# Bibliografía


[1] M. Adleman and K. Kompella, Using smoothness to achieve parallelism, *Proceedings of the 20th ACM Symposium on the Theory of Computing*, pp. 528-538, 1988.

[2] G. Agnew, R. Mullin, S. Vanstone. An implementation of elliptic curve cryptosystems over $GF(2^{155})$. *IEEE Journal on Selected Areas in Communication*. vol. 11, pp. 804-813, 1993.

[3] H.R. Amirazizi, M.E. Hellman. Time-memory-processor trade-offs. *IEEE Transactions on Information Theory*. vol. 34, pp. 505-512, 1988.

[4] ANSI X9.62, Public Key Cryptography for the Financial Services Industry - The Elliptic Curve Digital Signature Algorithm (ECDSA), *draft*, ASC X9 Secretariat, American Bankers Association, 1998.

[5] ANSI X9.63, Public Key Cryptography for the Financial Services Industry - The Elliptic Curve Key Agreement and Key Transport Protocols, *draft*, ASC X9 Secretariat, American Bankers Association, 1999.

[6] D. Ash, I. Blake, S. Vanstone. Low complexity normal bases. *Discrete Applied Mathematics*, vol. 25, pp. 191-210, 1989.

[7] D.H. Bailey. The computation of Pi to 29,360,000 decimal digits using Borwein's Quartically Convergent Algorithm. *Mathematics of Computation*, vol. 50, pp. 283-296, 1988.

[8] R. Balasubramanian, N. Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm, *Journal of Cryptology*, vol. 11, pp. 141-145, 1998.

[9] P.W. Beame, S.A. Cook and H.J. Hoover, Log depth circuits for division and related problems, *SIAM Journal on Computing*, vol. 15, pp. 994-1003, 1986.

[10] D. Beauregard. Efficient algorithms for implementing elliptic curve public-key schemes. Master's thesis, ECE Dept., Worcester Polytechnic Institute, Worcester, USA, May 1996.

[11] D.J. Becker, T. Sterling, D. Savarese, J.E. Dorband, U.A. Ranawake, C.V.Packer. BEOWULF: A parallel workstation for scientific computation, *Proceedings of the 1995 International Conference on Parallel Processing (ICPP)*, pp. 11-14, 1995.

[12] I. Blake, G. Seroussi, N. Smart, *Elliptic Curves in Cryptography*, London Mathematical Society Lecture Series 265, Cambridge University Press, 2002.

[13] A. Borodin, I. Munro. *The Computational Complexity of Algebraic and Numeric Problems*. American Elsevier, NY, 1975.

[14] R.P. Brent, On the Addition of Binary Numbers, *IEEE Transactions on Computers*, vol. 19, pp. 758-759, 1970.

[15] R.P. Brent, The parallel evaluation of general arithmetic expressions. *Journal of ACM*, vol. 21, pp. 201-206, 1974.

[16] R.P. Brent, D.J. Kuck, K. Murayama. The parallel evaluation of arithmetic expressions without division. *IEEE Transactions on Computers*, vol. 22, pp.532-534, 1973.

[17] Certicom, Remarks on the security of the elliptic curve cryptosystem. *Certicom Whitepaper*. Disponible en http://www.certicom.com/

[18] D.V. Chudnovsky and G.V. Chudnovsky, Sequences of numbers generated by addition in formal groups and new primality and factorization tests, *Advances in Applied Mathematics*, vol. 7, pp. 385-434, 1986.

[19] H. Cohen. *A Course in Computational Algebraic Number Theory*. Springer-Verlag, 1993.

[20] H. Cohen, A. Miyaji and T. Ono, Efficient elliptic curve exponentiation, *Advances in Cryptology - Proceedings of ICICS'97*, LNCS 1334, pp. 282-290, 1997.

[21] H. Cohen, A. Miyaji and T. Ono, Efficient elliptic curve exponentiation using mixed coordinates, *Advances in Cryptology - ASIACRYPT'98*, LNCS 1514, pp. 51-65, 1998.

[22] J.M. Cooley, J.W. Tukey. An algorithm for machine calculation of complex Fourier series. *Mathematics of Computation*, vol. 19, pp. 297-301, 1965.

[23] W. Diffie, M.E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, vol. 22, n. 6, pp. 644-654, 1976.

[24] W.S. Dorn. Generalization of Horner's Rule for polynomial evaluation, *IBM Journal of Research and Development*, pp. 239-245, 1962.

[25] I. Duursma, P. Gaudry, F. Morain. Speeding up the discrete log computation on curves with automorphisms. *Report LIX/RR/99/03*, Laboratoire D'Informatique, CNRS, France, 1999.

[26] T. ElGamal. A public-key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, vol. 31, n. 4, pp. 469-472, 1985.

[27] A.E. Escot, J.C. Sager, A.P.L. Selkirk, D. Tsapakidis. Attacking elliptic curve cryptosystems using the parallel Pollard rho method. *CryptoBytes (The technical newsletter of RSA Laboratories)*, vol. 4, no. 2, pp. 15-19, 1998.

[28] R.J. Fateman. Polynomial multiplication, powers and asymptotic analysis: Some comments. *SIAM Journal on Computation*, vol. 7, n. 3, pp. 196-210, 1974.

[29] G. Frey, H. Rück. A remark considering $m$-divisibility end the discrete logarithm problem in the divisor class group of curves. *Mathematics of Computation*, vol. 64, pp. 865-874, 1994.

[30] S. Galbraith, N. Smart. A cryptographic application of Weil descent. *Codes and Cryptography*, LNCS 1746, pp. 191-200, 1999.

[31] R. Gallant, R. Lambert, S. Vanstone. Improving the parallelized Pollard lambda search on binary anomalous curves. *http://www.certicom.com/chal/download/paper.ps*, 1998.

[32] J.M. García, R.F. Menchaca. Desarrollo de un sistema criptográfico basado en curvas elípticas. *Simposium de Redes de Computadoras CICREDCOMP'99*, CIC-IPN, 1999.

[33] J.M. García, R.F. Menchaca. Parallel preprocessing for discrete exponentiation, *IV Coloquio Nacional de Teoría de Códigos, Criptografía y áreas relacionadas*, Cd. de México, Junio del 2000.

[34] J.M. García, R.F. Menchaca, Quantum cryptoanalisis of elliptic curve systems, *Computación y Sistemas*, vol. 4, No. 2, 2001.

[35] J.M. García, R.F. Menchaca, Parallel algorithm for multiplication on elliptic curves, *Proceedings of the ENC'01*, Sept. 2001.

[36] J.M. García, R.F. Menchaca, Computación en paralelo de múltiplos de puntos sobre curvas de Koblitz, *Actas de la VII Reunión Española de Criptologia y Seguridad de la Información*, Universidad de Oviedo, España, Septiembre 2002.

[37] P. Gaudry, F. Hess, N. Smart. Constructive and destructive facets of Weil descent on elliptic curves,preprint,January 2000. *http://www.hpl.hp.com/techreports/2000/HPL-2000-10.html*

[38] A. Geist, A. Beguelin, J. Dongarra, W. Jiang, B. Mancheck, V. Sunderam. *PVM: Parallel Virtual Machine - A User's Guide and Tutorial for Network Parallel Computing*. MIT Press, 1994.

[39] D. Gordon. A survey of fast exponentiation methods. *Journal of Algorithms*, vol. 27, pp. 129-146, 1998.

[40] J. Guajardo, C. Paar. Efficient algorithms for elliptic curve cryptosystems. *Advances in Cryptology - CRYPTO'97*. LNCS 1294, pp. 342-356, 1997.

[41] J.L. Gustafson. Compute-intensive processors and multicomputers, en K. Hwang, D. DeGroot (eds.), *Parallel Processing for Supercomputers and Artificial Intelligence*. McGraw-Hill, 1989.

[42] G. Harper, A. Menezes, S. Vanstone. Public-key cryptosystems with very small key lengths. *Advances in Cryptology - EUROCRYPT'92*. pp. 163-173, 1992.

[43] T. Hasegawa, J. Nakajima, M. Matsui. A practical implementation of elliptic curve cryptosystems over $GF(p)$ on a 16-bit microcomputer. *Public Key Cryptography - Proceedings of the PKC'98*, LNCS 1431, pp. 182-194, 1998.

[44] K. Hwang. Exploiting parallelism in multiprocessors and multicomputers, en K. Hwang, D. DeGroot (eds.), *Parallel Processing for Supercomputers and Artificial Intelligence*. McGraw-Hill, 1989.

[45] ISO/IEC 15946. *Information Technology - Security Techniques - Cryptographic Techniques Based on Elliptic Curves*, Committee Draft (CD), 1999.

[46] P. Ivey, S. Walker, J. Stern, S. Davidson. An ultra-high speed public key encryption processor. *Proceedings of IEEE Custom Integrated Circuit Conference*, Boston, 1992, 19.6.1-19.6.4.

[47] A. Karatsuba, Y. Ofman. Multiplication of multidigit numbers on automata. *Soviet Physics Doklady*, vol. 7, pp. 595-596, 1963.

[48] D. E. Knuth. *The Art of Computer Programming. Vol. 2: Seminumerical Algorithms*. Addison-Wesley, 2nd. Ed.,1981.

[49] N. Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, vol. 48, pp. 203-209, 1987.

[50] N. Koblitz, CM-curves with good cryptographic properties, *Advances in Cryptology - CRYPTO'91*, LNCS 576, pp. 279-287, 1997.

[51] C.K. Koc. Analysis of sliding window techniques for exponentiation. *Computers and Mathematics with Applications*, vol. 30, n. 10, pp. 17-24, 1995.

[52] J. Koeller, A. Menezes, M. Qu, S. Vanstone. Elliptic curve systems. Draft 8. *IEEE P1363 Standard for RSA, Diffie-Hellman and Related Public-Key Cryptography*, 1996.

[53] K. Koyama and T. Tsuruoka, Speeding up elliptic cryptosystems by using a signed binary window method, *Advances in Cryptology - CRYPTO'92*, LNCS 740, pp. 345-357, 1993.

[54] S. Lakshmivarahan, S.K. Dhall. *Analysis and Design of Parallel Algorithms: Arithmetic and Matrix Problems*. McGraw-Hill, 1990.

[55] G. Lay, H. Zimmer. Constructing elliptic curves with given group order over large finite fileds. *Algorithmic Number Theory: First International Symposium*, LNCS 877, pp. 250-263, 1994.

[56] H.W. Lenstra, Jr. Factoring integers with elliptic curves. *Annals of Mathematics*. vol. 2, no. 126, pp. 649-673, 1987.

[57] R. Lercier, F. Morain. Counting the number of points on elliptic curves with given group order over large finite fields. *Advances in Cryptology - EUROCRYPT'95*, LNCS 921, pp.79-94, 1995.

[58] R. Lidl, H. Niederreiter. *Introduction to Finite Fields and their Applications*, Cambridge University Press, 1984.

[59] C.H. Lim, P.J. Lee, More flexible exponentiation with precomputation, *Advances in Cryptology - CRYPTO'94*, LNCS 389, pp. 95-107, 1994.

[60] J. Lopez, R. Dahab, Fast multiplication on elliptic curves over $GF(2^m)$ without precomputation, *CHES'99*, LNCS 1717, pp. 316-327, 1999.

[61] R. McEliece. *Finite Fields for Computer Scientists and Engineers*, Kluwer Academic Publishers, 1987.

[62] W. Meier, O. Staffelbach. Efficient multiplication on certain nonsupersingular elliptic curves. *Advances in Cryptology - CRYPTO'92*, LNCS 740, pp. 333-344, 1993.

[63] A.J. Menezes. *Application of Finite Fields*, Kluwer Academic Publishers, 1993.

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

[65] A.J. Menezes, T. Okamoto, S. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions on Information Theory*. vol. 39, pp. 1639-1646, 1993.

[66] A.J.Menezes, P.C. van Oorschot, S.A. Vanstone. *Handbook of Applied Cryptography*, CRC Press,1997.

[67] Message Passing Interface Forum. MPI: A Message-Passing Interface standard. *The International Journal of Supercomputer Applications and High Performance Computing*, no. 8, 1994.

[68] V. Miller, Uses of elliptic curves in cryptography. *Advances in Cryptology - CRYPTO'85*, LNCS 218, pp. 417-426, 1986.

[69] F. Morain. Building cyclic elliptic curves modulo large primes. *Advances in Cryptology - EUROCRYPT'91*, LNCS 547, pp. 328-336, 1993.

[70] F. Morain, J. Olivos. Speeding up the computations on an elliptic curve using addition-substraction chains. *Inf. Theor. Appl.*, vol. 24, pp. 531-543, 1990.

[71] R. Mullin, I. Onyszchuk, S. Vanstone, R. Wilson. Optimal normal bases in $GF(p^n)$. *Discrete Applied Mathematics*, vol. 22, pp. 149-161, 1988.

[72] Y. Muraoka. Parallelism exposure and explotation in programs. *Ph. D. Thesis*, Department of Computer Science, University of Illinois, Urbana, IL, 1971.

[73] National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, FIPS Publication 186-2, 2000.

[74] NTL, A Number Theoretic Library, *http://www.shoup.net/ntl/*.

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

[76] C. Paar. A new architecture for a parallel finite field multiplier with low complexity based on composite fields. *IEEE Transactions on Computers*, vol. 45, no. 7, pp. 856-861, 1996.

[77] C. Paar, P. Soria Rodriguez. A new class of fast finite field architectures for public-key algorithms. *Advances in Cryptology - EUROCRYPT'97*, LNCS 1233, pp. 363-378, 1997.

[78] V.Y. Pan. Methods of computing values of polynomials. *Russian Mathematical Surveys*, vol. 21, no. 1, pp. 105-136, 1966.

[79] S. Pohlig, M. Hellman. An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance. *IEEE Transactions on Information Theory*, vol. 24, pp. 106-110, 1978.

[80] J. Pollard, Monte Carlo methods for index computation mod p. *Mathematics of Computation*. vol. 32, pp. 918-924, 1978.

[81] F.P. Preparata, D.E. Muller. Efficient parallel evaluation of Boolean expressions. *IEEE Transactions on Computers*, vol. 27, pp. 548-549, 1976.

[82] R.L. Rivest, A. Shamir, L.M. Adleman, A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM*, vol. 21, n. 2, pp. 120-126, 1978.

[83] RSA Laboratories. *The Public-Key Cryptography Standards (PKCS)*. RSA Data Security, Inc., Nov. 1993.

[84] T. Satoh, K. Araki. Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves. *Comentarii Mathematici Universitatis Sanct Pauli*, vol. 47, pp. 81-92, 1998.

[85] A. Schönhage. A lower bound for the length of addition chains. *Theoretical Computer Science*, vol. 1, pp. 1-12, 1975.

[86] A. Schönhage, V. Strassen. Schnelle Multiplikation Grosser Zahlen. *Computing*, vol. 7, pp. 281-292, 1971.

[87] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod $p$. *Mathematics of Computation*, vol. 44, pp. 483-494, 1985.

[88] R. Schroeppel, H. Orman, S. O'Malley, O. Spatscheck. Fast key exchange with elliptic curve systems. *Advances in Cryptology - CRYPTO'95*, pp. 43-56, 1995.

[89] I. Semaev. Evaluation of discrete logarithms in a group of $p$-torsion points of an elliptic curve in characteristic $p$. *Mathematics of Computation*, vol. 67, pp. 352-356, 1998.

[90] P.W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, *Proc. 35th Annual Symposium on Foundations of Computer Science*, IEEE Computer Soc. Press, pp. 124-134, 1994.

[91] P.W. Shor, Polynomial tyme algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM Journal on Computing*, vol. 26, pp. 1484-1509, 1997.

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

[93] J.H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Graduate Text in Mathematics, vol. 151, Springer-Verlag, 1994.

[94] J.H. Silverman, J. Suzuki. Elliptic curve discrete logarithms and the index calculus. *Advances in Cryptology - ASIACRYPT'98*. LNCS 1514, pp. 110-125, 1999.

[95] J.H. Silverman, J. Tate. *Rational Points on Elliptic Curves*, Undergraduate Texts in Mathematics, Springer-Verlag, 1992.

[96] R. Silverman, J. Stapleton. Contribution to ANSI X9F1 workgroup. cit. por D. Johnson, A. Menezes. *Technical Report CORR 99-34*. Dept. of C&O, University of Waterloo, Canada. 1999.

[97] N. Smart. The discrete logarithm problem on elliptic curves of trace one. *Journal of Cryptology*, vol. 12, pp. 193-196, 1999.

[98] M. Snir, W. Gropp. *MPI: The Complete Reference*. MIT Press, 1998.

[99] J. Solinas, An improved algorithm for arithmetic on a family of elliptic curves, *Advances in Cryptology - CRYPTO'97*. LNCS 1294, pp. 357-371, 1997.

[100] J. Solinas, Efficient arithmetic on Koblitz curves, *Design, Codes and Cryptography*, vol. 19, pp. 195-249, 2000.

[101] D.R. Stinson. Some observations on parallel algorithms for fast exponentiation in $GF(2^n)$. *SIAM Journal on Computation*, vol. 19, pp. 711-717, 1990.

[102] E. Teske. Speeding up Pollard's rho method for computing discrete logarithms. *Algorithmic Number Theory*. LNCS 1423, pp. 541-554, 1998.

[103] P. van Oorschot, M. Wiener. Parallel collision search with cryptoanalytic aplications. *Journal of Cryptology*, vol. 12, pp. 1-28, 1999.

[104] J. van zur Gathen, M. Nocker, Exponentiation in finite fields: theory and practice. *Proc. 12th Symposium Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, LNCS 1255, pp. 88-133, 1997.

[105] M. Wiener, R. Zucherato. Faster attacks on elliptic curve cryptosystems. *Selected Areas in Cryptography*. LNCS 1556, pp. 190-200, 1999.

[106] E. De Win, A. Bosselaers, S. Vandenberghe, P. De Gersem, J. Vandewalle. A fast software implementation for arithmetic operations in $GF(2^m)$. *Advances in Cryptology - ASIACRYPT'96*, LNCS, 1996.