Bibliography

[A-1] L.M. Adleman and M.-D. Huang, editors. *ANTS-1: Algorithmic Number Theory.* Springer-Verlag, LNCS 877, 1994.

[A-2] H. Cohen, editor. *ANTS-2: Algorithmic Number Theory.* Springer-Verlag, LNCS 1122, 1996.

[A-3] J. Buhler, editor. *ANTS-3: Algorithmic Number Theory.* Springer-Verlag, LNCS 1423, 1998.

[A92] J. Seberry and Y. Zheng, editors. *Advances in Cryptology, AUSCRYPT 92.* Springer-Verlag, LNCS 718, 1993.

[A94] J. Pieprzyk and R. Safavi-Naini, editors. *Advances in Cryptology, ASIACRYPT 94.* Springer-Verlag, LNCS 917, 1995.

[A98] K. Ohta and D. Pei, editors. *Advances in Cryptology, ASIACRYPT 98.* Springer-Verlag, LNCS 1514, 1998.

[B98] D.A. Buell and J.T. Teitelbaum, editors. *Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A.O.L. Atkin*, American Mathematical Society International Press, **7**, 1998.

[C85] H.C. Williams, editor. *Advances in Cryptology, CRYPTO 85.* Springer-Verlag, LNCS 218, 1986.

[C90] A.J. Menezes and S.A. Vanstone, editors. *Advances in Cryptology, CRYPTO 90.* Springer-Verlag, LNCS 537, 1991.

[C91] J. Feigenbaum, editor. *Advances in Cryptology, CRYPTO 91.* Springer-Verlag, LNCS 576, 1992.

[C92] E.F. Bickell, editor. *Advances in Cryptology, CRYPTO 92.* Springer-Verlag, LNCS 740, 1992.

[C94] Y.G. Desmedt, editor. *Advances in Cryptology, CRYPTO 94.* Springer-Verlag, LNCS 839, 1994.

[C96] N. Koblitz, editor. *Advances in Cryptology, CRYPTO 96.* Springer-Verlag, LNCS 1109, 1996.

[C97] B. Kaliski, editor. *Advances in Cryptology, CRYPTO 97.* Springer-Verlag, LNCS 1294, 1997.

[E84] F. Pichler, editor. *Advances in Cryptology, EUROCRYPT 84.* Springer-Verlag, LNCS 219, 1985.

[E89] J.-J. Quisquater and J. Vandewalle, editors. *Advances in Cryptology, EUROCRYPT 89.* Springer-Verlag, LNCS 434, 1990.

[E90] I.B. Damgard, editor. *Advances in Cryptology, EUROCRYPT 90.* Springer-Verlag, LNCS 473, 1991.

[E91] D.W. Davies. *Advances in Cryptology, EUROCRYPT 91.* Springer-Verlag, LNCS 547, 1991.

[E95] L.C. Guillou and J.-J. Quisquater, editors. *Advances in Cryptology, EUROCRYPT 95.* Springer-Verlag, LNCS 921, 1995.

[E96] U.M. Maurer, editor. *Advances in Cryptology, EUROCRYPT 96.* Springer-Verlag, LNCS 1070, 1996.

[E97] W. Fumy, editor. *Advances in Cryptology, EUROCRYPT 97.* Springer-Verlag, LNCS 1233, 1997.

[E98] K. Nyberg, editor. *Advances in Cryptology, EUROCRYPT 98.* Springer-Verlag, LNCS 1403, 1998.

[FIPS186] FIPS 186. *Digital Signature Standard.* Federal Information Processing Standards Publication 186, U.S. Department of Commerce/N.I.S.T. National Technical Information Service, 1994.

[P1363] IEEE P1363/D3 (Draft version 3). Standard specifications for public key cryptography. May 1998.

[1] L. Adleman. The function field sieve. In [**A-1**], 108–121.

[2] L. Adleman, J. De Marrais, and M.-D. Huang. A sub-exponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields. In [**A-1**], 28–40.

[3] L. Adleman and M.-D. Huang. *Primality Testing and Abelian Varieties over Finite Fields.* Springer-Verlag, LNM 1512, 1992.

[4] L. Adleman and M.-D. Huang. Counting rational points on curves and abelian varieties over finite fields. In [**A-2**], 1–16.

[5] A.V. Aho, J.E. Hopcroft and J.D. Ullman. *The Design and Analysis of Computer Algorithms.* Addison-Wesley Publishing Co., 1974.

[6] S. Arno and F.S. Wheeler. Signed digit representations of minimal Hamming weight. *IEEE Trans. Comp.*, **42**, 1007–1010, 1993.

[7] A.O.L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, **61**, 29–67, 1993.

[8] R. Balasubramanian and N. Koblitz. The improbability that an elliptic curve has sub-exponential discrete log problem under the Menezes–Okamoto–Vanstone algorithm. *J. Crypto.*, **11**, 141–145, 1998.

[9] E.R. Berlekamp. *Algebraic Coding Theory.* Aegean Park Press, 1984.

[10] I. Biehl, J. Buchmann and C. Thiel. Cryptographic protocols based on discrete logarithms in real-quadratic orders. In [**C94**], 56–60.

[11] B.J. Birch. Atkin and the Atlas Lab. In [**B98**], 13–20.

[12] B.J. Birch and H.P.F. Swinnerton-Dyer. Notes on elliptic curves. I. *J. Reine Angew. Math.*, **212**, 7–25, 1963.

[13] B.J. Birch and H.P.F. Swinnerton-Dyer. Notes on elliptic curves. II. *J. Reine Angew. Math.*, **218**, 79–108, 1965.

[14] I.F. Blake, S. Gao and R.J. Lambert. Construction and distribution problems for irreducible trinomials over finite fields. In *Applications of Finite Fields*, D. Gollman, editor, Oxford University Press, 1996.

[15] I.F. Blake, X.H. Gao, R.C. Mullin, S.A. Vanstone and T. Yaghoobian. *Applications of Finite Fields.* A.J. Menezes, Editor. Kluwer Academic Publishers, 1993.

[16] I.F. Blake, R.M. Roth, G. Seroussi. Efficient arithmetic in finite fields through palindromic representation. Hewlett–Packard Technical Report No. HPL-98-134, August 1998.

[17] D. Bleichenbacher. On the security of the KMOV public key cryptosystem. In [**C97**], 235–248.

[18] D. Boneh and R. Lipton. Algorithms for black-box fields and their application to cryptography. In [**C96**], 283–297.

[19] D. Boneh and R. Venkatesan. Breaking RSA may not be equivalent to factoring. In [**E98**], 59–71.

[20] J. Buchmann, S. Düllman and H.C. Williams. On the complexity and efficiency of a new key exchange system. In [**E89**], 597–616.

[21] J. Buchmann, M. Jacobson and E. Teske. On some computational problems in finite abelian groups. *Math. Comp.*, **66**, 1663–1687, 1997.

[22] J. Buchmann and S. Paulus. A one way function based on ideal arithmetic in number fields. In [**C97**], 385–394.

[23] J. Buchmann and H.C. Williams. A key-exchange system based on imaginary quadratic fields. *J. Crypto.*, **1**, 107–118, 1988.

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

[25] J.W.S. Cassels. Diophantine equations with special reference to elliptic curves. *J. LMS*, **41**, 193–291, 1966.

[26] L. S. Charlap, R. Coley and D. P. Robbins. Enumeration of rational points on elliptic curves over finite fields. *Preprint*, 1992.

[27] D.V. Chudnovsky and G.V. Chudnovsky. Sequences of numbers generated by addition in formal groups and new primality and factorization tests. *Adv. in Appl. Math.*, **7**, 385–434, 1987.

[28] W.E. Clark and J.J. Liang. On arithmetic weight for a general radix representation of integers. *IEEE Trans. Info. Theory*, **19**, 823–826, 1973.

[29] H. Cohen. *A Course In Computational Algebraic Number Theory*. Springer-Verlag, GTM 138, 1993.

[30] H. Cohen, A. Miyaji and T. Ono. Efficient elliptic curve exponentiation using mixed coordinates. In [**A98**], 51–65.

[31] P. Cohen. On the coefficients of the transformation polynomials for the elliptic modular function. *Math. Proc. Camb. Phil. Soc.*, **95**, 389–402, 1984.

[32] J.-M. Couveignes. Computing a square root for the number field sieve. In [**77**], 95–102.

[33] J.-M. Couveignes. Computing l-isogenies using the p-torsion. In [**A-2**], 59–65.

[34] J.-M. Couveignes. *Quelques calculs en théorie des nombres*. Thèse, Université de Bordeaux I, July 1994.

[35] J.-M. Couveignes. *Isogeny cycles and the Schoof–Elkies–Atkin algorithm*. L'École Polytechnique, Laboratoire D'Informatique, CNRS, Palaiseau, August, 1996.

[36] J.-M. Couveignes and F. Morain. Schoof's algorithm and isogeny cycles. In [**A-1**], 43–58.

[37] R. Crandall. Method and apparatus for public key exchange in a cryptographic system. U.S. Patent Number 5159632, 1992.

[38] S.R. Dussé and B.S. Kaliski. A cryptographic library for the Motorola DSP56000. In [**E90**], 230–244.

[39] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Info. Theory*, **31**, 469-472, 1985.

[40] N.D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In [**B98**], 21–76.

[41] P. Erdös. Remarks on number theory. III. On addition chains. *Acta Arith.*, 77–81, 1960.

[42] W. Feller. *An Introduction to Probability Theory and its Applications*. John Wiley & Sons, 1970.

[43] R. Flassenberg and S. Paulus. Sieving in function fields. *Preprint*, 1997.

[44] 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**, 865–874, 1994.

[45] S. Gao and H.W. Lenstra. Optimal normal bases. *Designs, Codes and Cryptography*, **2**, 315–323, 1992.

[46] S. Goldwasser and J. Kilian. Almost all primes can be quickly certified. In *Proc. 18th STOC*, 316–329, 1986.

[47] S.W. Golomb. *Shift Register Sequences*. Holden–Day, 1967.

[48] D.M. Gordon. A survey of fast exponentiation methods. *J. Algorithms*, **27**, 129–146, 1998.

[49] J. Guajardo and C. Paar. Efficient algorithms for elliptic curve cryptosystems. In [**C97**], 342–356.

[50] J.L. Hafner and K.S. McCurley. A rigorous sub-exponential algorithm for computation of class groups. *J. AMS*, **2**, 837–850, 1989.

[51] O. Herrman. Über die Berechnung der Fourierkoeffizienten der Funktion $j(\tau)$. *J. Reine Angew. Math.*, **274/275**, 187–195, 1975.

[52] D. Hühnlein, M. Jacobson, S. Paulus and T. Takagi. A cryptosystem based on non-maximal imaginary quadratic orders with fast decryption. In [**E98**], 279–287.

[53] J.I. Igusa. Arithmetic variety of moduli for genus two. *Ann. Math.*, **72**, 612–649, 1960.

[54] T. Itoh and S. Tsujii. A fast algorithm for computing multiplicative inverses in $GF(2^m)$ using normal bases. *Info. and Comput.*, **78**(3), 171–177, 1988.

[55] M. Jacobson, N. Koblitz, J.H. Silverman, A. Stein and E. Teske. Analysis of the Xedni calculus attack. *Preprint*, 1999.

[56] J. Jedwab and C.J. Mitchell. Minimum weight modified signed-digit representations and fast exponentiation. *Electronics Letters*, **25**, 1171–1172, 1989.

[57] M. Joye and J.-J. Quisquater. Reducing the elliptic curve cryptosystem of Meyer–Müller to the cryptosystem of Rabin–Williams. *Designs, Codes and Cryptography*, **14**, 53–56, 1998.

[58] B.S. Kaliski. The Montgomery inverse and its applications. *IEEE Trans. Comp.*, **44**, 1064–1065, 1995.

[59] A. Karatsuba. *Doklady Akad. Nauk SSSR*, **145**, 293–294, 1962. English translation in *Soviet Physics–Doklady*, **7**, 595–596, 1963.

[60] A. W. Knapp. *Elliptic Curves*. Princeton University Press, 1993.

[61] D.E. Knuth. *The Art of Computer Programming*, **2** – *Semi-numerical Algorithms*. Addison-Wesley, 2nd edition, 1981.

[62] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, **48**, 203–209, 1987.

[63] N. Koblitz. Hyperelliptic cryptosystems. *J. Crypto.*, **1**, 139–150, 1989.

[64] N. Koblitz. Constructing elliptic curve cryptosystems in characteristic 2. In [**C90**], 156–167.

[65] N. Koblitz. CM-curves with good cryptographic properties. In [**C91**], 279–287.

[66] N. Koblitz, *Algebraic aspects of cryptography. 3, Algorithms and Computation in Mathematics*, Springer-Verlag, Berlin, 1998.

[67] C.K. Koç and T. Acar. Montgomery multiplication in $GF(2^k)$. *Designs, Codes and Cryptography*, **14**, 57–69, 1998.

[68] K. Koyama, U. Maurer, T. Okamoto and S.A. Vanstone. New public-key scheme based on elliptic curves over the ring $\mathbb{Z}_n$. In [**C91**], 252–266.

[69] K. Koyama and Y. Tsuruoka. Speeding up elliptic cryptosystems by using a signed binary window method. In [**C92**], 345–357.

[70] K. Kurosawa, K. Okada and S. Tsujii. Low exponent attack against elliptic curve RSA. In [**A94**], 376–383.

[71] K.-Y. Lam and L.C.K. Hui. Efficiency of SS(l) square-and-multiply exponentiation algorithms. *Electronics Letters*, **30**, 2115–2116, 1994.

[72] S. Lang. *Elliptic Curves: Diophantine Analysis*. Springer-Verlag, 1978.

[73] G.-J. Lay and H.G. Zimmer. Constructing elliptic curves with given group order over large finite fields. In [**A-1**], 250–263.

[74] F. Lehmann, M. Maurer, V. Müller and V. Shoup. Counting the number of points on elliptic curves over finite fields of characteristic greater than three. In [**A-1**], 60–70.

[75] F. Lemmermeyer. The Euclidean algorithm in algebraic number fields. *Expo. Math.*, **13**, 385–416, 1995.

[76] A. Lempel, G. Seroussi, and S. Winograd. On the complexity of multiplication in finite fields. *Theoretical Comp. Sci.*, **22**, 285–296, 1983.

[77] A.K. Lenstra and H.W. Lenstra, editors. *The Development of the Number Field Sieve*. Springer-Verlag, LNM 1554, 1993.

[78] H.W. Lenstra. Factoring integers with elliptic curves. *Ann. Math.*, **126**, 649–673, 1987.

[79] H.W. Lenstra and C.P. Schnorr. A Monte Carlo factoring algorithm with linear storage. *Math. Comp.*, **43**, 289–311, 1984.

[80] R. Lercier. Computing isogenies in $\mathbb{F}_{2^n}$. In [**A-2**], 197–212.

[81] R. Lercier. *Algorithmique des courbes elliptiques dans les corps finis*. Thèse, L'École Polytechnique, Laboratoire D'Informatique, CNRS, Paris, June, 1997.

[82] R. Lercier. Finding good random elliptic curves for cryptosystems defined over $\mathbb{F}_{2^n}$. In [**E97**], 379–392.

[83] R. Lercier and F. Morain. Counting the number of points on elliptic curves over finite fields: strategies and performances. In [**E95**], 79–94.

[84] R. Lercier and F. Morain. Algorithms for computing isogenies between elliptic curves. In [**B98**], 77-96.

[85] R. Lercier and F. Morain. Counting points on elliptic curves over $\mathbb{F}_{p^n}$ using Couveignes algorithm. Rapport de Recherche LIX/RR/95/09, 1995.

[86] R. Lidl and H. Niederreiter. *Finite Fields*, in *Encyclopedia of Mathematics and its Applications*, G.-C. Rota, editor, Addison-Wesley, 1983.

[87] J.H. van Lint. *Introduction to Coding Theory*. Springer-Verlag, 1982.

[88] K.S. McCurley. The discrete logarithm problem. In *Cryptology and Computational Number Theory*, C. Pomerance, editor, 49–74. Proc. Symp. Applied Maths **42**, 1990.

[89] J. McKee. Subtleties in the distribution of the numbers of points on elliptic curves over a finite prime field. *J. LMS*, **59**, 448–460, 1999.

[90] J. McKee and R.G.E. Pinch. On a cryptosystem of Vanstone and Zuccherato. *Preprint*, 1998.

[91] K. Mahler. On the coefficients of the 2^mth transformation polynomial for $j(\omega)$. *Acta Arith.*, **21**, 89–97, 1972.

[92] K. Mahler. On the coefficients of transformation polynomials for the modular functions. *Bull. Austral. Math. Soc.*, **10**, 197–218, 1974.

[93] J.L. Massey and O.N. Garcia. Error correcting codes in computer arithmetic. In *Advances in Information Systems Science*, J.L. Tou, editor, **4**, 273–326. Plenum, New York, 1971.

[94] U.M. Maurer. Towards the equivalence of breaking the Diffie–Hellman protocol and computing discrete logarithms. In [**C94**], 271–281.

[95] U.M. Maurer and S. Wolf. Diffie–Hellman oracles. In [**C96**], 268–282.

[96] W. Meier and O. Staffelbach. Efficient multiplication on certain non-supersingular elliptic curves. In [**C92**], 333–344.

[97] A.J. Menezes. *Elliptic Curve Public Key Cryptosystems*. Kluwer Academic Publishers, 1993.

[98] A.J. Menezes, T. Okamoto and S.A. Vanstone. Reducing elliptic curve logarithms to a finite field. *IEEE Trans. Info. Theory*, **39**, 1639–1646, 1993.

[99] A.J. Menezes, P.C. van Oorschot and S.A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.

[100] A.J. Menezes, S.A. Vanstone and R. J. Zuccherato. Counting points on elliptic curves over $\mathbb{F}_{2^n}$. *Math. Comp.*, **60**, 407–420, 1993.

[101] B. Meyer and V. Müller. A public key cryptosystem based on elliptic curves over $\mathbb{Z}/n\mathbb{Z}$ equivalent to factoring. In [**E96**], 49–59.

[102] G. Miller. Riemann's hypothesis and test for primality. *J. Comp. and Sys. Sci.*, **13**, 300–317, 1976.

[103] V. Miller. Use of elliptic curves in cryptography. In [**C85**], 417–426.

[104] A. Miyaji. Elliptic curves over $\mathbb{F}_p$ suitable for cryptosystems. In [**A92**], 479–491.

[105] P.L. Montgomery. Modular multiplication without trial division. *Math. Comp.*, **44**, 519–521, 1985.

[106] P.L. Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Math. Comp.*, **48**, 243–264, 1987.

[107] F. Morain. Building cyclic elliptic curves modulo large primes. In [**E91**], 328–336.

[108] F. Morain. Calcul du nombre de points sur une courbe elliptique dans un corps fini: aspects algorithmiques. *J. Théorie des Nombres de Bordeaux*, **7**, 255–282, 1995.

[109] F. Morain and J. Olivos. Speeding up the computations on an elliptic curve using addition–subtraction chains. *Info. Theory Appl.*, **24**, 531–543, 1990.

[110] V. Müller. Ein Algorithmus zur Bestimmung der Punktzahl elliptischer Kurven über endlichen Körpern der Charakteristik grösser drei. Ph.D. Thesis, Universität des Saarlandes, 1995.

[111] V. Müller. Fast multiplication on elliptic curves over small fields of characteristic two. *J. Crypto.*, **11**, 219–234, 1998.

[112] R. Mullin, I. Onyszchuk, S.A. Vanstone and R. Wilson. Optimal normal bases in $GF(p^n)$. *Discrete Appl. Math.*, **22**, 149–161, 1988/89.

[113] K. Nyberg and R.A. Rueppel. Message recovery for signature schemes based on the discrete logarithm problem. *Designs, Codes and Cryptography*, **7**, 61–81, 1996.

[114] A.M. Odlyzko. Discrete logarithms in finite fields and their cryptographic significance. In [**E84**], 417–426.

[115] J. Omura and J. Massey. Computational method and apparatus for finite field arithmetic. U.S. Patent number 4,587,627, May 1986.

[116] P.C. van Oorschot and M.J. Wiener. Parallel collision search with cryptanalytic applications. *J. Crypto.*, **12**, 1–28, 1999.

[117] S. Paulus. An algorithm of sub-exponential type computing the class group of quadratic orders over principal ideal domains. In [**A-2**], 243–257.

[118] S. Paulus and H.-G. Rück. Real and imaginary quadratic representation of hyperelliptic function fields. *Math. Comp.*, **68**, 1233–1241, 1999.

[119] S. Paulus and A. Stein. Comparing real and imaginary arithmetics for divisor class groups of hyperelliptic curves. In [**A-3**], 576–591.

[120] J. Pila. Frobenius maps of abelian varieties and finding roots of unity in finite fields. *Math. Comp.*, **55**, 745–763, 1996.

[121] R.G.E. Pinch. Extending the Wiener attack to RSA-type cryptosystems. *Electronics Letters*, **31**, 1736–1738, 1995.

[122] J.-M. Piveteau. New signature scheme with message recovery. *Electronics Letters*, **29**, 2185, 1993.

[123] H.C. Pocklington. The determination of the prime and composite nature of large numbers by Fermat's theorem. *Proc. Camb. Phil. Soc.*, **18**, 29–30, 1914/16.

[124] G.C. Pohlig and M.E. Hellman. An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance. *IEEE Trans. Info. Theory*, **24**, 106–110, 1978.

[125] J.M. Pollard. Monte Carlo methods for index computation (mod p). *Math. Comp.*, **32**, 918–924, 1978.

[126] K.C. Posch and R. Posch. Modulo reduction in residue number systems. *IEEE Trans. Parallel and Dist. Systems*, **6**, 449–454, 1995.

[127] K.C. Posch and R. Posch. Division in residue number systems involving length indicators. *J. Comp. Appl. Maths.*, **66**, 411-419, 1996.

[128] J.-J. Quisquater and J.-P. Delescaille. How easy is collision search? Application to DES. In [**E89**], 408–413.

[129] M. Rabin. Digitized signatures and public key functions as intractable as factorization. *MIT/LCS/TR-212*, MIT Laboratory for Computer Science, 1979.

[130] M. Rabin. Probabilistic algorithms for testing primality. *J. Number Theory*, **12**, 128–138, 1980.

[131] G. Reitwiesner. Binary arithmetic. *Adv. in Comp.*, **1**, 231–308, 1960.

[132] H. Riesel. *Prime Numbers and Computer Methods for Factorization.* Birkhäuser, 1985.

[133] R.L. Rivest, Shamir A. and L.M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM*, **21**, 120–126, 1978.

[134] R.L. Rivest, Shamir A. and L.M. Adleman. Cryptographic communications system and method. US Patent No 4405829, 1983.

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

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

[137] J. Sattler and C.P. Schnorr. Generating random walks in groups. *Ann. Univ. Sci. Budapest. Sect. Comp.*, **6**, 65–79, 1985.

[138] E.F. Schaefer. Computing a Selmer group of a Jacobian using functions on the curve. *Math. Ann.*, **310**, 447-471, 1998.

[139] B. Schneier. *Applied Cryptography.* John Wiley and Sons, 1996.

[140] A. Schönhage. Schnelle Multiplikation von Polynomen über Körpen der Charakteristik 2. *Acta Info.*, **7**, 395–398, 1977.

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

[142] R. Schoof. Counting points on elliptic curves over finite fields. *J. Théorie des Nombres de Bordeaux*, **7**, 219–254, 1995.

[143] I.A. Semaev. Evaluation of discrete logarithms on some elliptic curves. *Math. Comp.*, **67**, 353–356, 1998.

[144] G. Seroussi. Table of low-weight irreducible polynomials over $\mathbb{F}_2$. Hewlett–Packard Laboratories Technical Report No. HPL-98-135, August 1998.

[145] G. Seroussi. Compact representation of elliptic curve points over $\mathbb{F}_{2^n}$. Hewlett–Packard Laboratories Technical Report No. HPL-98-94R1, September 1998.

[146] V. Shoup. Lower bounds for discrete logarithm and related problems. In [**E97**], 313–328.

[147] J.H. Silverman. *The Arithmetic of Elliptic Curves.* Springer-Verlag, GTM 106, 1986.

[148] J.H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves.* Springer-Verlag, GTM 151, 1994.

[149] J.H. Silverman and J. Suzuki. Elliptic curve discrete logarithms and the index calculus. In [**A98**], 110–125.

[150] J.H. Silverman. The xedni calculus and the elliptic curve discrete logarithm problem. *Preprint*, 1998.

[151] N.P. Smart. *The Algorithmic Resolution of Diophantine Equations.* Cambridge University Press, 1998.

[152] N.P. Smart. Elliptic curves over small fields of odd characteristic *J. Crypto.*, **12**, 141–151, 1999.

[153] N.P. Smart. The discrete logarithm problem on elliptic curves of trace one. *J. Crypto.*, **12**, 193–196, 1999.

[154] J.A. Solinas. An improved algorithm for arithmetic on a family of elliptic curves. In [**C97**], 357-371.

[155] A.-M. Spallek. Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosytemen *Ph.D. Thesis*, Universität Essen, 1994.

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

[157] E. Teske. Speeding up Pollard's Rho method for computing discrete logarithms. In [**A-3**], 541–554.

[158] E. Teske. A space efficient algorithm for group structure computation. *Math. Comp.*, **67**, 1637–1663, 1998.

[159] S.A. Vanstone and R.J. Zuccherato. Elliptic curve cryptosystems using curves of smooth order over the ring $\mathbb{Z}_n$. *IEEE Trans. Info. Theory*, **43**, 1231–1237, 1997.

[160] J. Vélu. Isogénies entre courbes elliptiques. *Comptes Rendus l'Acad. Sci. Paris, Ser. A*, **273**, 238-241 1971.

[161] J.F. Voloch. The discrete logarithm problem on elliptic curves and descents *Preprint*, 1997.

[162] A. Wiles. Modular elliptic curves and Fermat's Last Theorem. *Ann. Math.*, **142**, 443–551, 1995.

[163] H.C. Williams. A modification of the RSA public-key encryption procedure. *IEEE Trans. Info. Theory*, **26**, 726–729, 1980.

[164] S. Winograd. Some bilinear forms whose complexity depends on the field of constants. *Math. Sys. Theory*, **10**, 169–180, 1977.