Lattice reduction in cryptology: An update*, ANTS IV (W. Bosma, ed.), LNCS, vol. 1838, Springer, 2000, pp. 85–112.

[463] ———, *The two faces of lattices in cryptology*, Cryptography and Lattices (CaLC) (J. H. Silverman, ed.), LNCS, vol. 2146, Springer, 2001, pp. 146–180.

[464] P. Q. Nguyen and B. Vallée, *The LLL algorithm: Survey and applications*, Information Security and Cryptography, Springer, 2010.

[465] P. Q. Nguyen and T. Vidick, *Sieve algorithms for the shortest vector problem are practical*, J. Math. Crypt. **2** (2008), no. 2, 181–207.

[466] H. Niederreiter, *A new efficient factorization algorithm for polynomials over small finite fields*, Applicable Algebra in Engineering, Communication and Computing **4** (1993), no. 2, 81–87.

[467] G. Nivasch, *Cycle detection using a stack*, Inf. Process. Lett. **90** (2004), no. 3, 135–140.

[468] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An introduction to the theory of numbers*, 5th ed., Wiley, 1991.

[469] A. M. Odlyzko, *Discrete logarithms in finite fields and their cryptographic significance*, EUROCRYPT 1984 (T. Beth, N. Cot, and I. Ingemarsson, eds.), LNCS, vol. 209, Springer, 1985, pp. 224–314.

[470] ______, *The rise and fall of knapsack cryptosystems*, Cryptology and Computational Number Theory (C. Pomerance, ed.), Proc. Symp. Appl. Math., vol. 42, Am. Math. Soc., 1990, pp. 75–88.

[471] T. Okamoto and S. Uchiyama, *A new public-key cryptosystem as secure as factoring*, EUROCRYPT 1998 (K. Nyberg, ed.), LNCS, vol. 1403, Springer, 1998, pp. 308–318.

[472] P. C. van Oorschot and M. J. Wiener, *On Diffie-Hellman key agreement with short exponents*, EUROCRYPT 1996 (U. M. Maurer, ed.), LNCS, vol. 1070, Springer, 1996, pp. 332–343.

[473] ______, *Parallel collision search with cryptanalytic applications*, J. Crypt. **12** (1999), no. 1, 1–28.

[474] P. Paillier, *Public-key cryptosystems based on composite degree residuosity classes*, EUROCRYPT 1999 (J. Stern, ed.), LNCS, vol. 1592, Springer, 1999, pp. 223–238.

[475] ______, *Impossibility proofs for RSA signatures in the standard model*, CT-RSA 2007 (M. Abe, ed.), LNCS, vol. 4377, Springer, 2007, pp. 31–48.

[476] P. Paillier and D. Vergnaud, *Discrete-log-based signatures may not be equivalent to discrete log*, ASIACRYPT 2005 (B. K. Roy, ed.), LNCS, vol. 3788, Springer, 2005, pp. 1–20.

[477] P. Paillier and J. L. Villar, *Trading one-wayness against chosen-ciphertext security in factoring-based encryption*, ASIACRYPT 2006 (X. Lai and K. Chen, eds.), LNCS, vol. 4284, Springer, 2006, pp. 252–266.

[478] S. Patel and G. S. Sundaram, *An efficient discrete log pseudo random generator*, CRYPTO 1998 (H. Krawczyk, ed.), LNCS, vol. 1462, Springer, 1998, pp. 304–317.

[479] S. Paulus and H.-G. Rück, *Real and imaginary quadratic representations of hyperelliptic function fields*, Math. Comp. **68** (1999), no. 227, 1233–1241.

[480] R. Peralta, *Simultaneous security of bits in the discrete log*, EUROCRYPT 1985 (F. Pichler, ed.), LNCS, vol. 219, Springer, 1986, pp. 62–72.

[481] A. K. Pizer, *Ramanujan graphs*, Computational Perspectives on Number Theory (D. A. Buell and J. T. Teitelbaum, eds.), Studies in Advanced Mathematics, vol. 7, AMS, 1998, pp. 159–178.

[482] S. Pohlig and M. Hellman, *An improved algorithm for computing logarithms over GF(p) and its cryptographic significance*, IEEE Trans. Inf. Theory **24** (1978), 106–110.

[483] D. Pointcheval and J. Stern, *Security arguments for digital signatures and blind signatures*, J. Crypt. **13** (2000), no. 3, 361–396.

[484] D. Pointcheval and S. Vaudenay, *On provable security for digital signature algorithms*, Technical report LIENS 96-17, École Normale Supérieure, 1996.

[485] J. M. Pollard, *Theorems on factorisation and primality testing*, Proc. Camb. Phil. Soc. **76** (1974), 521–528.

[486] ———, *A Monte Carlo method for factorization*, BIT **15** (1975), 331–334.

[487] ———, *Monte Carlo methods for index computation (mod p)*, Math. Comp. **32** (1978), no. 143, 918–924.

[488] ———, *Kangaroos, Monopoly and discrete logarithms*, J. Crypt. **13** (2000), no. 4, 437–447.

[489] C. Pomerance, *A tale of two sieves*, Notices of the Amer. Math. Soc. **43** (1996), 1473–1485.

[490] V. R. Pratt, *Every prime has a succinct certificate*, SIAM J. Comput. **4** (1974), no. 3, 214–220.

[491] X. Pujol and D. Stehlé, *Rigorous and efficient short lattice vectors enumeration*, ASIACRYPT 2008 (J. Pieprzyk, ed.), LNCS, vol. 5350, Springer, 2008, pp. 390–405.

[492] G. Qiao and K.-Y. Lam, *RSA signature algorithm for microcontroller implementation*, CARDIS 1998 (J.-J. Quisquater and B. Schneier, eds.), LNCS, vol. 1820, Springer, 2000, pp. 353–356.

[493] J. J. Quisquater and C. Couvreur, *Fast decipherment algorithm for RSA public-key cryptosystem*, Electronics Letters (1982), no. 21, 905–907.

[494] M.O. Rabin, *Digitalized signatures and public-key functions as intractable as factorization*, Tech. Report MIT/LCS/TR-212, MIT Laboratory for Computer Science, 1979.

[495] J.-F. Raymond and A. Stiglic, *Security issues in the Diffie-Hellman key agreement protocol*, Preprint, 2000.

[496] O. Regev, *The learning with errors problem (Invited survey)*, 25th Annual IEEE Conference on Computational Complexity, IEEE, 2010, pp. 191–204.

[497] M. Reid, *Undergraduate algebraic geometry*, Cambridge, 1988.

[498] ———, *Graded rings and varieties in weighted projective space*, Chapter of unfinished book, 2002.

[499] G. Reitwiesner, *Binary arithmetic*, Advances in Computers **1** (1960), 231–308.

[500] P. Rogaway, *Formalizing human ignorance*, VIETCRYPT 2006 (P. Q. Nguyen, ed.), LNCS, vol. 4341, Springer, 2006, pp. 211–228.

[501] P. Roquette, *Abschätzung der Automorphismenanzahl von Funktionenkörpern bei Primzahlcharakteristik*, Math. Zeit. **117** (1970), 157–163.

[502] S. Ross, *A first course in probability (6th ed.)*, Prentice Hall, 2001.

[503] K. Rubin and A. Silverberg, *Torus-based cryptography*, CRYPTO 2003 (D. Boneh, ed.), LNCS, vol. 2729, Springer, 2003, pp. 349–365.

[504] ______, *Compression in finite fields and torus-based cryptography*, SIAM J. Comput. **37** (2008), no. 5, 1401–1428.

[505] H.-G. Rück, *A note on elliptic curves over finite fields*, Math. Comp. **49** (1987), no. 179, 301–304.

[506] ______, *On the discrete logarithm in the divisor class group of curves*, Math. Comp. **68** (1999), no. 226, 805–806.

[507] A. Rupp, G. Leander, E. Bangerter, A. W. Dent, and A.-R. Sadeghi, *Sufficient conditions for intractability over black-box groups: Generic lower bounds for generalized DL and DH problems*, ASIACRYPT 2008 (J. Pieprzyk, ed.), LNCS, vol. 5350, Springer, 2008, pp. 489–505.

[508] A.-R. Sadeghi and M. Steiner, *Assumptions related to discrete logarithms: Why subtleties make a real difference*, EUROCRYPT 2001 (B. Pfitzmann, ed.), LNCS, vol. 2045, Springer, 2001, pp. 244–261.

[509] R. Sakai, K. Ohgishi, and M. Kasahara, *Cryptosystems based on pairing*, Symposium on Cryptography and Information Security (SCIS), Okinawa, Japan, 2000.

[510] A. Sárközy and C. L. Stewart, *On pseudorandomness in families of sequences derived from the Legendre symbol*, Periodica Math. Hung. **54** (2007), no. 2, 163–173.

[511] T. Satoh, *On generalization of Cheon's algorithm*, Cryptology ePrint Archive, Report 2009/058, 2009.

[512] T. Satoh and K. Araki, *Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves*, Comment. Math. Univ. St. Paul. **47** (1998), no. 1, 81–92.

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

[514] A. Schinzel and M. Skałba, *On equations $y^2 = x^n + k$ in a finite field*, Bull. Polish Acad. Sci. Math. **52** (2004), no. 3, 223–226.

[515] O. Schirokauer, *Using number fields to compute logarithms in finite fields*, Math. Comp. **69** (2000), no. 231, 1267–1283.

[516] ______, *The special function field sieve*, SIAM J. Discrete Math **16** (2002), no. 1, 81–98.

[517] ______, *The impact of the number field sieve on the discrete logarithm problem in finite fields*, Algorithmic Number Theory (J. Buhler and P. Stevenhagen, eds.), MSRI publications, vol. 44, Cambridge, 2008, pp. 397–420.

[518] ______, *The number field sieve for integers of low weight*, Math. Comp. **79** (2010), no. 269, 583–602.

[519] O. Schirokauer, D. Weber, and T. F. Denny, *Discrete logarithms: The effectiveness of the index calculus method*, ANTS II (H. Cohen, ed.), LNCS, vol. 1122, Springer, 1996, pp. 337–361.

[520] K. Schmidt-Samoa, O. Semay, and T. Takagi, *Analysis of fractional window recoding methods and their application to elliptic curve cryptosystems*, IEEE Trans. Computers **55** (2006), no. 1, 48–57.

[521] C.-P. Schnorr, *A hierarchy of polynomial time lattice basis reduction algorithms*, Theor. Comput. Sci. **53** (1987), 201–224.

[522] ———, *Efficient identification and signatures for smart cards*, CRYPTO 1989 (G. Brassard, ed.), LNCS, vol. 435, Springer, 1990, pp. 239–252.

[523] ———, *Efficient signature generation by smart cards*, J. Crypt. **4** (1991), no. 3, 161–174.

[524] ———, *Security of almost all discrete log bits*, Electronic Colloquium on Computational Complexity (ECCC) **5** (1998), no. 33, 1–13.

[525] ———, *Progress on LLL and lattice reduction*, The LLL Algorithm (P. Q. Nguyen and B. Vallée, eds.), Springer, 2010, pp. 145–178.

[526] C.-P. Schnorr and M. Euchner, *Lattice basis reduction: Improved practical algorithms and solving subset sum problems*, Math. Program. **66** (1994), 181–199.

[527] C.-P. Schnorr and H. W. Lenstra Jr., *A Monte Carlo factoring algorithm with linear storage*, Math. Comp. **43** (1984), no. 167, 289–311.

[528] R. Schoof, *Elliptic curves over finite fields and the computation of square roots* (mod *) p*, Math. Comp. **44** (1985), no. 170, 483–494.

[529] ———, *Nonsingular plane cubic curves over finite fields*, J. Combin. Theory Ser. A **46** (1987), 183–211.

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

[531] A. Schrijver, *Theory of linear and integer programming*, Wiley, 1986.

[532] R. Schroeppel, H. K. Orman, S. W. O'Malley, and O. Spatscheck, *Fast key exchange with elliptic curve systems*, CRYPTO 1995 (D. Coppersmith, ed.), LNCS, vol. 963, Springer, 1995, pp. 43–56.

[533] E. Schulte-Geers, *Collision search in a random mapping: Some asymptotic results*, Presentation at ECC 2000, Essen, Germany, 2000.

[534] M. Scott, *Faster pairings using an elliptic curve with an efficient endomorphism*, INDOCRYPT 2005 (S. Maitra, C. E. V. Madhavan, and R. Venkatesan, eds.), LNCS, vol. 3797, Springer, 2005, pp. 258–269.

[535] R. Sedgewick, T. G. Szymanski, and A. C.-C. Yao, *The complexity of finding cycles in periodic functions*, SIAM J. Comput. **11** (1982), no. 2, 376–390.

[536] B. I. Selivanov, *On waiting time in the scheme of random allocation of coloured particles*, Discrete Math. Appl. **5** (1995), no. 1, 73–82.

[537] I. A. Semaev, *Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p*, Math. Comp. **67** (1998), no. 221, 353–356.

[538] ______, *A 3-dimensional lattice reduction algorithm*, Cryptography and Lattices (CaLC) (J. H. Silverman, ed.), LNCS, vol. 2146, Springer, 2001, pp. 181–193.

[539] ______, *Summation polynomials and the discrete logarithm problem on elliptic curves*, Cryptology ePrint Archive, Report 2004/031, 2004.

[540] G. Seroussi, *Compact representation of elliptic curve points over F_{2^n}*, Hewlett-Packard Labs technical report HPL-98-94, 1998.

[541] J.-P. Serre, *Sur la topologie des variétés algébriques en charactéristique p*, Symp. Int. Top. Alg., Mexico, 1958, pp. 24–53.

[542] ______, *Local fields*, GTM, vol. 67, Springer, 1979.

[543] I. R. Shafarevich, *Basic algebraic geometry*, 2nd ed., Springer, 1995.

[544] J. O. Shallit, *A primer on balanced binary representations*, Preprint, 1992.

[545] A. Shallue and C. E. van de Woestijne, *Construction of rational points on elliptic curves over finite fields*, ANTS VII (F. Hess, S. Pauli, and M. E. Pohst, eds.), LNCS, vol. 4076, Springer, 2006, pp. 510–524.

[546] A. Shamir, *A polynomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem*, IEEE Trans. Inf. Theory **30** (1984), no. 5, 699–704.

[547] ______, *Identity based cryptosystems and signature schemes*, CRYTO 1984 (G. R. Blakley and D. Chaum, eds.), LNCS, vol. 196, Springer, 1985, pp. 47–53.

[548] ______, *RSA for paranoids*, Cryptobytes **1** (1995), no. 3, 1–4.

[549] D. Shanks, *Five number-theoretic algorithms*, Proceedings of the Second Manitoba Conference on Numerical Mathematics, Congressus Numerantium, No. VII, Utilitas Math., Winnipeg, Man., 1973, pp. 51–70.

[550] T. Shioda, *On the graded ring of invariants of binary octavics*, Am. J. Math. **89** (1967), no. 4, 1022–1046.

[551] M. Shirase, D.-G. Han, Y. Hibino, H.-W. Kim, and T. Takagi, *Compressed XTR*, ACNS 2007 (J. Katz and M. Yung, eds.), LNCS, vol. 4521, Springer, 2007, pp. 420–431.

[552] Z. Shmuely, *Composite Diffie-Hellman public-key generating systems are hard to break*, Technical report No. 356, Computer Science Department, Technion, 1985.

[553] V. Shoup, *Lower bounds for discrete logarithms and related problems*, EUROCRYPT 1997 (W. Fumy, ed.), LNCS, vol. 1233, Springer, 1997, pp. 256–266.

[554] ______, *On formal models for secure key exchange (version 4), November 15, 1999*, Tech. report, IBM, 1999, Revision of Report RZ 3120.

[555] ______, *OAEP reconsidered*, CRYPTO 2001 (J. Kilian, ed.), LNCS, vol. 2139, Springer, 2001, pp. 239–259.

[556] ———, *A computational introduction to number theory and algebra*, Cambridge, 2005.

[557] I. E. Shparlinski, *Computing Jacobi symbols modulo sparse integers and polynomials and some applications*, J. Algorithms **36** (2000), 241–252.

[558] ———, *Cryptographic applications of analytic number theory*, Birkhauser, 2003.

[559] ———, *Playing "hide-and-seek" with numbers: The hidden number problem, lattices and exponential sums*, Public-Key Cryptography (P. Garrett and D. Lieman, eds.), Proceedings of Symposia in Applied Mathematics, vol. 62, AMS, 2005, pp. 153–177.

[560] I. E. Shparlinski and A. Winterhof, *A nonuniform algorithm for the hidden number problem in subgroups*, PKC 2004 (F. Bao, R. H. Deng, and J. Zhou, eds.), LNCS, vol. 2947, Springer, 2004, pp. 416–424.

[561] ———, *A hidden number problem in small subgroups*, Math. Comp. **74** (2005), no. 252, 2073–2080.

[562] A. Sidorenko, *Design and analysis of provably secure pseudorandom generators*, Ph.D. thesis, Eindhoven, 2007.

[563] C. L. Siegel, *Lectures on the geometry of numbers*, Springer, 1989.

[564] J. H. Silverman, *The arithmetic of elliptic curves*, GTM, vol. 106, Springer, 1986.

[565] ———, *Advanced topics in the arithmetic of elliptic curves*, GTM, vol. 151, Springer, 1994.

[566] J. H. Silverman and J. Suzuki, *Elliptic curve discrete logarithms and the index calculus*, ASIACRYPT 1998 (K. Ohta and D. Pei, eds.), LNCS, vol. 1514, Springer, 1998, pp. 110–125.

[567] J. H. Silverman and J. Tate, *Rational points on elliptic curves*, Springer, 1994.

[568] M. Sipser, *Introduction to the theory of computation*, Course Technology, 2005.

[569] M. Skałba, *Points on elliptic curves over finite fields*, Acta Arith. **117** (2005), no. 3, 293–301.

[570] N. P. Smart, *The discrete logarithm problem on elliptic curves of trace one*, J. Cryptology **12** (1999), no. 3, 193–196.

[571] ———, *Elliptic curve cryptosystems over small fields of odd characteristic*, J. Crypt. **12** (1999), no. 2, 141–151.

[572] ———, *Cryptography: An introduction*, McGraw-Hill, 2004.

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

[574] P. J. Smith and M. J. J. Lennon, *LUC: A new public key system*, International Conference on Information Security (E. Graham Dougall, ed.), IFIP Transactions, vol. A-37, North-Holland, 1993, pp. 103–117.

[575] P. J. Smith and C. Skinner, *A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms*, ASIACRYPT 1994 (J. Pieprzyk and R. Safavi-Naini, eds.), LNCS, vol. 917, Springer, 1994, pp. 357–364.

[576] J. A. Solinas, *Efficient arithmetic on Koblitz curves*, Des. Codes Crypt. **19** (2000), 195–249.

[577] ———, *Low-weight binary representations for pairs of integers*, Technical Report CORR 2001-41, 2001.

[578] M. Stam, *On Montgomery-like representations of elliptic curves over GF*(2^k), PKC 2003 (Y. G. Desmedt, ed.), LNCS, vol. 2567, Springer, 2003, pp. 240–253.

[579] ———, *Speeding up subgroup cryptosystems*, Ph.D. thesis, Eindhoven, 2003.

[580] M. Stam and A. K. Lenstra, *Speeding up XTR*, ASIACRYPT 2001 (C. Boyd, ed.), LNCS, vol. 2248, Springer, 2001, pp. 125–143.

[581] H. M. Stark, *Class-numbers of complex quadratic fields*, Modular Functions of One Variable I (W. Kuyk, ed.), LNM, vol. 320, Springer, 1972, pp. 153–174.

[582] D. Stehlé, *Floating point LLL: Theoretical and practical aspects*, The LLL Algorithm (P. Q. Nguyen and B. Vallée, eds.), Springer, 2010, pp. 179–213.

[583] D. Stehlé and P. Zimmermann, *A binary recursive GCD algorithm*, ANTS VI (D. A. Buell, ed.), LNCS, vol. 3076, Springer, 2004, pp. 411–425.

[584] P. Stevenhagen, *The number field sieve*, Algorithmic number theory (J. Buhler and P. Stevenhagen, eds.), MSRI publications, Cambridge, 2008, pp. 83–99.

[585] I. Stewart, *Galois theory*, 3rd ed., Chapman & Hall, 2003.

[586] I. Stewart and D. Tall, *Algebraic number theory and Fermat's last theorem*, 3rd ed., AK Peters, 2002.

[587] H. Stichtenoth, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. II. Ein Abschätzung der Ordnung der Automorphismengruppe*, Arch. Math. **24** (1973), 527–544.

[588] ———, *Die Hasse-Witt Invariante eines Kongruenzfunktionenkörpers*, Arch. Math. **33** (1979), 357–360.

[589] ———, *Algebraic function fields and codes*, Springer, 1993.

[590] H. Stichtenoth and C. Xing, *On the structure of the divisor class group of a class of curves over finite fields*, Arch. Math, **65** (1995), 141–150.

[591] D. R. Stinson, *Some baby-step giant-step algorithms for the low Hamming weight discrete logarithm problem*, Math. Comp. **71** (2001), no. 237, 379–391.

[592] ———, *Cryptography: Theory and practice*, 3rd ed., Chapman & Hall/CRC, 2005.

[593] A. Storjohann and G. Labahn, *Asymptotically fast computation of Hermite normal forms of integer matrices*, ISSAC 1996, ACM Press, 1996, pp. 259–266.

[594] E. G. Straus, *Addition chains of vectors*, American Mathematical Monthly **71** (1964), no. 7, 806–808.

[595] A. H. Suk, *Cryptanalysis of RSA with lattice attacks*, MSc thesis, University of Illinois at Urbana-Champaign, 2003.

[596] A. V. Sutherland, *Order computations in generic groups*, Ph.D. thesis, MIT, 2007.

[597] ______, *Computing Hilbert class polynomials with the Chinese remainder theorem*, Math. Comp. **80** (2011), no. 273, 501–538.

[598] ______, *Structure computation and discrete logarithms in finite abelian p-groups*, Math. Comp. **80** (2011), no. 273, 477–500.

[599] T. Takagi, *Fast RSA-type cryptosystem modulo p^kq*, CRYPTO 1998 (H. Krawczyk, ed.), LNCS, vol. 1462, Springer, 1998, pp. 318–326.

[600] J. Talbot and D. Welsh, *Complexity and cryptography: An introduction*, Cambridge, 2006.

[601] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144.

[602] ______, *Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)*, Séminarie Bourbaki 1968/69, LNM, vol. 179, Springer, 1971, pp. 95–109.

[603] E. Teske, *A space efficient algorithm for group structure computation*, Math. Comp. **67** (1998), no. 224, 1637–1663.

[604] ______, *Speeding up Pollard's rho method for computing discrete logarithms*, ANTS III (J. P. Buhler, ed.), LNCS, vol. 1423, Springer, 1998, pp. 541–554.

[605] ______, *On random walks for Pollard's rho method*, Math. Comp. **70** (2001), no. 234, 809–825.

[606] ______, *Computing discrete logarithms with the parallelized kangaroo method*, Discrete Applied Mathematics **130** (2003), 61–82.

[607] N. Thériault, *Index calculus attack for hyperelliptic curves of small genus*, ASIACRYPT 2003 (C.-S. Laih, ed.), LNCS, vol. 2894, Springer, 2003, pp. 75–92.

[608] E. Thomé, *Algorithmes de calcul de logarithmes discrets dans les corps finis*, Ph.D. thesis, L'École Polytechnique, 2003.

[609] W. Trappe and L. C. Washington, *Introduction to cryptography with coding theory*, 2nd ed., Pearson, 2005.

[610] M. A. Tsfasman, *Group of points of an elliptic curve over a finite field*, Theory of numbers and its applications,. Tbilisi, 1985, pp. 286–287.

[611] J. W. M. Turk, *Fast arithmetic operations on numbers and polynomials*, Computational methods in number theory, Part 1 (H. W. Lenstra Jr. and R. Tijdeman, eds.), Mathematical Centre Tracts 154, Amsterdam, 1984.

[612] M. Ulas, *Rational points on certain hyperelliptic curves over finite fields*, Bull. Pol. Acad. Sci. Math. **55** (2007), no. 2, 97–104.

[613] B. Vallée, *Une approche géométrique de la réduction de réseaux en petite dimension*, Ph.D. thesis, Université de Caen, 1986.

[614] ———, *Gauss' algorithm revisited*, J. Algorithms **12** (1991), no. 4, 556–572.

[615] S. Vaudenay, *Hidden collisions on DSS*, CRYPTO 1996 (N. Koblitz, ed.), LNCS, vol. 1109, Springer, 1996, pp. 83–88.

[616] ———, *A classical introduction to cryptography*, Springer, 2006.

[617] J. Vélu, *Isogénies entre courbes elliptiques*, C.R. Acad. Sc. Paris **273** (1971), 238–241.

[618] F. Vercauteren, *Optimal pairings*, IEEE Trans. Inf. Theory **56** (2010), no. 1, 455–461.

[619] E. R. Verheul, *Certificates of recoverability with scale recovery agent security*, PKC 2000 (H. Imai and Y. Zheng, eds.), LNCS, vol. 1751, Springer, 2000, pp. 258–275.

[620] ———, *Evidence that XTR is more secure than supersingular elliptic curve cryptosystems*, J. Crypt. **17** (2004), no. 4, 277–296.

[621] E. R. Verheul and H. C. A. van Tilborg, *Cryptanalysis of 'less short' RSA secret exponents*, Applicable Algebra in Engineering, Communication and Computing **8** (1997), no. 5, 425–435.

[622] M.-F. Vignéras, *Arithmétique des algèbres de quaternions*, LNM, vol. 800, Springer, 1980.

[623] J. F. Voloch, *A note on elliptic curves over finite fields*, Bulletin de la Société Mathématique de France **116** (1988), no. 4, 455–458.

[624] ———, *Jacobians of curves over finite fields*, Rocky Mountain Journal of Math. **30** (2000), no. 2, 755–759.

[625] D. Wagner, *A generalized birthday problem*, CRYPTO 2002 (M. Yung, ed.), LNCS, vol. 2442, Springer, 2002, pp. 288–303.

[626] L. C. Washington, *Elliptic curves: Number theory and cryptography*, 2nd ed., CRC Press, 2008.

[627] E. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. **2** (1969), 521–560.

[628] A. Weng, *Constructing hyperelliptic curves of genus 2 suitable for cryptography*, Math. Comp. **72** (2003), no. 241, 435–458.

[629] D. H. Wiedemann, *Solving sparse linear equations over finite fields*, IEEE Trans. Inf. Theory **32** (1986), 54–62.

[630] M. J. Wiener, *Cryptanalysis of short RSA secret exponents*, IEEE Trans. Inf. Theory **36** (1990), no. 3, 553–558.

[631] ———, *Bounds on birthday attack times*, Cryptology ePrint Archive, Report 2005/318, 2005.

[632] M. J. Wiener and R. J. Zuccherato, *Faster attacks on elliptic curve cryptosystems*, SAC 1998 (S. E. Tavares and H. Meijer, eds.), LNCS, vol. 1556, Springer, 1998, pp. 190–200.

[633] H. C. Williams, *A modification of the RSA public key encryption procedure*, IEEE Trans. Inf. Theory **26** (1980), no. 6, 726–729.

[634] ———, *A $p + 1$ method of factoring*, Math. Comp. **39** (1982), no. 159, 225–234.

[635] D. J. Winter, *The structure of fields*, GTM 16, Springer, 1974.

[636] M. Woodroofe, *Probability with applications*, McGraw-Hill, 1975.

[637] S.-M. Yen and C.-S. Laih, *Improved digital signature suitable for batch verification*, IEEE Trans. Computers **44** (1995), no. 7, 957–959.

[638] S.-M. Yen, C.-S. Laih, and A. K. Lenstra, *Multi-exponentiation*, IEEE Proceedings Computers and Digital Techniques **141** (1994), no. 6, 325–326.

[639] N. Yui, *On the Jacobian varieties of hyperelliptic curves over fields of characteristic $p > 2$*, J. Algebra **52** (1978), 378–410.

[640] O. Zariski and P. Samuel, *Commutative algebra (Vol. I and II)*, Van Nostrand, Princeton, 1960.

[641] N. Zierler, *A conversion algorithm for logarithms on $GF(2^n)$*, Journal of Pure and Applied Algebra **4** (1974), 353–356.

[642] P. Zimmermann, *Private communication*, March 10, 2009.