# References

1. S. Adam, J. Ioannidis, and A. D. Rubin. Using the Fluhrer, Mantin, and Shamir Attack to Break WEP. Technical report, ATT Labs TD-4ZCPZZ, Available at: http://www.cs.rice.edu/~astubble/wep., August 2001.
2. H. Aigner, H. Bock, M. Hütter, and J. Wolkerstorfer. A Low-Cost ECC Coprocessor for Smartcards. In *Cryptographic Hardware and Embedded Systems - CHES 2004: 6th International Workshop Cambridge, MA, USA, August 11-13, 2004. Proceedings*, volume 3156 of *Lecture Notes in Computer Science*, pages 107–118. Springer, 2004.
3. Altera. Design Software, 2006.
URL: http://www.altera.com/products/software/sfw-index.jsp.
4. Altera. Device Family Overview, 2006.
http://www.altera.com/products/devices/common/dev-family_overview.html.
5. Altera. The Nios II Processor, 2006.
url: http://www.altera.com/literature/lit-nio2.jsp.
6. D. N. Amanor, V. Bunimov, C. Paar, J. Pelzl, and M. Schimmler. Efficient Hardware Architectures for Modular Multiplication on FPGAs. In T. Rissa, S. J. E. Wilton, and P. H. W. Leong, editors, *Proceedings of the 2005 International Conference on Field Programmable Logic and Applications (FPL), Tampere, Finland, August 24-26, 2005*, pages 539–542. IEEE, 2005.
7. Amphion Semiconductor. *CS5210-40: High Performance AES Encryption Cores*, 2003.
8. R. J. Anderson and E. Biham. TIGER: A Fast New Hash Function. In *Proceedings of the Third International Workshop on Fast Software Encryption*, pages 89–97, London, UK, 1996. Springer-Verlag.
9. B. Ansari and H. Wu. Parallel Scalar Multiplication for Elliptic Curve Cryptosystems. In *International Conference on Communications, Circuits and Systems, 2005*, volume I, pages 71–73. IEEE Computer Society, May 2005.
10. F. Argüello. Lehmer-Based Algorithm for Computing Inverses in Galois Fields gf($2^m$). *IEE Electronic Letters*, 42(5):270–271, March 1997.
11. P. J. Ashenden. *Circuit Design with VHDL*. Morgan Kaufmann Publishers, second edition, 2002.
12. R. M. Avanzi, C. Heuberger, and H. Prodinger. Minimality of the Hamming Weight of the $\tau$-NAF for Koblitz Curves and Improved Combination

with Point Halving. Cryptology ePrint Archive, Report 2005/225, 2005. http://eprint.iacr.org/.

13. R. M. Avanzi and F. Sica. Scalar Multiplication on Koblitz Curves using Double Bases. Cryptology ePrint Archive, Report 2006/067, 2006. http://eprint.iacr.org/.
14. E. Bach and J. Shallit. *Algorithmic Number Theory, Volume I: Efficient Algorithms.* Kluwer Academic Publishers, Boston, MA, 1996.
15. D. Bae, G. Kim, J. Kim, S. Park, and O. Song. An Efficient Design of CCMP for Robust Security Network. In *International Conference on Information Security and Cryptology*, volume 3935, pages 337–346, Seoul, Korea, December 2005. Springer-Verlag.
16. J. C. Bajard, L. Imbert, and G. A. Jullien. Parallel Montgomery Multiplication in GF($2^k$) Using Trinomial Residue Arithmetic. In *17th IEEE Symposium on Computer Arithmetic (ARITH-17 2005), 27-29 June 2005, Cape Cod, MA, USA*, pages 164–171. IEEE Computer Society, 2005.
17. P. Barreto. The Hash Functions Lounge. Available at: http://paginas.terra.com.br/informatica/paulobarreto/hflounge.html#BC04.
18. L. Batina, N. Mentens, S.B. Ors, and B. Preneel. Serial Multiplier Architectures over GF($2^n$) for Elliptic Curve Cryptosystems. In *Proceedings of the 12th IEEE Mediterranean Electrotechnical Conference MELECON 2004*, volume 2, pages 779–782. IEEE Computer Society, May 2004.
19. F. Bauspiess and F. Damm. Requirements for Cryptographic Hash Functions. *Computers and Security*, 11(5):427–437, September 1992.
20. M. Bednara, M. Daldrup, J. Shokrollahi, J. Teich, and J. von zur Gathen. Reconfigurable Implementation of Elliptic Curve Crypto Algorithms. In *9th Reconfigurable Architectures Workshop (RAW-02)*, pages 157–164, Fort Lauderdale, Florida, U.S.A., April 2002.
21. G. Bertoni, L. Breveglieri, P. Fragneto, M. Macchetti, and S. Marchesin. Efficient Software Implementation of AES on 32-bits Platforms. In *Proceedings of the CHES 2002*, volume 2523 of *Lecture Notes in Computer Science*, pages 159–171. Springer, 2002.
22. E. Biham. A Fast New DES Implementation in Software. In *FSE '97: Proceedings of the 4th International Workshop on Fast Software Encryption*, pages 260–272, London, UK, 1997. Springer-Verlag.
23. E. Biham. A Fast New DES Implementation in Software. In *4th Int. Workshop on Fast Software Encryption, FSE97*, pages 260–271, Haifa, Israel, January 1997. Springer-Verlag, 1997.
24. E. Biham and R. Chen. Near-Collisions of SHA-0. In *Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings*, volume 3152 of *Lecture Notes in Computer Science*, pages 290–305. Springer, 2004.
25. M. Bishop. An Application of a Fast Data Encryption Standard Implementation. In *Computing Systems, 1(3)*, pages 221–254, Summer 1988.
26. I. F. Blake, V. K. Murty, and G. Xu. A Note on Window $\tau$-NAF Algorithm. *Inf. Process. Lett.*, 95(5):496–502, 2005.
27. G. R. Blakley. A Computer Algorithm for the Product AB modulo M. *IEEE Transactions on Computers*, 32(5):497–500, May 1983.
28. A. Blasius. Generating a Rotation Reduction Perfect Hashing Function. *Mathematics Magazine*, 68(1):35–41, Feb 1995.

29. T. Blum and C. Paar. High-Radix Montgomery Modular Exponentiation on Reconfigurable Hardware. *IEEE Trans. Computers*, 50(7):759–764, 2001.
30. J. Bos and M. Coster. Addition Chain Heuristics. *In G. Brassard, (editor)* Advances in Cryptology —CRYPTO 89 *Lecture Notes in Computer Science*, 435:400–407, 1989.
31. A. Bosselaers, R. Govaerts, and J. Vandewalle. Fast Hashing on the Pentium. In *CRYPTO '96: Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology*, pages 298–312, London, UK, 1996. Springer-Verlag.
32. R. P. Brent and H. T. Kung. A Regular Layout for Parallel Adders. *IEEE Transactions on Computers*, 31(3):260–264, March 1982.
33. E. F. Brickell. A Fast Modular Multiplication Algorithm with Application to Two Key Cryptography. In *Advances in Cryptology, Proceedings of Crypto 86*, pages 51–60, New York, NY, 1982. Plenum Press.
34. E. F. Brickell. A Survey of Hardware Implementation of RSA (abstract). In *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings*, Lecture Notes in Computer Science, pages 368–370. Springer, 1989.
35. E. F. Brickell, D. M. Gordon, K. S. McCurley, and D. B. Wilson. Fast Exponentiation with Precomputation. *In R. A. Rueppel, (editor)* Advances in Cryptology —EUROCRYPT 92 *Lecture Notes in Computer Science*, 658:200–207, 1992.
36. M. Brown, D. Hankerson, J. López, and A. Menezes. Software Implementation of the NIST Elliptic Curves over Prime Fields. In *CT-RSA 2001: Proceedings of the 2001 Conference on Topics in Cryptology*, pages 250–265, London, UK, 2001. Springer-Verlag.
37. G. J. Calderon, J. Velasco-Medina, and J. López-Hernández. Implementación en Hardware del Algoritmo Rijndael [in spanish]. In *X Workshop IBERCHIP*, page 113, 2004.
38. D. Canright. A Very Compact S-Box for AES. In J. R. Rao and B. Sunar, editors, *Cryptographic Hardware and Embedded Systems - CHES 2005, 7th International Workshop, Edinburgh, UK, August 29 - September 1, 2005, Proceedings*, volume 3659 of *Lecture Notes in Computer Science*, pages 441–455. Springer, 2005.
39. Celoxica. Agility compiler, version 1.2, 2006.
40. CERTICOM. Certicom challenge: Eccp-109 solved. Available at: http://www.certicom.com/index.php, 2002.
41. CERTICOM. Certicom challenge: Ecc2-109 solved. Available at: http://www.certicom.com/index.php, 2004.
42. Certicom$^{TM}$. ECC Tutorial. http://www.certicom.com/index.php?action=ecc_tutorial,home.
43. N. S. Chang, C. H. Kim, Y. H. Park, and J. Lim. A Non-Redundant and Efficient Architecture for Karatsuba-Ofman Algorithm. In *Information Security, 8th International Conference, ISC 2005, Singapore, September 20-23, 2005, Proceedings*, volume 3650 of *Lecture Notes in Computer Science*, pages 288–299. Springer, 2005.
44. S. Charlwood and P. James-Roxby. Evaluation of the XC6200-Series Architecture for Cryptographic Application. In *FPL 98, Lecture Notes in Computer Science 1482*, pages 218–227. Springer-Verlag Berlin Heidelberg 2003, August/September 1998.

45. F. Charot, E. Yahya, and C. Wagner. Efficient Modular-Pipelined AES Implementation in Counter Mode on ALTERA FPGA. In *Field-Programable Logic and Applications*, pages 282–291, 2003.
46. R. C. C. Cheung, N. J. Telle, W. Luk, and P. Y. K. Cheung. Customizable Elliptic Curve Cryptosystems. *IEEE Trans. Computers on Very Large Scale Integration (VLSI) Systems*, 13(9):1048–1059, September 2005.
47. L. Childs. *A Concrete Introduction to Higher Algebra.* Springer-Verlag Berlin Heidelberg, Germany, 1995.
48. P. Chodowiec and K. Gaj. Very Compact FPGA Implementation of the AES Algorithm. In C. D. Walter, Ç. K. Koç, and C. Paar, editors, *Cryptographic Hardware and Embedded Systems - CHES 2003, 5th International Workshop, Cologne, Germany, September 8-10, 2003, Proceedings*, volume 2779 of *Lecture Notes in Computer Science*, pages 319–333. Springer, 2003.
49. 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 Math.*, 7:385–434, 1986.
50. J. Cruz-Alcaraz and F. Rodríguez-Henríquez. Multiplicaciốn Escalar en Curvas de Koblitz: Arquitectura en Hardware Reconfigurable (in spanish). In *XII-IBERCHIP Workshop, IWS-2006*, pages 1–10. Iberoamerican Development Program of Science and Technology (CYTED), March 2006.
51. J. Daemen. *Cipher and Hash Function Design, Strategies Based on Linear and Differential Cryptanalysis.* PhD thesis, Katholieke Universiteit Leuven, 1995.
52. J. Daemen and C. S. K. Clapp. Fast Hashing and Stream Encryption with PANAMA. In *FSE '98: Proceedings of the 5th International Workshop on Fast Software Encryption*, pages 60–74, London, UK, 1998. Springer-Verlag.
53. J. Daemen, R. G., and J. Vandewalle. A Hardware Design Model for Cryptographic Algorithms. In *ESORICS '92: Proceedings of the Second European Symposium on Research in Computer Security*, pages 419–434, London, UK, 1992. Springer-Verlag.
54. J. Daemen, R. Govaerts, and J. Vandewalle. Fast Hashing Both in Hardware and Software. *ESAT-COSIC Report 92-2*, Department of Electrical Engineering, Katholieke Universiteit Leuven, April 1992.
55. J. Daemen, R. Govaerts, and J. Vandewalle. A Framework for the Design of One-Way Hash Functions including Cryptanalysis of Damgård's One-Way Function based on a Cellular Automaton. In *ASIACRYPT*, pages 82–96, 1991.
56. J. Daemen and V. Rijmen. *The Design of Rijndael, AES-The Advance Encryption Standard.* Springer-Verlag Berlin Heidelberg, New York, 2002.
57. W. M. Dal and R. G. Kammer. FIPS 180-1: Secure Hash Standard SHA1, January 2000. Available at: http://www.nist.org.
58. I. Damgard. A Design Principle for Hash Functions. In *CRYPTO '89: Proceedings of the 9th Annual International Cryptology Conference on Advances in Cryptology*, pages 416–427, London, UK, 1990. Springer-Verlag.
59. A. Dandalis, V. K. Prasanna, and J. D. P. Rolim. A Comparitive Study of Performance of AES Candidates Using FPGAs. In *The Third AES3 Candidate Conference*, New York, April 2000.
60. M. Davio, Y. Desmedt, J. Goubert, F. Hoornaert, and J. J. Quisquater. Efficient Hardware and Software Implementations for the DES. In *Proc. of Crypto' 83*, pages 144–146, August 1984.

61. J. Deepakumara, H. Heys, and R. Venkatesan. FPGA Implementation of MD5 Hash Algorithm. In *Proceedings of the Canadian Conference on Electrical and Computer Engineering (CCECE)*, pages 919–924, Toronto, Canada, May 2001.
62. A. Desboves. Résolution, en nombres entiers et sous sa forme la plus générale, de l'équation cubique, homogène, à trois inconnues. *Nouvelles Annales de Mathématiques 3-éme série*, 5:545–579, 1886.
63. J.M. Diez, S. Bojanic, Lj. Stanimirovicc, C. Carreras, and O. Nieto-Taladriz. Hash Algorithms for Cryptographic Protocols: FPGA Implementations. In *Proceedings of the* $10^{th}$ *Telecommunications Forum, TELFOR2002*, Belgrade, Yugoslavia, May 26 -28, 2002.
64. W. Diffie and M. E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, November 1976.
65. V. S. Dimitrov, L. Imbert, and P. K. Mishra. Fast Elliptic Curve Point Multiplication using Double-Base Chains. Cryptology ePrint Archive, Report 2005/069, 2005. Available at: http://eprint.iacr.org/.
66. H. Dobbertin, A. Bosselaers, and B. Preneel. RIPEMD-160: A Strengthened Version of RIPEMD. In *Proceedings of the Third International Workshop on Fast Software Encryption*, pages 71–82, London, UK, 1996. Springer-Verlag.
67. S. Dominikus. A Hardware Implementation of MD4-Family Hash Algorithms. In *Proceedings of the 9th IEEE International Conference on Electronics, Circuits and Systems, ICECS 2002*, Dubrovnik, Croatia, Sep. 15–18 2002.
68. S. R. Dussé and B. S. Kaliski, Jr. A Cryptographic Library for the Motorola DSP56000. In *EUROCRYPT '90: Proceedings of the workshop on the theory and application of cryptographic techniques on Advances in cryptology*, pages 230–244, New York, NY, USA, 1991. Springer-Verlag New York, Inc.
69. M. Dworkin. NIST Special Publication 800-58C: Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, May 2004. Available at: http://csrc.nist.gov/CryptoToolkit/modes/.
70. M. Dworkin. NIST Special Publication 800-58B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005. Available at: http://csrc.nist.gov/CryptoToolkit/modes/.
71. Morris Dworkin. NIST Special Publication 800-58A: Recommendation for Block Cipher Modes of Operation, December 2001. Available at: http://csrc.nist.gov/CryptoToolkit/modes/.
72. H. Eberle. A High Speed DES Implementation for Network Applications. In *Advances in Cryptology-CRYPTO'92, Lecture Notes in Computer Science*, pages 521–539, Berlin, Germany, September 1992. Springer-Verlag.
73. H. Eberle, N. Gura, S. C. Shantz, and V. Gupta. A Cryptographic Processor for Arbitrary Elliptic Curves over $GF(2^m)$. Technical Report TR-2003-123, Sun Microsystem Laboratories, Available at: http://research.sun.com/, May 2003.
74. H. Eberle and C. P. Thacker. A 1 Gbit/Second GaAs DES Chip. In *IEEE 1992 Custom Integrated Circuits Conference*, pages 19.7/1–4, New York,USA, 1992. Springer-Verlag.
75. E. E. Swartzlander (editor). *Computer Arithmetic, volume I and II.* IEEE Computer Society Press, Los Alamitos, CA, 1990.
76. Ö. Eğecioğlu and Ç. K. Koç. Fast Modular Exponentiation. In E. Arıkan, editor, *Communication, Control, and Signal Processing: Proceedings of 1990 Bilkent International Conference on New Trends in Communication, Control, and Signal Processing*, pages 188–194. Elsevier, 1990.

77. A. Elbirt and C. Paar. Efficient Implementation of Galois Field Fixed Field Constant Multiplication. In *Third International Conference on Information Technology: New Generations, ITNG 2006*, pages 172–177. IEEE Computer Society, April 2006.
78. A. J. Elbirt, W. Yip, B. Chetwynd, and C. Paar. An FPGA-based Performance Evaluation of the AES Block Cipher Candidate Algorithm Finalists. *IEEE Trans. Very Large Scale Integr. Syst.*, 9(4):545–557, 2001.
79. J. Elbirt, W. Yip, B. Chetwyned, and C. Paar. A FPGA Implementation and Performance Evaluation of the AES Block Cipher Candidate Algorithm Finalist. In *The Third AES3 Candidate Conference*, New York, April 2000.
80. T. ElGamal. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Transactions on Information Theory*, 31(4):469–472, July 1985.
81. S. S. Erdem and Ç. K. Koç. A Less Recursive Variant of Karatsuba-Ofman Algorithm for Multiplying Operands of Size a Power of Two. In *16th IEEE Symposium on Computer Arithmetic (Arith-16 2003), 15-18 June 2003, Santiago de Compostela, Spain*, pages 28–35. IEEE Computer Society, 2003.
82. M. Ernst, M. Jung, F. Madlener, S. Huss, and R. Blümel. A Reconfigurable System on Chip Implementation for Elliptic Curve Cryptography over GF($2^{\mathrm{n}}$). In *Cryptographic Hardware and Embedded Systems - CHES 2002, 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002*, volume 2523 of *Lecture Notes in Computer Science*, pages 381–399. Springer-Verlag, 2003.
83. ETSI. European Telecommunications Standards Institute. URL: http://www.etsi.//org/.
84. ETSI. ETSI Technical Specification. Access Transmission Systems on Metallic Access Cables; Very High Speed Digital Subscriber Line (VDSL); Part 1: Functional requirements.
85. H. Fan and Y. Dai. Low Complexity Bit-Parallel Normal Bases Multipliers for GF($2^n$). *IEE Electronics Letters*, 40(1):24–26, 2004.
86. H. Fan and Y. Dai. Fast Bit-Parallel GF($2^n$) Multiplier for All Trinomials. *IEEE Trans. Computers*, 54(4):485–490, 2005.
87. H. Fan and M. Anwar Hasan. A New Approach to Subquadratic Space Complexity Parallel Multipliers for Extended Binary Fields. Centre for Applied Cryptographic Research (CACR) Technical Report CACR 2006-02, 2006. available at: http://www.cacr.math.uwaterloo.ca/.
88. D. C. Feldmeier. A High Speed Crypt Program, April 1989. Technical Memo TM-ARH-013711.
89. G. L. Feng. A VLSI Architecture for Fast Inversion in GF($2^m$). *IEEE Transactions on Computers*, 38(10):1383–1386, October 1989.
90. FIPS. Data Encryption Standard. Federal Information Standards Publication, Dec. 1993. Federal Information Processing Standards Publication 46-2.
91. FIPS (Federal Information Processing Standards Publication). *Secure Hash Standard: FIPS PUB 180.* Federal Information Processing Standards Publication, May 1993. Available at: http://www.nist.org.
92. K. Fong, D. Hankerson, J. López, and A. Menezes. Field Inversion and Point Halving Revisited. *IEEE Trans. Computers*, 53(8):1047–1059, 2004.
93. A. P. Fournaris and O. Koufopavlou. GF($2^k$) Multipliers Based on Montgomery Multiplication Algorithm. In *Proceedings of the 2004 International Symposium on Circuits and Systems ISCAS'04*, volume 2, pages 849–852, May 2004.

94. M. K. Franklin, editor. *Advances in Cryptology - CRYPTO 2004, 24th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings*, volume 3152 of *Lecture Notes in Computer Science*. Springer, 2004.
95. Free-DES. Free-DES Core (2000), March 2000. URL: http://www.free-ip.com/DES/.
96. Y. Fu, L. Hao, and X. Zhang. Design of an Extremely High Performance Counter Mode AES Reconfigurable Processor. In *Proceedings of the Second International Conference on Embedded Software and Systems (ICESS'05)*, pages 262–268. IEEE Computer Society, 2005.
97. G. Estrin. Organization of Computer Systems – the Fixed Plus Variable Structure Computer. In *Western Joint Computer Conference*, volume 3, pages 33–40, 1960.
98. K. Gaj and P. Chodowiec. Comparison of the Hardware Performance of the AES Candidates Using Reconfigurable Hardware. In *The Third AES3 Candidate Conference*, pages 40–54, New York, April 2000.
99. K. Gaj and P. Chodowiec. Fast Implementation and Fair Comparison of the Final Candidates for Advanced Encryption Standard Using Field Programmable Gate Arrays. In *CT-RSA 2001: Proceedings of the 2001 Conference on Topics in Cryptology*, pages 84–99, London, UK, 2001. Springer-Verlag.
100. M. García-Martínez, R. Posada-Gamez, G. Morales-Luna, and F. Rodríguez-Henríquez. FPGA Implementation of an Efficient Multiplier over Finite Fields GF($2^m$). In *International Conference on Reconfigurable Computing and FPGAs ReConFig05, Puebla City, Mexico*, pages 1–4, September 2005.
101. H. L. Garner. The Residue Number Systems. *IRE Transactions on Electronic Computers*, 8(6):140–147, June 1959.
102. J. Gathen and J. Shokrollahi. Efficient FPGA-Based Karatsuba Multipliers for Polynomials over $F_2$. In *Selected Areas in Cryptography, 12th International Workshop, SAC 2005, Kingston, ON, Canada, August 11-12, 2005, Revised Selected Papers*, volume 3897 of *Lecture Notes in Computer Science*, pages 359–369. Springer-Verlag, 2006.
103. P. Gauravaram, W. Millan, and J. Gonzalez-Nieto. Some Thoughts on Collision Attacks in the Hash Functions MD5, SHA-0 and SHA-1. Cryptology ePrint Archive, Report 2005/391, 2005. Available at: http://eprint.iacr.org/.
104. B. Gilchrist, J. H. Pomerene, and S. Y. Wong. Fast Carry Logic for Digital Computers. *IRE Transactions on Electronic Computers*, 4:133–136, 1955.
105. B. Gladman. The AES Algorithm (Rijndael) in C and C++. Available at: http://fp.gladman.plus.com/cryptography_technology/rijndael/.
106. O. Goldreich. *Foundations of Cryptography Volume 1, Basic Tools*. Cambridge University Press, 2003. Reprinted with corrections.
107. O. Goldreich. *Foundations of Cryptography Volume 2, Basic Applications*. Cambridge University Press, 2004.
108. D. Gollmann. Equally Spaced Polynomials, Dual Bases, and Multiplication in $F_{2^n}$. *IEEE Trans. Computers*, 51(5):588–591, 2002.
109. T. Good and M. Benaissa. AES on FPGA from the Fastest to the Smallest. In J. R. Rao and B. Sunar, editors, *Cryptographic Hardware and Embedded Systems - CHES 2005, 7th International Workshop, Edinburgh, UK, August 29 - September 1, 2005, Proceedings*, volume 3659 of *Lecture Notes in Computer Science*, pages 427–440. Springer, 2005.

110. J. Goodman and A. P. Chandrakasan. An Energy-Efficient Reconfigurable Public-Key Cryptography Processor. *IEEE Journal of Solid-State Circuits*, 36(11):1808–1820, Nov. 2001.

111. D. Gordon. Discrete Logaritms in $GF(P)$ Using the Number Field Sieve. *SIAM Journal on Discrete Mathematics*, 6:124–138, 1993.

112. D. M. Gordon. A Survey of Fast Exponentiation Methods. *Journal of Algorithms*, 27(1):129–146, April 1998.

113. C. Grabbe, M. B., J. Gathen, J. Shokrollahi, and J. Teich. A High Performance VLIW Processor for Finite Field Arithmetic. In *17th International Parallel and Distributed Processing Symposium (IPDPS 2003), 22-26 April 2003, Nice, France, CD-ROM/Abstracts Proceedings*, page 189. IEEE Computer Society, 2003.

114. C. Grabbe, M. Bednara, J. Teich, J. Gathen, and J. Shokrollahi. FPGA Designs of Parallel High Performance GF($2^{233}$) Multipliers. In *ISCAS (2)*, pages 268–271, 2003.

115. X. Gregg. Hashing Forth: It's a Topic Discussed so Nonchalantly that Neophytes Hesitate to Ask How it Works. *Forth Dimensions*, 17(4), 1995.

116. T. Grembowski, R. Lien, K. Gaj, N. Nguyen, P. Bellows, J. Flidr, T. Lehman, and B. Schott. Comparative Analysis of the Hardware Implementations of Hash Functions SHA-1 and SHA-512. In *ISC '02: Proceedings of the 5th International Conference on Information Security*, pages 75–89, London, UK, 2002. Springer-Verlag.

117. J. Guajardo and C. Paar. Efficient Algorithms for Elliptic Curve Cryptosystems. In *Advances in Cryptology-CRYPTO 97*, volume 1294 of *Lecture Notes in Computer Science*, pages 342–356, Berlin, Germany, 1997. Springer-Verlag.

118. J. Guajardo and C. Paar. Itoh-Tsujii Inversion in Standard Basis and Its Application in Cryptography and Codes. *Designs, Codes and Cryptography*, 25:207–216, 2002.

119. Z. Guo, B. Buyukkurt, W. Najjar, and K. Vissers. Optimized Generation of Data-Path from C Codes for FPGAs. In *DATE '05: Proceedings of the conference on Design, Automation and Test in Europe*, pages 112–117, Washington, DC, USA, 2005. IEEE Computer Society.

120. Z. Guo, W. Najjar, F. Vahid, and K. Vissers. A Quantitative Analysis of the Speedup Factors of FPGAs over Processors. In *FPGA '04: Proceedings of the 2004 ACM/SIGDA 12th international symposium on Field programmable gate arrays*, pages 162–170, New York, NY, USA, 2004. ACM Press.

121. N. Gura, S. Shantz, and H. Eberle et. al. An End-to-End Systems Approach to Elliptic Curve Cryptography. *Cryptographic Hardware and Embedded Systems - CHES 2002, 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers*, 2523:349–365, August 2003.

122. A. A. A. Gutub, M. K. Ibrahim, and A. Kayali. Pipelining GF(P) Elliptic Curve Cryptography Computation. In *International Conference on Communications, Circuits and Systems, 2005*, pages 93–99. IEEE Computer Society, March 2006.

123. A. A. A. Gutub, A. F. Tenca, E. Savas, and Ç. K. Koç. Scalable and Unified Hardware to Compute Montgomery Inverse in GF($P$) and GF($2^n$). *Cryptographic Hardware and Embedded Systems - CHES 2002, 4th International Workshop, Redwood Shores, CA, USA*, 2523:484–499, August 20002.

124. A. Halbutogullari and Ç. K. Koç. Mastrovito Multiplier for General Irreducible Polynomials. *IEEE Transactions on Computers*, 49(5):503–518, 2000.

125. A. Halbutogullari and Ç. K. Koç. Parallel Multiplication in using Polynomial Residue Arithmetic. *Des. Codes Cryptography*, 20(2):155–173, 2000.

126. T. R. Halfhill. MIPS Embraces Configurable Technology: Pro Series Processors with Corextend Compete with ARC and Tensilica, March 2003. Available at: http://www.altera.com/literature/lit-nio2.jsp.

127. P. Hämäläinen, M. Hännikäinen, and J. Saarinen. Configurable Hardware Implementation of Triple-DES Encryption Algorithm for Wireless Local Network. In *Proc. of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP2001)*, volume II, pages 1221–1224, Salt Lake City, USA, May 2001. IEEE.

128. D. Hankerson, J. López-Hernández, and A. Menezes. Software Implementation of Elliptic Curve Cryptography Over Binary Fields. *Cryptographic Hardware and Embedded Systems - CHES 2000, Second International Workshop, Worcester, MA, USA, August 17-18, 2000, Proceedings*, 1965:1–24, August 2000.

129. D. Hankerson, A. Menezes, and S. Vanstone. *Guide to Elliptic Cryptography.* Springer-Verlag, New York, 2004.

130. D. Harris, R. Krishnamurthy, M. Anders, S. Mathew, and S. Hsu. An Improved Unified Scalable Radix-2 Montgomery Multiplier. In *17th IEEE Symposium on Computer Arithmetic (ARITH-17 2005), 27-29 June 2005, Cape Cod, MA, USA*, pages 172–178. IEEE Computer Society, 2005.

131. M. A. Hasan. Efficient Computation of Multiplicative Inverses for Cryptographic Applications. In *15th IEEE Symposium on Computer Arithmetic*, Vail, Colorado, U.S.A., June 2001.

132. M. A. Hasan, M. Z. Wang, and V. K. Bhargava. A Modified Massey-Omura Parallel Multiplier for a Class of Finite Fields. *IEEE Transactions on Computers*, 42(10):1278–1280, November 1993.

133. S. M. Hernández-Rodríguez and F. Rodríguez-Henríquez. An FPGA Arithmetic Logic Unit for Computing Scalar Multiplication Using the Half-and-Add Method. In *IEEE International Conference on Reconfigurable Computing and FPGAs (ReConFig05)*, pages 1–7. IEEE Computer Society Press, September 2005.

134. Y. Hirano, T. Satoh, and F. Miura. Improved Extendible Hashing with High Concurrency. *Systems and Computers in Japan*, 26(13):1–11, 1995.

135. F. Hoornaert, M. Decroos, J. Vandewalle, and R. Govaerts. Fast RSA-Hardware: Dream or Reality? In *Advances in Cryptology — EUROCRYPT 88*, volume 330 of *Lecture Notes in Computer Science*, pages 257–264. Springer, 1988.

136. S. F. Hsiao and M. C. Chen. Efficient Substructure Sharing Methods for Optimising the Inner-Product Operations in Rijndael Advanced Encryption Standard. *IEE Proceedings on Computer and Digital Technology*, 152(5):653–665, September 2005.

137. M. Hutton, J. Rabaey, G. Delp, R. Vasishta, V. Betz, and S. Knapp. Will Power Kill FPGAs?, 2006. Session Chair-Mike Hutton.

138. K. Hwang. *Computer Arithmetic, Principles, Architecture, and Design.* John Wiley & Sons, New York, NY, 1979.

139. T. Ichikawa, T. Kasuya, and M. Matsui. Hardware Evaluation of the AES Finalists. In *The Third AES3 Candidate Conference*, pages 279–285, New York, April 2000.

140. IEEE. IEEE 802 LAN/MAN Standards Committee. URL: http://grouper.ieee.org/groups/802/index.html.

141. IEEE standards documents. *IEEE P1363: Standard Specifications for Public Key Cryptography. Draft Version D18.* IEEE, November 2004. http://grouper.ieee.org/groups/1363/.
142. J. L. Imana, J. M. Sanchez, and F. Tirado. Bit-Parallel Finite Field Multipliers for Irreducible Trinomials. *IEEE Transactions on Computers*, 55(5):520–533, 2006.
143. CAST Inc. DES Encryption Core. available from URL: http://www.cast-inc.com.
144. Xilinx Inc., V. Pasham, and S. Triemberger. High-speed DES and TripleDES Encryptor/Decryptor, August 2001. URL: http://www.xilinx.com/xapp/xapp270.pdf.
145. Y. Inoguchi. Outline of the Ultra Fine Grained Parallel Processing by FPGA. In *Seventh International COnference on High Performance Computing and Grid in Asia Pacific Region HPCAsia'04*, pages 434–441. IEEE Computer Society Press, July 2004.
146. ISO. ISO standard 8731-2, 1988. Available at: http://www.iso.org/.
147. ISO. ISO N179 AR Fingerprint Function. Working document, ISO-IEC/JTC1/SC27 /WG2, International Organization for Standardization, 1992.
148. ISO/IEC 15946. Information Technology - Security Techniques - Cryptographic techniques based on Elliptic Curve. *Committee Draft (CD),*, 1999. URL: http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CS NUMBER=31077.
149. T. Itoh and S. Tsujii. A Fast Algorithm for Computing Multiplicative Inverses in GF($2^m$) Using Normal Basis. *Information and Computing*, 78:171–177, 1988.
150. ITU. International Telecommunication Union. URL: http://www.itu.int/home/index.html.
151. K. Jarvinen, M. Tommiska, and J. Skytta. A Scalable Architecture for Elliptic Curve Point Multiplication. In *IEEE International Conference on Field-Programmable Technology, FPT2004*, pages 303–306. IEEE Computer Society Press, December 2004.
152. K. Jarvinen, M. Tommiska, and J. Skytta. Hardware Implementation Analysis of the MD5 Hash Algorithm. In *Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS'05) - Track 9*, page 298.1, Washington, DC, USA, 2005. IEEE Computer Society.
153. K. U. Jarvinen, M. T. Tommiska, and J. O. Skytta. A Fully Pipelined Memoryless 17.8 Gbps AES-128 Encryptor. In *Proc. of Int. Symp. Field-Programmable Gate-Arrays (FPGA2003*, pages 207–215, Monterey, CA, Feb. 2003.
154. J. Jedwab and C. J. Mitchell. Minimum Weight Modified Signed-Digit Representations and Fast Exponentiation. *IEE Electronics Letters*, 25(17):1171–1172, August 1989.
155. A. Joux. Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions. In *Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings*, volume 3152 of *Lecture Notes in Computer Science*, pages 306–316. Springer, 2004.
156. M. Joye and J. Quisquater. Hessian Elliptic Curves and Side-Channel Attacks. *Cryptographic Hardware and Embedded Systems - CHES 2001, Third International Workshop, Paris, France, May 14-16, 2001, Proceedings*, 2162:402–410, May 2001.

157. M. Joye and J. J. Quisquater, editors. *Cryptographic Hardware and Embedded Systems - CHES 2004: 6th International Workshop Cambridge, MA, USA, August 11-13, 2004. Proceedings*, volume 3156 of *Lecture Notes in Computer Science*. Springer, 2004.

158. B. S. Kaliski Jr. *RFC 1319: The MD2 Message-Digest Algorithm*. Internet Activities Board, April 1992.

159. B. S. Kaliski Jr., Ç. K. Koç, and C. Paar, editors. *Cryptographic Hardware and Embedded Systems - CHES 2002, 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers*, volume 2523 of *Lecture Notes in Computer Science*. Springer, 2003.

160. M. Juliato, G. Araujo, J. López, and R. Dahab. A Custom Instruction Approach for Hardware and Software Implementations of Finite Field Arithmetic over $\mathrm{F}_2^{163}$ using Gaussian Normal Bases. In *Proceedings of the 2005 IEEE International Conference on Field-Programmable Technology, FPT 2005, 11-14 December 2005, Singagore*, pages 5–12. IEEE Computer Society, 2005.

161. A. Kahate. *Cryptography and Network Security*. Tata McGraw-Hill, 2003.

162. Y. K. Kang, D. W. Kim, T. W. Kwon, and J. R. Choi. An Efficient Implementation of Hash Function Processor for IPSEC. In *Proceedings of 2002 IEEE Asia-Pacific Conference on ASIC*, pages 93–96, Taipei, Taiwan, Aug 2002.

163. J. P. Kaps and C. Paar. Fast DES Implementations for FPGAs and its Application to a Universal Key-Search Machine. In *Proc. 5th Annual Workshop on selected areas in cryptography-Sac' 98*, pages 234–247, Ontario, Canada, August 1998. Springer-Verlag, 1998.

164. A. Karatsuba and Y. Ofman. Multiplication of Multidigit Numbers on Automata. *Soviet Phys. Doklady (English Translation)*, 7(7):595–596, January 1963.

165. P. R. Karn. Karns DES implementation source code.

166. K. Kelley and D. Harris. Very High Radix Scalable Montgomery Multipliers. In *Proceedings of the 5th IEEE International Workshop on System-on-Chip for Real-Time Applications (IWSOC 2005), 20-24 July 2004, Banff, Alberta, Canada*, pages 400–404. IEEE Computer Society, 2005.

167. M. Khabbazian and T.A. Gulliver. A New Minimal Average Weight Representation for Left-to-Right Point Multiplication Methods. Cryptology ePrint Archive, Report 2004/266, 2004. Available at: http://eprint.iacr.org/.

168. J. H. Kim and D. H. Lee. A Compact Finite Field Processor over GF($2^m$) for Elliptic Curve Cryptography. In *IEEE International Conference on Communications, Circuits and Systems, ICCCAS 2002*, volume II, pages 340–342. IEEE Computer Society Press, May 2002.

169. P. Kitsos and O. Koufopavlou. Efficient Architecture and Hardware Implementation of the Whirlpool Hash Function. *IEEE Transactions on Consumer Electronics*, 50(1):208–214, February 2004.

170. V. Klima. Finding MD5 Collisions a Toy for a Notebook. Cryptology ePrint Archive, Report 2005/075, 2005. Available at: http://eprint.iacr.org/.

171. V. Klima. Tunnels in Hash Functions: MD5 Collisions Within a Minute. Cryptology ePrint Archive, Report 2006/105, 2006. Available at: http://eprint.iacr.org/.

172. E. W. Knudsen. Elliptic Scalar Multiplication Using Point Halving. In K. Y. Lam, E. Okamoto, and C. Xing, editors, *Advances in Cryptology - ASIACRYPT '99*, volume 1716 of *Lecture Notes in Computer Science*, pages 135–149. Springer, 1999.

173. L. R. Knudsen. SMASH A Cryptographic Hash Function. In *FSE*, pages 228–242, 2005. to appear.
174. D. E. Knuth. *The Art of Computer Programming 3rd. ed.* Addison-Wesley, Reading, Massachusetts, 1997.
175. N. Koblitz. Elliptic Curve Cryptosystems. *Mathematics of Computation*, 48(177):203–209, Janury 1987.
176. N. Koblitz. CM-Curves with Good Cryptographic Properties. In *CRYPTO*, volume 576 of *Lecture Notes in Computer Science*, pages 279–287. Springer, 1991.
177. Ç. K. Koç. High-Speed RSA Implementation. Technical Report TR 201, 71 pages, RSA Laboratories, Redwood City, CA, 1994.
178. Ç. K. Koç and T. Acar. Montgomery Multiplication in GF($2^k$). *Designs, Codes and Cryptography*, 14(1):57–69, 1998.
179. Ç. K. Koç and C. Y. Hung. Carry Save Adders for Computing the Product *AB* modulo *N*. *IEE Electronics Letters*, 26(13):899–900, June 1990.
180. Ç. K. Koç and C. Y. Hung. Multi-Operand Modulo Addition Using Carry Save Adders. *IEE Electronics Letters*, 26(6):361–363, March 1990.
181. Ç. K. Koç and C. Y. Hung. Bit-Level Systolic Arrays for Modular Multiplication. *Journal of VLSI Signal Processing*, 3(3):215–223, 1991.
182. Ç. K. Koç, D. Naccache, and C. Paar, editors. *Cryptographic Hardware and Embedded Systems - CHES 2001, Third International Workshop, Paris, France, May 14-16, 2001, Proceedings*, volume 2162 of *Lecture Notes in Computer Science*. Springer, 2001.
183. Ç. K. Koç and C. Paar, editors. *Cryptographic Hardware and Embedded Systems, First International Workshop, CHES'99, Worcester, MA, USA, August 12-13, 1999, Proceedings*, volume 1717 of *Lecture Notes in Computer Science*. Springer, 1999.
184. Ç. K. Koç and C. Paar, editors. *Cryptographic Hardware and Embedded Systems - CHES 2000, Second International Workshop, Worcester, MA, USA, August 17-18, 2000, Proceedings*, volume 1965 of *Lecture Notes in Computer Science*. Springer, 2000.
185. M. Kochanski. Developing an RSA Chip. In *Advances in Cryptology - CRYPTO '85, Santa Barbara, California, USA, August 18-22, 1985, Proceedings*, volume 218 of *Lecture Notes in Computer Science*, pages 350–357. Springer, 1985.
186. P. C. Kocher, J. Jaffe, and B. Jun. Differential Power Analysis. In *CRYPTO '99: Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*, pages 388–397, London, UK, 1999. Springer-Verlag.
187. I. Koren. *Computer Arithmetic Algorithms*. Prentice-Hall, Englewood Cliffs, NJ, 1993.
188. D. C. Kozen. *The Design and Analysis of Algorithms*. Springer-Verlag, New York, NY, 1992.
189. D. Kulkarni, W. A. Najjar, R. Rinker, and F. J. Kurdahi. Compile-time Area Estimation for LUT-based FPGAs. *ACM Trans. Des. Autom. Electron. Syst.*, 11(1):104–122, 2006.
190. N. Kunihiro and H. Yamamoto. New Methods for Generating Short Addition Chains. *IEICE Trans. Fundamentals*, E83-A(1):60–67, January 2000.
191. I. Kuon and J. Rose. Measuring the Gap Between FPGAs and ASICs. In *FPGA'06: Proceedings of the internation symposium on Field programmable gate arrays*, pages 21–30, New York, NY, USA, 2006. ACM Press.

192. A. Labbé and A. Pérez. AES Implementations on FPGA: Time Flexibility Tradeoff. In *Proceedings of FPL02*, pages 836–844, 2002.
193. RSA Laboratories. The Public-Key Cryptography Standards (PKCS), June 2002. Available at: http://www.rsasecurity.com/rsalabs/node.asp?id=2124.
194. RSA Laboratories. RSA Challenge. Available at: http://www.rsasecurity.com/rsalabs/node.asp?id=2092, November 2005.
195. RSA Laboratories. RSA Security, 2005. http://www.rsasecurity.com/rsalabs/.
196. R. E. Ladner and M. J. Fischer. Parallel Prefix Computation. *Journal of the ACM*, 27(4):831–838, 1980.
197. S. Lakshmivarahan and S. K. Dhall. *Parallelism in the Prefix Problem*. Oxford University Press, Oxford, London, 1994.
198. J. Lamoureux and S. J. E. Wilton. FPGA Clock Network Architecture: Flexibility vs. Area and Power. In *FPGA'06: Proceedings of the international symposium on Field programmable gate arrays*, pages 101–108, New York, NY, USA, 2006. ACM Press.
199. D. Laurichesse and L. Blain. Optimized Implementation of RSA Cryptosystem. *Computers & Security*, 10(3):263–267, May 1991.
200. S. O. Lee, S. W. Jung, C. H. Kim, J. Yoon, J. Y. Koh, and D. Kim. Design of Bit Parallel Multiplier with Lower Time Complexity. In *Information Security and Cryptology - ICISC 2003, 6th International Conference, Seoul, Korea, November 27-28, 2003, Revised Papers*, volume 2971 of *Lecture Notes in Computer Science*, pages 127–139. Springer-Verlag, 2004.
201. H. Leitold, W. Mayerwieser, U. Payer, K. C. Posch, R. Posch, and J. Wolkerstorfer. A 155 Mbps Triple-DES Network Encryptor. In *CHESS 2000*, pages 164–174, LNCS 1965, 2000. Springer-Verlag.
202. A. Lenstra and H. Lenstra, editors. *The Development of the Number Field Sieve, Lecture Notes in Mathematics 1554*. Springer-Verlag, 1993.
203. J. Leonard and W. H. Magione-Smith. A Case Study of Partially Evaluated Hardware Circuits: Key Specific DES. In *Field-Programmable Logic and Applications, FPL' 97*, pages 234–247, London, UK, September 1997. Springer-Verlag, 1997.
204. I. K. H. Leung and P. H. W. Leong. A Microcoded Elliptic Curve Processor using FPGA Technology. *IEEE Transactions on VLSI Systems*, 10(5):550–559, 2002.
205. S. Levy. The Open Secret. *Wired Magazine*, 7(04):1–6, April 1999. Available at: http://www.wired.com/wired/archive/7.04/crypto.html.
206. D. Lewis, E. Ahmed, G. Baeckler, V. Betz, and et al. The Stratix II Logic and Routing Architecture. In *FPGA '05: Proceedings of the 2005 ACM/SIGDA 13th international symposium on Field-programmable gate arrays*, pages 14–20, New York, NY, USA, 2005. ACM Press.
207. D. Lewis, V. Betz, D. Jefferson, A. Lee, C. Lane, P. Leventis, and et al. The Stratix 960; Routing and Logic Architecture. In *FPGA '03: Proceedings of the 2003 ACM/SIGDA eleventh international symposium on Field programmable gate arrays*, pages 12–20, New York, NY, USA, 2003. ACM Press.
208. J. D. Lipson. *Elements of Algebra and Algebraic Computing*. Addison-Wesley, Reading, MA, 1981.
209. Q. Liu, D. Tong, and X. Cheng. Non-Interleaving Architecture for Hardware Implementation of Modular Multiplication. In *IEEE International Symposium on Circuits and Systems, 2005. ISCAS 2005*, volume 1, pages 660–663. IEEE, May 2005.

210. J. López and R. Dahab. Improved Algorithms for Elliptic Curve Arithmetic in GF($2^n$). In *SAC'98*, volume 1556 of *Lecture Notes in Computer Science*, pages 201–212, 1998.

211. J. Lopez and R. Dahab. Fast Multiplication on Elliptic Curves over $GF(2^m)$ without Precomputation. *Cryptographic Hardware and Embedded Systems, First International Workshop, CHES'99, Worcester, MA, USA, August 12-13, 1999, Proceedings*, 1717:316–327, August 1999.

212. J. López-Hernández. Personal communication with J. López-Hernández, 2006.

213. E. López-Trejo, F. Rodríguez Henríquez, and A. Díaz-Pérez. An Efficient FPGA Implementation of CCM Mode Using AES. In *International Conference on Information Security and Cryptology*, volume 3935 of *Lecture Notes in Computer Science*, pages 208–215, Seoul, Korea, December 2005. Springer-Verlag.

214. A. K. Lutz, J. Treichler, F. K. Gurkaynak, H. Kaeslin, G. Basler, A. Erni, S. Reichmuth, P. Rommens, S. Oetiker, and W. Fitchtner. 2 Gbits/s Hardware Realization of RIJNDAEL and SERPENT-A Comparative Analysis. In *Proceedings of the CHES 2002*, volume 2523 of *Lecture Notes in Computer Science*, pages 171–184. Springer, 2002.

215. J. Lutz. High Performance Elliptic Curve Cryptographic Co-processor. Master's thesis, University of Waterloo, 2004.

216. R. Lysecky and F. Vahid. A Study of the Speedups and Competitiveness of FPGA Soft Processor Cores using Dynamic Hardware/Software Partitioning. In *DATE '05: Proceedings of the conference on Design, Automation and Test in Europe*, pages 18–23. IEEE Computer Society, 2005.

217. S. Mangard. A High Regular and Scalable AES Hardware Architecture. *IEEE Transactions on Computers*, 52(4):483–491, April 2003.

218. G. Martínez-Silva, F. Rodríguez-Henríquez, N. Cruz-Cortés, and L. G. De la Fraga. On the Generation of X.509v3 Certificates with Biometric Information. Technical report, CINVESTAV-IPN, April 2006. Available at: http://delta.cs.cinvestav.mx/ francisco/.

219. E. D. Mastrovito. VLSI Designs for Multiplication over Finite Fields GF $(2^{\mathrm{m}})$. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 6th International Conference, AAECC-6, Rome, Italy, July 4-8, 1988, Proceedings*, volume 357 of *Lecture Notes in Computer Science*, pages 297–309. Springer-Verlag, 1989.

220. R. J. McEliece. *Finite Fields for Computer Scientists and Engineers.* Kluwer Academic Publishers, Boston, MA, 1987.

221. R. P. McEvoy, F. M. Crowe, C. C. Murphy, and W. P. Marnane. Optimisation of the SHA-2 Family of Hash Functions on FPGAs. *ISVLSI 2006*, pages 317–322, 2006.

222. M. McLoone and J. V. McCanny. High Performance FPGA Rijndael Algorithm Implementation. In *Proceedings of the CHES 2001*, volume 2162 of *Lecture Notes in Computer Science*, pages 68–80. Springer, 2001.

223. M. McLoone and J.V. McCanny. Efficient Single-Chip Implementation of SHA-384 and SHA-512. In *Proceedings. 2002 IEEE International Conference on Field- Programmable Technology, FPT02*, volume 5, pages 311–314, Hong Kong, December 16-18, 2002.

224. M. McLoone and J.V. McCanny. High-performance FPGA Implementation of DES Using a Novel Method for Implementing the Key Schedule. *IEE Proc.: Circuits, Devices & Systems*, 150(5):373–378, October 2003.

225. M. McLoone, C. McIvor, and A. Savage. High-Speed Hardware Architectures of the Whirlpool Hash Function. In *FPT'05*, pages 147–162. IEEE Computer Society Press, 2005.
226. A. J. Menezes, I. F. Blake, X. Gao, R. C. Mullen, S. A. Vanstone, and T. Yaghoobian. *Applications of Finite Fields*. Kluwer Academic Publishers, Boston, MA, 1993.
227. A. J. Menezes, P. C. van Oorschot, and S. A.Vanstone. *Handbook of Applied Cryptography*. CRC Press, Boca Raton, Florida, 1996.
228. A.J. Menezes. *Elliptic Curve Public Key Cryptosystems*. Kluwer Academic Publishers, 1993.
229. Mentor Graphics. Catapult C, 2005.
230. Mentor Graphics, http://www.model.com/. *ModelSim*, 2005.
231. MentorGraphics, http://www.mentor.com/products/fpga_pld/synthesis/. *LeonardoSpectrum*, 2003.
232. R. Merkle. Secrecy, Authentication, and Public Key Systems. Stanford University, 1979.
233. R. C. Merkle. One Way Hash Functions and DES. In *CRYPTO '89: Proceedings on Advances in cryptology*, pages 428–446, New York, NY, USA, 1989. Springer-Verlag New York, Inc.
234. R. C. Merkle. A Fast Software One-Way Hash Function. *Journal of Cryptology*, 3:43–58, 1990.
235. V. Miller. Uses of Elliptic Curves in Cryptography. *In H. C. Williams (editor)* Advances in Cryptology — CRYPTO 85 Proceedings, *Lecture Notes in Computer Science*, 218:417–426, January 1985.
236. S. Miyaguchi, K. Ohta, and M. Iwata. 128-bit Hash Function (N-Hash). In *SECURICOM '90*, pages 123–137, 1990.
237. P. L. Montgomery. Modular Multiplication Without Trial Division. *Mathematics of Computation*, 44(170):519–521, April 1985.
238. P. L. Montgomery. Five, Six, and Seven-Term Karatsuba-Like Formulae. *IEEE Trans. Comput.*, 54(3):362–369, 2005.
239. F. Morain and J. Olivos. Speeding Up the Computations on an Elliptic Curve Using Addition-Subtraction Chains. Rapport de Recherche 983, INRIA, March 1989.
240. M. Morii, M. Kasahara, and D. L. Whiting. Efficient Bit-Serial Multiplication and the Discrete-Time Wiener-Hopf Equation over Finite Fields. *IEEE Transactions on Information Theory*, 35(6):1177–1183, 1989.
241. S. Morioka and A. Satoh. An Optimized S-Box Circuit Architecture for Low Power AES Design. In *Proceesings of the CHES 2002*, volume 2523 of *Lecture Notes in Computer Science*, pages 172–183. Springer, 2002.
242. K. Mukaida, M. Takenaka, N. Torii, and S. Masui. Design of High-Speed and Area-Efficient Montgomery Modular Multiplier for RSA Algorithm. In *IEEE Symposium on VLSI Circuits, 2004*, pages 320–323. IEEE Computer Society, 2004.
243. R. Murgai, R. K. Brayton, and A. Sangiovanni-Vincentelli. *Logic Synthesis for Field-Programmable Gate Arrays*. Kluwer Academic Publishers, Norwell, MA, USA, 1995.
244. M. Naor and M. Yung. Universal One-way Hash Functions and their Cryptographic Applications. In *STOC '89: Proceedings of the twenty-first annual ACM symposium on Theory of computing*, pages 33–43, New York, NY, USA, 1989. ACM Press.

245. J. Nechvatal. Public Key Cryptography. In *In G. Simmons ed. Contemporary Cryptology: The Science of Information Integrity*, Piseataway, NJ, 1992. IEEE Press.
246. C. Nègre. Quadrinomial Modular Arithmetic using Modified Polynomial Basis. In *International Symposium on Information Technology: Coding and Computing (ITCC 2005), Volume 1, 4-6 April 2005, Las Vegas, Nevada, USA*, pages 550–555. IEEE Computer Society, 2005.
247. M. Negrete-Cervantes, K. Gómez-Avila, and F. Rodríguez-Henríquez. Investigating Modular Inversion in Binary Finite Fields (in spanish). Technical Report CINVESTAV_COMP 2006-1, 29 pages, Computer Science Department CINVESTAV-IPN, Mexico, May 2006.
248. C. W. Ng, T. S. Ng, and K. W. Yip. A Unified Architecture of MD5 and RIPEMD-160 Hash Algorithms. In *Proceedings of IEEE International Symposium on Circuits and Systems, ISCAS 2004*, volume 2, pages II–889– II–892, Vancouver, Canada, 2004.
249. R. K. Nichols and P. C. Lekkas. *Wireless Security: Models, Threats, and Solutions.* McGraw Hill, 2000.
250. NIST. FIPS 46-3: Data Encryption Standard DES. Federal Information Processing Standards Publication 46-3, 1999. Available at:http://csrc.nist.gov/publications/fips/.
251. NIST. ANSI T1E1.4, Sep. 1 1999. Draft Technical Document, Revision16, Very High Speed Digital Subscriber Lines; System requirements.
252. NIST. Announcing the Advanced Encryption Standard AES. Federal Information Standards Publication, November 2001. Available at: http://csrc.nist.gov/CryptoToolkit/aes/index.html.
253. NIST. FIPS 186-2: Digital Signature Standard DSS. Federal Information Processing Standards Publication 186-2, October 2001. Available at:http://csrc.nist.gov/publications/fips/.
254. NIST. Secure Hash Signature Standard (SHS). Technical Report FIPS PUB 180-2, NIST, August 1 2002.
255. NIST. FIPS 186-3: Digital Signature Standard DSS. Federal Information Processing Standards Publication 186-3, march 2006. Available at: http://csrc.nist.gov/publications/drafts/.
256. Government Committee of Russia for Standards. Information Technology. Cryptographic Data Security. Hashing function, 1994. Gosudarstvennyi Standard of Russian Federation.
257. National Institute of Standards and Technology. NIST Special Publication 800-57: Recommendation for Key Management Part 1: General, August 2005.
258. J. V. Oldfield and R. C. Dorf. *Field Programmable Gate Arrays: Reconfigurable Logic for Rapid Prototyping and Implementations of Digital Systems.* John Wiley & Sons, Inc., New York, NY, USA, 1995.
259. J. K. Omura. A Public Key Cell Design for Smart Card Chips. In *International Symposium on Information Theory and its Applications*, pages 27–30, November 1990.
260. G. Orlando and C. Paar. A High-Performance Reconfigurable Elliptic Curve Processor for $GF(2^m)$. *Cryptographic Hardware and Embedded Systems - CHES 2000, Second International Workshop, Worcester, MA, USA, August 17-18, 2000, Proceedings*, 1965:41–56, August 2000.

261. G. Orlando and C. Paar. A Scalable $GF(P)$ Elliptic Curve Processor Architecture for Programmable Hardware. *Cryptographic Hardware and Embedded Systems - CHES 2001, Third International Workshop, Paris, France, May 14-16, 2001, Proceedings*, 2162:348–363, May 2001.
262. S. B. Örs, E. Oswald, and B. Preneel. Power-Analysis Attacks on an FPGA - First Experimental Results. In *Cryptographic Hardware and Embedded Systems - CHES 2003, 5th International Workshop, Cologne, Germany, September 8-10, 2003, Proceedings*, volume 2779 of *Lecture Notes in Computer Science*, pages 35–50. Springer, 2003.
263. E. Öztürk, B. Sunar, and E. Savas. Low-Power Elliptic Curve Cryptography Using Scaled Modular Arithmetic. In *Cryptographic Hardware and Embedded Systems - CHES 2004: 6th International Workshop Cambridge, MA, USA, August 11-13, 2004. Proceedings*, volume 3156 of *Lecture Notes in Computer Science*, pages 92–106. Springer, 2004.
264. G. Theodoridis P. Kitsos and O. Koufopavlou. An Efficient Reconfigurable Multiplier for Galois Field $GF(2^m)$. *Elsevier Microelectronics Journal*, 34(10):975–980, October 2003.
265. C. Paar. *Efficient VLSI Architectures for Bit Parallel Computation in Galois Fields.* PhD thesis, Universität GH Essen, 1994.
266. C. Paar. A New Architecture for a Parallel Finite Field Multiplier with Low Complexity Based on Composite Fields. *IEEE Transactions on Computers*, 45(7):856–861, July 1996.
267. C. Paar, P. Fleischmann, and P. Roelse. Efficient Multiplier Architectures for Galois Fields GF(2 $^{4n}$). *IEEE Trans. Computers*, 47(2):162–170, 1998.
268. C. Paar, P. Fleischmann, and P. Soria-Rodriguez. Fast Arithmetic for Public-Key Algorithms in Galois Fields with Composite Exponents. *IEEE Trans. Computers*, 48(10):1025–1034, 1999.
269. C. Patterson. High Performance DES Encryption in Virtex FPGAs using Jbits. In *Field-programmable custom computing machines, FCCM' 00*, pages 113–121, Napa Valley, CA, USA, January 2000. IEEE Comput. Soc., CA, USA, 2000.
270. V. A. Pedroni. *Circuit Design with VHDL.* The MIT Press, August 2004.
271. J. Pollard. Montecarlo Methods for Index Computacion (mod $p$). *Mathematics of Computation*, 13:918–924, 1978.
272. N. Pramstaller, C. Rechberger, and V. Rijmen. A Compact FPGA Implementation of the Hash Function Whirlpool. In *FPGA'06: Proceedings of the international symposium on Field Programmable Gate Arrays*, pages 159–166, New York, NY, USA, 2006. ACM Press.
273. B. Preneel. *Analysis and Design of Cryptographic Hash Functions.* PhD thesis, Katholieke Universiteit Leuven, 1993.
274. B. Preneel. Cryptographic Hash Functions. *European Transactions on Telecommunications*, 5(4):431–448, 1994.
275. B. Preneel. Design Principles for Dedicated Hash Functions. In *Fast Software Encryption, FSE 1993*, volume 809 of *Lecture Notes in Computer Science*, pages 71–82. Springer, 1994.
276. B. Preneel, R. Govaerts, and J. Vandewalle. Hash Functions Based on Block Ciphers: A Synthetic Approach. In *Advances in Cryptology - CRYPTO '93, 13th Annual International Cryptology Conference, Santa Barbara, California, USA, August 22-26, 1993, Proceedings*, volume 773 of *Lecture Notes in Computer Science*, pages 368–378. Springer, 1994.

277. J. J. Quisquater and C. Couvreur. Fast Decipherment Algorithm for RSA Public-Key Cryptosystem. *Electronics Letters*, 18(21):905–907, October 1982.

278. J. R. Rao and B. Sunar, editors. *Cryptographic Hardware and Embedded Systems - CHES 2005, 7th International Workshop, Edinburgh, UK, August 29 - September 1, 2005, Proceedings*, volume 3659 of *Lecture Notes in Computer Science*. Springer, 2005.

279. A. Reyhani-Masoleh. Efficient Algorithms and Architectures for Field Multiplication Using Gaussian Normal Bases. *IEEE Trans. Comput.*, 55(1):34–47, 2006.

280. A. Reyhani-Masoleh and M. A. Hasan. A New Construction of Massey-Omura Parallel Multiplier over GF(2). *IEEE Trans. Computers*, 51(5):511–520, 2002.

281. A. Reyhani-Masoleh and M. A. Hasan. Efficient Multiplication Beyond Optimal Normal Bases. *IEEE Trans. Computers*, 52(4):428–439, 2003.

282. A. Reyhani-Masoleh and M. A. Hasan. Low Complexity Bit Parallel Architectures for Polynomial Basis Multiplication over GF($2^m$). *IEEE Trans. Computers*, 53(8):945–959, 2004.

283. A. Reyhani-Masoleh and M. Anwar Hasan. Low Complexity Word-Level Sequential Normal Basis Multipliers. *IEEE Trans. Comput.*, 54(2):98–110, 2005.

284. V. Rijmen and P. S. L. M. Barreto. The Whirlpool Hash Function. First open NESSIE Workshop, Nov. 13–14 2000.

285. RIPE. RIPE Integrity Primitives: Final Report of RACE Integrity Primitives Evaluation (R1040). Technical report, Research and Development in Advanced Communication Technologies in Europe, June 1992.

286. R. Rivest. The Md4 Message Digest Algorithm. In *Advances in Cryptology – CRYPTO '90 Proceedings*, pages 303–311, 1991.

287. R. Rivest. The MD5 Message-Digest Algorithm. Technical Report Internet RFC-1321, IETF, 1992. http://www.ietf.org/rfc/rfc1321.txt.

288. Ronald L. Rivest. RSA Chips (Past/Present/Future). In *Advances in Cryptology, Proceedings of EUROCRYPT 84*, volume 209 of *Lecture Notes in Computer Science*, pages 159–165, 1984.

289. F. Rodríguez-Henríquez. New Algorithms and Architectures for Arithmetic in GF($2^m$) Suitable for Elliptic Curve Cryptography, PhD thesis: Oregon State University, 2000.

290. F. Rodríguez-Henríquez and Ç. K. Koç. On Fully Parallel Karatsuba Multipliers for $GF(2^m)$. In *International Conference on Computer Science and Technology (CST 2003)*, pages 405–410, Cancun, Mexico, May 2003.

291. F. Rodríguez-Henríquez and Ç. K. KoÇ. Parallel Multipliers Based on Special Irreducible Pentanomials. *IEEE Trans. Computers*, 52(12):1535–1542, 2003.

292. F. Rodríguez-Henríquez, C.E. Lōpez-Peza, and M.A León-Chávez. Comparative Performance Analysis of Public-Key Cryptographic Operations in the WTLS Handshake Protocol. In *1st International Conference on Electrical and Electronics Engineering ICEEE 2004*, pages 124–129. IEEE Computer Society, 2004.

293. F. Rodríguez-Henríquez, G. Morales-Luna, N. Saqib, and N. Cruz-Cortés. Parallel Itoh-Tsujii Multiplicative Inversion Algorithm for a Special Class of Trinomials. Cryptology ePrint Archive, Report 2006/035, 2006. http://eprint.iacr.org/.

294. F. Rodríguez-Henríquez, N. A. Saqib, and N. Cruz-Cortés. A Fast Implementation of Multiplicative Inversion over GF($2^m$). In *International Symposium*

*on Information Technology (ITCC 2005)*, volume 1, pages 574–579, Las Vegas, Nevada, U.S.A., April 2005.

295. F. Rodríguez-Henríquez, N. A. Saqib, and A. Díaz-Pérez. 4.2 Gbit/s Single-Chip FPGA Implementation of AES Algorithm. *IEE Electronics Letters*, 39(15):1115–1116, July 2003.
296. F. Rodríguez-Henríquez, N. A. Saqib, and A. Díaz-Pérez. A Fast Parallel Implementation of Elliptic Curve Point Multiplication over GF($2^m$). *Microprocessor and Microsystems*, 28(5-6):329–339, August 2004.
297. K. Rosen. *Elementary Number Theory and its Applications.* Addison-Wesley, Reading, MA, 1992.
298. G. Rouvroy, F. X. Standaert, J. J. Quisquater, and J. D. Legat. Design Strategies and Modified Descriptions to Optimize Cipher FPGA Implementations: Fast and Compact Results for DES and Triple-DES. In *FPL 2003*, volume 2778 of *Lecture Notes in Computer Science*, pages 181–193. Springer-Verlag Berlin Heidelberg 2003, 2003.
299. G. Rouvroy, F. X. Standaert, J. J. Quisquater, and J. D. Legat. Eficcient Uses of FPGAs for Implementations of DES and its Experimental Linear Cryptoanalysis. *IEEE Transactions on Computers*, 52(4):473–482, 2003.
300. G. Rouvroy, F. X. Standaert, J. J. Quisquater, and J. D. Legat. Compact and Efficient Encryption/Decryption Module for FPGA Implementation of AES Rijndael Very Well Suited for Embedded Applications. In *International Conference on Information Technology: Coding and Computing 2004 (ITCC2004)*, volume 2, pages 538–587, 2004.
301. A. Rudra, P. K. Dubey, C. S. Julta, V. Kumar, J. R. Rao, and P. Rohatgi. Efficient Rijndael Encryption Implementation with Composite Field Arithmetic. In *Proceedings of the CHES 2001*, volume 2162 of *Lecture Notes in Computer Science*, pages 171–184. Springer, 2001.
302. A. Rushton. *VHDL for Logic Synthesis.* John Wiley & Sons, Inc., New York, NY, USA, 1998.
303. G. P. Saggese, A. Mazzeo, N. Mazzocca, and A. G. M. Strollo. An FPGA-Based Performance Analysis of the Unrolling, Tiling, and Pipelining of the AES Algorithm. In *Field-Programable Logic and Applications FPL03, Lecture Notes in Computer Science 2778*, pages 292–302, 2003.
304. N. A. Saqib, A. Díaz-Pérez, and F. Rodríguez-Henríquez. Highly Optimized Single-Chip FPGA Implementations of AES Encryption and Decryption Cores. In *X Workshop Iberchip*, pages 117–118, Cartagena-Colombia, March 2004.
305. N. A. Saqib, F. Rodríguez-Henríquez, and A. Díaz-Pérez. Sequential and Pipelined Architecures for AES Implementation. In *Proceedings of the IASTED International Conference on Computer Science and Technology*, pages 159–163, Cancun, Mexico, May 2003. IASTED/ACTA Press.
306. N. A. Saqib, F. Rodríguez-Henríquez, and A. Díaz-Pérez. Two Approaches for a Single-Chip FPGA Implementation of an Encryptor/Decryptor AES Core. In *FPL 2003*, volume 2778 of *Lecture Notes in Computer Science*, pages 303–312. Springer-Verlag Berlin Heidelberg 2003, 2003.
307. N. A. Saqib, F. Rodríguez-Henríquez, and A. Díaz-Pérez. A Compact and Efficient FPGA Implementation of the DES Algorithm. In *International Conference on Reconfigurable Computing and FPGAs (ReConFig04)*, pages 12–18, Colima, Mexico, September 2004. Mexican Society for Computer Sciences.

308. N. A. Saqib, F. Rodríguez-Henríquez, and A. Díaz-Pérez. A Reconfigurable Processor for High Speed Point Multiplication in Elliptic Curves. *International Journal of Embedded Systems, (*In press *)*, 2006.
309. N. A. Saquib, F. Rodríguez-Henríquez, and A. Díaz-Pérez. AES Algorithm Implementation - An Efficient Approach for Sequential and Pipeline Architecures. In *Fourth Mexican International Conference on Computer Science*, pages 126–130, Tlaxcala-Mexico, September 2003. IEEE Computer Society Press.
310. A. Satoh and T. Inoue. ASIC-Hardware-Focused Comparison for Hash Functions MD5, RIPEMD-160, and SHS. In *ITCC '05: Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05) - Volume I*, pages 532–537, Washington, DC, USA, 2005. IEEE Computer Society.
311. A. Satoh and K. Takano. A Scalable Dual-Field Elliptic Curve Cryptographic Processor. *IEEE Transactions on Computers*, 52(4):449–460, April 2003.
312. E. Savas, M. Naseer, A. Gutub A.A, and Ç. K. Koç. Efficient Unified Montgomery Inversion with Multibit Shifting. *IEE Proceedings-Computers and Digital Techniques*, 152(4):489–498, July 2005.
313. E. Savas, A. F. Tenca, and Ç. K. Koç. A Scalable and Unified Multiplier Architecture for Finite Fields GF() and GF($2^m$). In *Cryptographic Hardware and Embedded Systems - CHES 2000, Second International Workshop, Worcester, MA, USA, August 17-18, 2000, Proceedings*, volume 1965 of *Lecture Notes in Computer Science*, pages 277–292. Springer-Verlag, 2000.
314. N. Schappacher. Développement de la loi de groupe sur une cubique. *Progress in Mathematics-Birkhäuser*, pages 159–184, 1991. available at:http://www-irma.u-strasbg.fr/ schappa/Publications.html.
315. B. Schneier. *Applied Cryptography*. John Wiley and Sons, New York, second edition edition, 1998.
316. C. P. Schnorr. FFT-Hashing, An Efficient Cryptographic Hash Function, 1991. Crypto'91 rump session, unpublished manuscript.
317. C. P. Schnorr. FFT-hash II, Efficient Cryptographic Hashing. *Lecture Notes in Computer Sciences*, 658:45–54, 1993.
318. C. P. Schnorr and S. Vaudenay. Parallel FFT-Hashing. In *Fast Software Encryption, Cambridge Security Workshop*, pages 149–156, London, UK, 1994. Springer-Verlag.
319. A. Schönhage. A Lower Bound for the Length of Addition Chains. *Theoretical Computer Science*, 1:1–12, 1975.
320. R. Schroeppel, C. Beaver, R. Gonzales, R. Miller, and T. Draelos. A low-power Design for an Elliptic Curve Digital Signature Chip. *Cryptographic Hardware and Embedded Systems - CHES 2002, 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers*, 2523:366–380, August 2003.
321. R. Schroeppel, H. Orman, S. W. O'Malley, and O. Spatscheck. Fast Key Exchange with Elliptic Curve Systems. In *CRYPTO '95: Proceedings of the 15th Annual International Cryptology Conference on Advances in Cryptology*, pages 43–56, London, UK, 1995. Springer-Verlag.
322. H. Sedlak. The RSA Cryptography Processor. In *Advances in Cryptology — EUROCRYPT 87*, volume 304 of *Lecture Notes in Computer Science*, pages 95–105, 1987.
323. A. Segredoas, E. Zabala, and G. Bello. Diseño de un Procesador Criptográfico Rijndael en FPGA [in spanish]. In *X Workshop IBERCHIP*, page 64, 2004.

324. V. Serrano-Hernández and F. Rodríguez-Henríquez. An FPGA Evaluation of Karatusba-Ofman Multiplier Variants (in spanish). Technical Report CINVESTAV_COMP 2006-2, 12 pages, Computer Science Department CINVESTAV-IPN, Mexico, May 2006.
325. A. Shamir. Turing Lecture on Cryptology: A Status Report. Available at: http://www.acm.org/awards/turing_citations/rivest-shamir-adleman.html, 2002.
326. M. B. Sherigar, A. S. Mahadevan, K. S. Kumar, and S. David. A Pipelined Parallel Processor to Implement MD4 Message Digest Algorithm on Xilinx FPGA. In *VLSID '98: Proceedings of the Eleventh International Conference on VLSI Design: VLSI for Signal Processing*, page 394, Washington, DC, USA, 1998. IEEE Computer Society.
327. C. Shu, K. Gaj, and T. A. El-Ghazawi. Low Latency Elliptic Curve Cryptography Accelerators for NIST Curves Over Binary Fields. In *Proceedings of the 2005 IEEE International Conference on Field-Programmable Technology, FPT 2005, 11-14 December 2005, Singagore*, pages 309–310. IEEE, 2005.
328. W. Shuhua and Z. Yuefei. A Timing-and-Area Tradeoff GF(P) Elliptic Curve Processor Architecture for FPGA. In *IEEE International Conference on Communications, Circuits and Systems, ICCCAS 2005*, pages 1308–1312. IEEE Computer Society Press, June 2005.
329. K. Siozios, G. Koutroumpezis, K. Tatas, D. Soudris, and A. Thanailakis. DAGGER: A Novel Generic Methodology for FPGA Bitstream Generation and its Software Tool Implementation. In *19th International Parallel and Distributed Processing Symposium (IPDPS 2005), CD-ROM / Abstracts Proceedings, 4-8 April 2005, Denver, CA, USA*. IEEE Computer Society, 2005.
330. N. Sklavos, P. Kitsos, K. Papadomanolakis, and O. Koufopavlou. Random Number Generator Architecture and VLSI Implementation. In *Proceedings of IEEE International Symposium on Circuits and Systems, ISCAS 2002*, pages IV–854- IV–857, Scottsdale, Arizona, May 2002.
331. N. Sklavos and O. Koufopavlou. On the Hardware Implementations of the SHA-2 (256, 384, 512) Hash Functions. In *Proceedings of IEEE International Symposium on Circuits and Systems, ISCAS 2003*, volume 5, pages V–153–V–156, Bangkok, Thailand, 2003.
332. K. R. Sloan, Jr. Comments on "A Computer Algorithm for the Product AB modulo M". *IEEE Transactions on Computers*, 34(3):290–292, March 1985.
333. N. Smart. The Hessian Form of an Elliptic Curve. *Cryptographic Hardware and Embedded Systems - CHES 2001, Third International Workshop, Paris, France, May 14-16, 2001, Proceedings*, 2162:118–125, May 2001.
334. N. Smart and E. Westwood. Point Multiplication on Ordinary Elliptic Curves over Fields of Characteristic Three. *Applicable Algebra in Engineering, Communication and Computing*, 13:485–497, 2003.
335. M. A. Soderstrand, W. K. Jenkins, G. A. Jullien, and editors F. J. Taylor. *Residue Arithmetic: Modern Applications in Digital Signal Processing.* IEEE Press, New York, NY, 1986.
336. J. Solinas. Generalized Mersenne Numbers. Technical Report CORR 1999-39, Dept. of Combinatorics and Optimization, Univ. of Waterloo, Canada, 1999.
337. J. A. Solinas. An Improved Algorithm for Arithmetic on a Family of Elliptic Curves. In *CRYPTO '97: Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology*, pages 357–371, London, UK, 1997. Springer-Verlag.

338. J. A. Solinas. Efficient Arithmetic on Koblitz Curves. *Des. Codes Cryptography*, 19(2-3):195–249, 2000.
339. F. Sozzani, G. Bertoni, S. Turcato, and L. Breveglieri. A Parallelized Design for an Elliptic Curve Cryptosystem Coprocessor. In *ITCC '05: Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05) - Volume I*, pages 626–630, Washington, DC, USA, 2005. IEEE Computer Society.
340. W. Stallings. *Cryptography and Network Security:* Principles and Practice. Prentice Hall, Upper Saddle River, New Jersey 07458, 1999.
341. F. X. Standaert, L. O. T. Oldenzeel, D. Samyde, and J. J. Quisquater. Power Analysis of FPGAs: How Practical is the Attack? In *Field Programmable Logic and Application, 13th International Conference, FPL 2003, Lisbon, Portugal, September 1-3, 2003, Proceedings*, volume 2778 of *Lecture Notes in Computer Science*, pages 701–711. Springer, 2003.
342. F. X. Standaert, S. B. Örs, and B. Preneel. Power Analysis of an FPGA: Implementation of Rijndael: Is Pipelining a DPA Countermeasure? In M. Joye and J. J. Quisquater, editors, *Cryptographic Hardware and Embedded Systems - CHES 2004: 6th International Workshop Cambridge, MA, USA, August 11-13, 2004. Proceedings*, volume 3156 of *Lecture Notes in Computer Science*, pages 30–44. Springer, 2004.
343. F. X. Standaert, S. B. Örs, J. J. Quisquater, and B. Preneel. Power Analysis Attacks Against FPGA Implementations of the DES. In *Field Programmable Logic and Application, 14th International Conference , FPL 2004, Leuven, Belgium, August 30-September 1, 2004, Proceedings*, volume 3203 of *Lecture Notes in Computer Science*, pages 84–94. Springer, 2004.
344. F. X. Standaert, G. Rouvroy, J. J. Quisquater, and J. D. Legat. Efficient Implementation of Rijndael Encryption in Reconfigurable Hardware: Improvements and Design Tradeoffs. In C. D. Walter, Ç. K. Koç, and C. Paar, editors, *Cryptographic Hardware and Embedded Systems - CHES 2003, 5th International Workshop, Cologne, Germany, September 8-10, 2003, Proceedings*, volume 2779 of *Lecture Notes in Computer Science*, pages 334–350. Springer, 2003.
345. D. R. Stinson. Combinatorial Techniques for Universal Hashing. *Computer and System Sciences*, 48(2):337–346, April 1994.
346. D. R. Stinson. Universal Hashing and Authentication Codes. *Designs, Codes and Cryptography*, 4(4):369–380, 1994.
347. B. Sunar. A Generalized Method for Constructing Subquadratic Complexity GF($2^k$) Multipliers. *IEEE Trans. Computers*, 53(9):1097–1105, 2004.
348. B. Sunar and Ç. K. Koç. Mastrovito Multiplier for All Trinomials. *IEEE Transactions on Computers*, 48(5):522–527, May 1999.
349. B. Sunar and Ç. K. Koç. An Efficient Optimal Normal Basis Type II Multiplier. *IEEE Trans. Computers*, 50(1):83–87, 2001.
350. E. J. Swankowski, R. R. Brooks, V. Narayanan, M. Kandemir, and M. J. Irwin. A Parallel Architecture for Secure FPGA Symmetric Encryption. In *18th International Parallel and Distributed Symposium IPDPS'04*, page 132. IEEE Computer Society, 2004.
351. Synopsys, http://www.synopsys.com/products/. *Galaxy Design Platform*, 2006.
352. N. S. Szabo and R. I. Tanaka. *Residue Arithmetic and its Applications to Computer Technology.* McGraw-Hill, New York, NY, 1967.

353. N. Takagi, J. Yoshiki, and K. Tagaki. A Fast Algorithm for Multiplicative Inversion in GF($2^m$) Using Normal Basis. *IEEE Transactions on Computers*, 50(5):394–398, May 2001.

354. Helion Tech. High Performance Solution in Silicon: AES (Rijndael) Cores. Available at: http://www.heliontech.com/core2.htm.

355. Helion Technology. Datasheet - High Performance MD5 Hash Core for Xilinx FPGA. url: http://www.heliontech.com/downloads/md5_xilinx_helioncore.pdf.

356. A. F. Tenca and Ç. K. Koç. A Scalable Architecture for Modular Multiplication Based on Montgomery's Algorithm. *IEEE Trans. Comput.*, 52(9):1215–1221, 2003.

357. J. P. Tillich and G. Zémor. Group-Theoretic Hash Functions. In *Algebraic Coding, First French-Israeli Workshop, Paris, France, July 19-21, 1993, Proceedings*, volume 781 of *Lecture Notes in Computer Science*, pages 90–110. Springer, 1993.

358. G. Todorov. ASIC Design, Implementation and Analysis of a Scalable High-Radix Montgomery Multiplier. Master's thesis, Oregon State University, December 2000.

359. W. Trappe and L.C. Washington. *Introduction to Cryptography with Coding Theory.* Prentice Hall, Inc., Upper Saddle River, NJ 07458, 2002.

360. S. Trimberger, R. Pang, and A. Singh. A 12 Gbps DES Encryptor/Decryptor Core in an FPGA. In *CHESS 2000*, pages 156–163, LNCS 1965, 2000. Springer-Verlag.

361. T. Tuan, S. Kao, A. Rahman, S. Das, and S. Trimberger. A 90nm Low-power FPGA for Battery-Powered Applications. In *FPGA '06: Proceedings of the internation symposium on Field programmable gate arrays*, pages 3–11, New York, NY, USA, 2006. ACM Press.

362. K. Underwood. FPGAs vs. CPUs: Trends in Peak Floating-Point Performance. In *FPGA '04: Proceedings of the 2004 ACM/SIGDA 12th international symposium on Field programmable gate arrays*, pages 171–180, New York, NY, USA, 2004. ACM Press.

363. George Mason University. Hardware IP Cores of Advanced Encryption Standard AES-Rijndael. Available at: http://ece.gmu.edu/crypto/rijndael.htm.

364. VASG. VHDL Analysis and Standardization Group, March 2003.

365. C. D. Walter. Systolic Modular Multiplication. *IEEE Transactions on Computers*, 42(3):376–378, March 1993.

366. C. D. Walter, Ç. K. Koç, and C. Paar, editors. *Cryptographic Hardware and Embedded Systems - CHES 2003, 5th International Workshop, Cologne, Germany, September 8-10, 2003, Proceedings*, volume 2779 of *Lecture Notes in Computer Science*. Springer, 2003.

367. X. Wang, D. Feng, X. Lai, and H. Yu. Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD. RUmp Session, Crypto 2004, Cryptology ePrint Archive, Report 2004/199, 2004. Available at: http://eprint.iacr.org/.

368. X. Wang, Y. L. Yin, and H. Yu. Finding collisions in the full sha-1. In *Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings*, volume 3621 of *Lecture Notes in Computer Science*, pages 17–36. Springer, 2005.

369. X. Wang and H. Yu. How to Break MD5 and Other Hash Functions. In *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings*, volume 3494 of *Lecture Notes in Computer Science*, pages 19–35. Springer, 2005.
370. S. Waser and M. J. Flynn. *Introduction to Arithmetic for Digital System Designers*. Holt, Rinehart and Winston, New York, NY, 1982.
371. P. Wayner. British Document Outlines Early Encryption Discovery, 1997. http://www.nytimes.com/library/cyber/week/122497encrypt.html.
372. N. Weaver and J. Wawrzynek. High Performance, Compact AES Implementations in Xilinx FPGAs. Technical report, U.C. Berkeley BRASS group, available at http://www.cs.berkeley.edu/ nnweaver/sfra/rijndael.pdf, 2002.
373. B. Weeks, M. Bean, T. Rozylowicz, and C. Ficke. Hardware Performance of Round 2 Advanced Encryption Standard Algorithms. In *The Third AES3 Candidate Conference*, New York, April 2000.
374. A. Weimerskirch and C. Paar. Generalizations of the Karatsuba Algorithm for Efficient Implementations. Ruhr-Universität-Bochum, Germany. Technical Report, 2003. available at: http://www.crypto.ruhr-uni-bochum.de/en_publications.html.
375. D. Whiting, R. Housley, and N. Ferguson. Counter with CBC-MAC (CCM). In *Submission to NIST*, 2002.
376. S. Wicker. *Error Control Systems for Digital Communication and Storage*. Prentice-Hall, Englewood Cliffs, NJ, 1995.
377. S. B. Wicker and V. K. Bhargava (editors). *Reed-Solomon Codes and Their Applications*. Prentice-Hall, Englewood Cliffs, NJ, 1994.
378. D. C. Wilcox, L. G. Pierson, P. J. Robertson, E. L. Witzke, and K. Gass. A DES ASIC Suitable for Network Encryption at 10 Gbs and Beyond. In *CHES 99*, pages 37–48, LNCS 1717, August 1999.
379. T. Wollinger, J. Guajardo, and C. Paar. Security on FPGAs: State-of-the-art Implementations and Attacks. *Trans. on Embedded Computing Sys.*, 3(3):534–574, 2004.
380. T. J. Wollinger and C. Paar. How Secure Are FPGAs in Cryptographic Applications? In *Field Programmable Logic and Application, 13th International Conference, FPL 2003, Lisbon, Portugal, September 1-3, 2003, Proceedings*, volume 2778 of *Lecture Notes in Computer Science*, pages 91–100. Springer, 2003.
381. K. Wong, M. Wark, and E. Dawson. A Single-Chip FPGA Implementation of the Data Encryption Standard (DES) Algorithm. In *IEEE Globecom Communication Conf.*, pages 827–832, Sydney, Australia, Nov. 1998.
382. K. W. Wong, E. C. W. Lee, L. M. Cheng, and X. Liao. Fast Elliptic Scalar Multiplication using New Double-base Chain and Point Halving. Cryptology ePrint Archive, Report 2006/124, 2006. Available at: http://eprint.iacr.org/.
383. H. Wu. Low Complexity Bit-Parallel Finite Field Arithmetic using Polynomial Basis. In Ç. K. Koç and C. Paar, editors, *Workshop on Cryptographic Hardware and Embedded Systems (CHES 99)*, volume 1717 of *Lecture Notes in Computer Science*, pages 280–291. Springer-Verlag, August 1999.
384. H. Wu. On Complexity of Squaring Using Polynomial Basis in GF($2^m$). In S. Tavares D. Stinson, editor, *Workshop on Selected Areas in Cryptography (SAC 2000)*, volume LNCS 2012, pages 118–129. Springer-Verlag, September 2000.

385. H. Wu. Montgomery Multiplier and Squarer for a Class of Finite Fields. *IEEE Trans. Computers*, 51(5):521–529, 2002.
386. H. Wu and M. A. Hasan. Low Complexity Bit-Parallel Multipliers for a Class of Finite Fields. *IEEE Trans. Computers*, 47(8):883–887, 1998.
387. H. Wu, M. A. Hasan, and I. F. Blake. New Low-Complexity Bit-Parallel Finite Field Multipliers Using Weakly Dual Bases. *IEEE Trans. Computers*, 47(11):1223–1234, 1998.
388. H. Wu, M. A. Hasan, I. F. Blake, and S. Gao. Finite Field Multiplier Using Redundant Representation. *IEEE Trans. Computers*, 51(11):1306–1316, 2002.
389. ANSI X9.62. Federal Information Processing Standard (FIPS) 46, National Bureau Standards, January 1977.
390. Xilinx, http://www.xilinx.com/support/techsup/tutorials/index.htm. *ISE 7 In-Depth Tutorial*, 2005.
391. Xilinx. MicroBlaze Soft Processor Core, 2005. Available at: http://www.xilinx.com/.
392. Xilinx, http://www.xilinx.com/bvdocs/publications/ds099.pdf. *Spartan-3 FPGA Family: Complete Data Sheet*, January 2005.
393. Xilinx. Virtex-4 Multi-Platform FPGA, 2005. Available at: http://www.xilinx.com/.
394. Xilinx. Virtex-II platform FPGAs: Complete Data Sheet, 2005. Available at: http://www.xilinx.com/.
395. Xilinx. Virtex-5 Multi-Platform FPGA, May 2006. Available at: http://www.xilinx.com/.
396. S. M. Yen. Improved Normal Basis Inversion in GF($2^m$). *IEE Electronic Letters*, 33(3):196–197, January 1997.
397. J. Zambreno, D. Nguyen, and A. Choudhary. Exploring Area/Delay Trade-offs in an AES FPGA Implementation. In *Proc. of Field Programmable Logic and Applications (FPL*, volume 3203 of *Lecture Notes in Computer Science*, pages 575–585. Springer-Verlag, 2004.
398. T. Zhang and K. K. Parhi. Systematic Design of Original and Modified Mastrovito Multipliers for General Irreducible Polynomials. *IEEE Transactions on Computers*, 50(7):734–749, 2001.
399. Y. Zheng, J. Pieprzyk, and J. Seberry. HAVAL A One-Way Hashing Algorithm with Variable Length of Output. In *ASIACRYPT '92: Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques*, pages 83–104, London, UK, 1993. Springer-Verlag.
400. J. Y. Zhou, X. G. Jiang, and H. H. Chen. An Efficient Architecture for Computing Division over GF($2^m$) in Elliptic Curve Cryptography. In *Proceedings of the 6th International Conference On ASIC, ASICON 2005*, volume 1, pages 274–277. IEEE Computer Society, October 2005.
401. D. Zibin and Z. Ning. FPGA Implementation of SHA-1 Algorithm. In *Proceedings of the* $5^{th}$ *International Conference on ASIC*, pages 1321–1324, Oct 2003.
402. J. zur Gathen and M. Nöcker. Polynomial and Normal Bases for Finite Fields. *J. Cryptology*, 18(4):337–355, 2005.

# Glossary

**Adittion Chains** An *addition chain* for an integer $m-1$ consists of a finite sequence of integers $U = (u_0, u_1, \ldots, u_t)$, and a sequence of integer pairs $V = ((k_1, j_1), \ldots, (k_t, j_t))$ such that $u_0 = 1$, $u_t = m-1$, and whenever $1 \leq i \leq t$, $u_i = u_{k_i} + u_{j_i}$. Addition chains are particularly useful for performing field exponentiation.

**Area (hardware)** Hardware resources occupied by the design. In terms of FPGAs, hardware area includes number of CLBs, memory blocks, IOBs, etc.

**Authentication** It is a security service related to identification. This function applies to both entities and information itself.

**Block cipher** A type of symmetric key cipher which operates on groups of bits of a fixed length, termed blocks.

**BlockRAMs** Built-in memory modules in FPGAs.

**Brute force attack** A brute force attack is brute force search for key space: trying all possible keys to recover plaintext from ciphertext.

**Cipher** A cipher is an algorithm for performing encryption and decryption.

**Ciphertext** An encrypted message is called ciphertext.

**CLB** Configurable logic block (CLB) is a programmable unit in FPGAs. A CLB can be reconfigured by the designer resulting a functionally new digital circuit.

**Confidentiality** It guarantees that sensitive information can only be accessed by those users/entities authorized to unveil it.

**Configurable Soc (CSoC)** CSoc integrates reconfigurable hardware, one or more processor and memory blocks on a single chip.

**Confusion** Confusion makes the output dependent on the key. Ideally every key bit influences every output bit.

**Cryptographic Security Strength** the Security strength of a given cryptographic algorithm is determined by the quality of the algorithm itself, the key size used and the block size handled by the algorithm.

**Data Integrity** It is a service which addresses the unauthorized alteration of data. This property refers to data that has not been changed, destroyed, or lost in a malicious or accidental manner.

**Decryption** The process of retrieving plaintext from ciphertext is called decryption.

**Diffie-Hellman Key Exchange Protocol** Invented in 1976 by Whitfield Diffie, Martin Hellman and Ralph Merkle, the Diffie-Hellman key exchange protocol was the first practical method for establishing a shared secret over an unprotected communication channel.

**Difussion** Diffusion makes the output dependent on the previous input (plaintext/ciphertext). Ideally each output bit is influenced by every input bit.

**Discrete Logarithm Problem** Given a number $p$, a generator $g \in \mathbb{Z}_p{}^*$ and an arbitrary element $a \in \mathbb{Z}_p{}^*$, find the unique number $i$, $0 \leq i < p-1$, such that $a \equiv g^i (mod\, p)$.

**Downstream** It defines the transmission from line terminal to network terminal (from customer to network premise).

**Elliptic curve** In mathematics, elliptic curves are defined by certain cubic (third degree) equations. They find applications in cryptography.

**Elliptic curve cryptography** Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the mathematics of elliptic curves.

**Elliptic Curve Discrete logarithmic problem** Let $E_{F_q}$ be an elliptic curve defined over the finite field $F_q$and let $P$ be a point $P \in E_{F_q}$ with primer order $n$. Consider the $k$-multiple of the point $P$, $Q = kP$ defined as the elliptic curve point resulting of adding $P$, $k-1$ times with itself, where $k$ is a positive scalar in $[\![1, n-1]\!]$. The elliptic curve discrete logarithm problem consists on finding the scalar $k$ that satisfies the equation $Q = kP$.

**Elliptic curve scalar multiplication** Let P be a point on Elliptic curve then the scalar product $n$P can be obtained by adding n copies of the same point P. The product $n$P = P + P+.........+ P obtained in this way is referred as elliptic curve scalar multiplication.

**Encryption** Encoding the contents of the message in such a way that it hides its contents from outsiders is called Encryption.

**Extended Euclidean Algorithm** In order to obtain the modular inverse of a number $a$ we may use the extended Euclidean algorithm, with which it is possible to find the two unique integer numbers $x$, $y$ that satisfy the equation, $ax + my = 1$.

**FPGA** A field-programmable gate array or FPGA is a gate array that can be reprogrammed, after it is manufactured.

**Full Adder** A full-adder is a combinational circuit with 3 input and 2 outputs. The inputs $A_i$, $B_i$, $C_i$ and the outputs $S_i$ and $C_{i+1}$ are boolean variables. It is assumed that $A_i$ and $B_i$ are the $i$th bits of the integers $A$ and $B$, respectively, and $C_i$ is the carry bit received by the $i$th position.

The FA cell computes the sum bit $S_i$ and the carry-out bit $C_{i+1}$ which is to be received by the next cell.

**Fundamental Theorem of Arithmetic** Any natural number $n > 1$ is either a prime number, or it can be factored as a product of powers of prime numbers $p_i$. Furthermore, except for the order of the factors, this factorization is unique.

**Granularity** Granularity of the reconfigurable logic is defined as the size of the smallest functional unit that can be addressed by device programming tools.

**Greatest common divisor** Given two integers $a$ and $b$ different than 0, we say that the integer $d > 1$ is the greatest common divisor, or *gcd*, of $a$ and $b$ if $d|a$, $d|b$ and for any other integer $c$ such that $c|a$ and $c|b$ then $c|d$. In other words, $d$ is the greatest positive number that divides both, $a$ and $b$.

**HDL** Hardware Description Languages (HDLs) are used for formal description of electronic circuits. They describe circuit's operation, its design, and tests to verify its operation by means of simulation. Typical HDL compilers tools, verify, compile and synthesize an HDL code, providing a list of electronic components that represent the circuit and also giving details of how they are connected.

**Integer Factorization Problem** Given an integer number $n$, obtain its prime factorization, i.e., find $n = {p_1}^{e_1}{p_2}^{e_2}{p_3}^{e_3}\cdots{p_k}^{e_k}$, where $p_i$ is a prime number and $e_i \geq 1$.

**Iterative Looping** It implements only one round and $n$ iterations of the algorithm are carried out by feeding back previous round results.

**JTAG** The Joint Test Action Group (JTAG) is the common name for the IEEE 1149.1 standard that defines the interface protocol between programmable devices and high-end computers.

**Key schedule** In cryptography, the algorithm for computing the sub-keys for each round in a block cipher from the encryption (or decryption) key is called the key schedule."

**Logic Cell** A logic cell is a very basic unit in FPGA which includes a 4-input function generator, carry logic, and a storage element (flip-flop).

**Look Up Table** A function generator in a logic cell is implemented as a look-up table which can be programmed to a desired Boolean logic, in addition, each look up table acts as a memory unit.

**Loop unrolling** It implements $n$ rounds of the algorithm, thus after an initial delay, output appears at each clock cycle.

**Message Digest** A cryptograph hash function takes a message of an arbitrary length and outputs a fixed length string, referred to as message digest or hash of that message. The purpose of message digest is to provide fingerprint of that message.

**Montgomery Multiplier** In 1985, P. L. Montgomery introduced an efficient algorithm for computing $R = A \cdot B \bmod n$ where $A$, $B$, and $n$ are $k$-bit binary numbers. The Montgomery reduction algorithm computes the resulting $k$-bit number $R$ without performing a division by the modulus $n$. Via an ingenious representation of the residue class modulo $n$, this algorithm replaces division by $n$ operation with division by a power of 2.

**Non-Repudiation** It is a security service which prevents an entity from denying previous commitments or actions.

**One Way Function** Is an injective function $f(x)$, such that $f(x)$ can be computed efficiently, but the computation of $f^{-1}(y)$ is computational intractable, even when using the most advanced algorithms along with the most sophisticated computer systems.

**One-way Trapdoor Function** We say that a one-way function is a One-way trapdoor function if is feasible to compute $f^{-1}(y)$ if and only if a supplementary information (usually the secret key) is provided.

**Permutation** Permutation refers to the rearrangement of an element. In cryptography, elements (bit strings) are generally permuted in according to some fixed permutation tables provided by the algorithm.

**Plaintext** In cryptographic terminology, message is called plaintext.

**Portable Digital Assistants(PDAs)** PDAs are handheld small computers that were originally designed as personal organizers. PDAs usually contain note pad, address book, task list, clock and calculator, etc. Modern PDAs are even more versatile. Most of them are equipped with an Intel XScale $\mu$Processor running at 400 MHz with up to 128MB of RAM memory.

**Reconfigurable computing** Denotes the use of reconfigurable hardware, also called custom computing.

**Reconfigurable hardware** Hardware devices in which the functionality of the logic gates is customizable at run-time. FPGAs is a type of reconfigurable hardware.

**Stream cipher** Stream ciphers encrypt each bit of the plaintext individually before moving on to the next.

**Substitution** Substitution refers to the replacement of an element with a new element. In cryptography, substitution operation is mainly used in block ciphers where an element is replaced with the elements from the substitution boxes called as S-boxes. The substituted values in some block ciphers can also be calculated.

**System-on-Chip (SoC)** SoC is a programmable platform which integrates many functions into a single chip. It may include analog as well digital components. A typical SoC includes one or more processing element (microcontroller/microprocessor or DSP), memory blocks, oscillators, analog to digital or digital to analog or both and other peripherals (counter timers, USB, Ethernet, power supply).

**Throughput** It is a measure for timing performance of a design and is calculated as: Throughput= (Allowed Frequency x Number of bits )/ Number of rounds (bits/s).

**Upstream** It defines the transmission from network terminal to line terminal (from network to customer premise).

# Index

# Signals and Communication Technology

(continued from page ii)

**Information Measures**
Information and its Description in Science and Engineering
C. Arndt ISBN 3-540-40855-X

**Processing of SAR Data**
Fundamentals, Signal Processing, Interferometry
A. Hein ISBN 3-540-05043-4

**Chaos-Based Digital Communication Systems**
Operating Principles, Analysis Methods, and Performance Evalutation
F.C.M. Lau and C.K. Tse
ISBN 3-540-00602-8

**Adaptive Signal Processing**
Application to Real-World Problems
J. Benesty and Y. Huang (Eds.)
ISBN 3-540-00051-8

**Multimedia Information Retrieval and Management Technological**
Fundamentals and Applications D. Feng, W.C. Siu, and H.J. Zhang (Eds.)
ISBN 3-540-00244-8

**Structured Cable Systems**
A.B. Semenov, S.K. Strizhakov,and I.R. Suncheley
ISBN 3-540-43000-8

**UMTS**
The Physical Layer of the Universal Mobile Telecommunications System
A. Springer and R. Weigel
ISBN 3-540-42162-9

**Advanced Theory of Signal Detection**
Weak Signal Detection in Generalized Obeservations
I. Song, J. Bae, and S.Y. Kim
ISBN 3-540-43064-4

**Wireless Internet Access over GSMand UMTS**
M. Taferner and E. Bonek
ISBN 3-540-42551-9

Printed in the United States of America.