Concurrent Error Detection in Polynomial Basis Multiplier over GF(2^m) Using Irreducible Trinomial

Hung-Wei Chang[1, *], Che-Wun Chiou[2], Fu-Hua Chou[3], and Wen-Yew Liang[1]

[1] Department of Computer Science and Information Engineering,
National Taipei University of Technology,
Taipei 106, Taiwan
{t6599009, wyliang}@ntut.edu.tw

[2] Department of Computer Science and Information Engineering,
Ching Yun University,
Chung-Li 320, Taiwan
cwchiou@cyu.edu.tw

[3] Department of Electronic Engineering,
Ching Yun University,
Chung-Li 320, Taiwan
fhchou@cyu.edu.tw

Received 20 June 2011; Revised 27 July 2011; Accepted 10 September 2011

Abstract. Due to the rapid development of smart-phones, mobile commerce becomes very popular and valuable. The communication and information security of the mobile commerce is heavily dependent on the public key cryptosystems such as RSA. However, existing public key cryptosystems are not available for the resource constrained devices like smart-phone. Therefore, the new elliptic curve cryptosystem with very low cost as compared to RSA is useful and suggested for mobile commerce. The polynomial basis multiplication is the most important arithmetic operation in the elliptic curve cryptosystem. A new and proved effective cryptanalysis is called fault based cryptanalysis. To protect such type cryptanalysis, the simple way is to redesign cryptosystems with concurrent error detection capability and only output error-free computed results. The polynomial basis multipliers generated by trinomials have advantages of low complexity and easy VLSI implementation. However, no existing polynomial basis multipliers which are generated by trinomials have concurrent error detection capability. Thus, a new polynomial basis multiplier using trinomial with concurrent error detection capability will be presented. As compared to other existing polynomial basis multipliers using general polynomials, the proposed polynomial basis multiplier using trinomial with concurrent error detection capability saves about 40% space complexity.

Keywords: Finite field arithmetic, concurrent error detection, polynomial basis multiplier, elliptic curve cryptosystem, fault based cryptanalysis

References

[1] F. J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes, North Holland, Amsterdam, 1988.

[2] R. Lidl and H. Niederreiter, Introduction to Finite Fields and their Applications, Cambridge University Press, New York, 1994.

[3] R. E. Blahut, Fast Algorithms for Digital Signal Processing, Addison-Wesley, 1985.

[4] I. S. Reed and T.K. Truong, “The Use of Finite Fields to Compute Convolutions,” *IEEE Transactions on Information Theory*, Vol. 21, No. 2, pp. 208-213, 1975.

[5] B. Benjauthrit and I. S. Reed, “Galois Switching Functions and Their Applications,” *IEEE Transactions on Computers*, Vol. C-25, No. 1, pp. 78-86, 1976.

[*] Correspondence author

[6] C.C. Wang and D. Pei, “A VLSI Design for Computing Exponentiations in GF(2^m) and Its Application to Generate Pseudorandom Number Sequences,” *IEEE Transactions on Computers*, Vol. 39, No. 2, pp. 258-262, 1990.

[7] E. Berlekamp, “Bit-serial Reed-solomon Encoders,” *IEEE Transactions on Information Theory*, Vol. 28, No. 6, pp. 869-874, 1982.

[8] M. Morii, M. Kasahara, D. L. Whiting, “Efficient Bit-serial Multiplication and the Discrete-time Wiener-hopf Equation Over Finite Fields,” *IEEE Transactions on Information Theory*, Vol. 35, No. 6, pp. 1177-1183, 1989.

[9] R. Schroeppel, H. Oman, S. O'Mallry, O. Sparscheck, “Fast Key Exchange with Elliptic Curve Systems,” in *Proceedings of Advances in Cryptology-CRYPTO*, Santa Barbara, California, USA, pp. 43-56, 1995.

[10] E.D. Win, A. Bosselaers, P. De Gersem, S. Vandenberghe, J. Vandewalle, “A Fast Software Implementation for Arithmetic Operations in GF (2^n),” in *Proceedings of Advances in Cryptology - ASIACRYPT'96*, Kyongju, Korea, pp. 65-76, 1996.

[11] A. J. Menezes and I. F. Blake, Applications of Finite Fields, Springer, 2010.

[12] C.Y. Lee, “Low Complexity Bit-parallel Systolic Multiplier Over GF(2^m) Using Irreducible Trinomials,” *IEE Proceedings-Computers and Digital Techniques*, Vol. 150, No. 1, pp. 39-42, 2003.

[13] 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.

[14] C.W. Chiou, L.C. Lin, F.H. Chou, S.F. Shu, “Low-complexity Finite Field Multiplier Using Irreducible Trinomials,” *Electronics Letters*, Vol. 39, No. 24, pp. 1709-1711, 2003.

[15] C.W. Chiou, C.Y. Lee, J.M. Lin, “Efficient Systolic Arrays for Power-sum, Inversion, and Division in GF (2^m),” *International Journal of Computer Sciences and Engineering Systems*, Vol. 1, No. 1, pp. 27-41, 2007.

[16] C.Y. Lee, Y.H. Chen, C.W. Chiou, J.M. Lin, “Unified Parallel Systolic Multiplier Over GF(2^m),” *Journal of Computer Science and Technology*, Vol. 22, No. 1, pp. 28-38, 2007.

[17] C.Y. Lee, J.M. Lin, C.W. Chiou, “Scalable and Systolic Architecture for Computing Double Exponentiation Over GF (2^m),” *Acta Applicandae Mathematicae*, Vol. 93, No. 1, pp. 161-178, 2006.

[18] J. L. Massey and J. K. Omura, Computational method and apparatus for finite field arithmetic, in US patent, pp. 627, 1986.

[19] A. Reyhani-Masoleh and M. A. Hasan, “A New Construction of Massey-Omura Parallel Multiplier Over GF(2^m),” *IEEE Transactions on Computers*, Vol. 51, No. 5, pp. 511-520, 2002.

[20] C.Y. Lee and C.W. Chiou, “Efficient Design of Low-complexity Bit-parallel Systolic Hankel Multipliers to Implement Multiplication in Normal and Dual Bases of GF (2^m),” I*EICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, Vol. 88, No. 11, pp. 3169-3179, 2005.

[21] C.W. Chiou and C.Y. Lee, “Multiplexer-based Double-exponentiation for Normal Basis of GF (2^m),” *Computers & Security*, Vol. 24, No. 1, pp. 83-86, 2005.

[22] H. Wu, M. A. Hasan, I. F. Blake, “New Low-complexity Bit-parallel Finite Field Multipliers Using Weakly Dual Bases,” *IEEE Transactions on Computers*, Vol. 47, No. 11, pp. 1223-1234, 1998.

[23] C.Y. Lee, C.W. Chiou, J.M. Lin, “Concurrent Error Detection in a Bit-parallel Systolic Multiplier for Dual Basis of GF (2^m),” *Journal of Electronic Testing*, Vol. 21, No. 5, pp. 539-549, 2005.

[24] J. Kelsey, B. Schneier, D. Wagner, H. Hall, “Side Channel Cryptanalysis of Product Ciphers,” *Journal of Computer Security*, Vol. 8, No. 2, pp. 141-158, 2000.

[25] E. Biham and A. Shamir, "Differential Fault Analysis of Secret Key Cryptosystems," in *Proceedings of Advances in Cryptology — CRYPTO'97*, Santa Barbara, California, USA, pp. 513-525, 1997.

[26] D. Boneh, R. DeMillo, R. Lipton, "On the Importance of Checking Cryptographic Protocols for Faults," in *Proceedings of Advances in Cryptology-EUROCRYPT'97*, Konstanz, Germany, Vol. 1233, pp. 37-51, 1997.

[27] R. Karri, G. Kuznetsov, M. Goessel, "Parity-based Concurrent Error Detection of Substitution-permutation Network Block Ciphers," in *Proceedings of Cryptographic Hardware and Embedded Systems-CHES 2003*, Cologne, Germany, pp. 113-124, 2003.

[28] G. Bertoni, L. Breveglieri, IP. Koren Maistri, V. Piuri, "Error Analysis and Detection Procedures for a Hardware Implementation of the Advanced Encryption Standard," *IEEE Transactions on Computers*, Vol. 52, No. 4, pp. 492-505, 2003.

[29] M. Joye, A. K. Lenstra, J. J. Quisquater, "Chinese Remaindering Based Cryptosystems in the Presence of Faults," *Journal of Cryptology*, Vol. 12, No. 4, pp. 241-245, 1999.

[30] D. Boneh, R. DeMillo, R. J. Lipton, "On the importance of Eliminating Errors in Cryptographic Computations," *Journal of Cryptology*, Vol. 14, No. 2, pp. 101-119, 2001.

[31] S. Fenn, M. Gossel, M. Benaissa, D. Taylor, "On-line Error Detection for Bit-serial Multipliers in GF (2^m)," *Journal of Electronic Testing*, Vol. 13, No. 1, pp. 29-40, 1998.

[32] A. Reyhani-Masoleh and M. A. Hasan, "Error Detection in Polynomial Basis Multipliers Over Binary Extension Fields," in *Proceedings of Cryptographic Hardware and Embedded Systems - CHES 2002*, CA, USA, pp. 515-528, 2003.

[33] C.W. Chiou, "Concurrent Error Detection in Array Multipliers for GF (2^m) Fields," *Electronics Letters*, Vol. 38, No. 14, pp. 688-689, 2002.

[34] C.Y. Lee, C.W. Chiou, J.L. Lin, "Concurrent Error Detection in a Polynomial Basis Multiplier Over GF (2^m)," *Journal of Electronic Testing*, Vol. 22, No. 2, pp. 143-150, 2006.

[35] C.W. Chiou, C.Y. Lee, A.W. Deng, J.M. Lin, "Concurrent Error Detection in Montgomery Multiplication Over GF (2^m)," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, Vol. 89, No. 2, pp. 566-574, 2006.

[36] J. H. Patel and L.Y. Fung, "Concurrent Error Detection in ALU's by Recomputing with Shifted Operands," *IEEE Transactions on Computers*, Vol. C-31, No.7, pp. 589-595, 1982.

[37] J. H. Patel, L.Y. Fung, "Concurrent Error Detection in Multiply and Divide Arrays," *IEEE Transactions on Computers*, Vol. C-32, No. 4, pp. 417-422, 1983.

[38] J. F. Wakerly, Error Detecting Codes, Self-checking Circuits and Applications, Elsevier, 1978.

[39] C.L. Wang and, J.L. Lin, "Systolic Array Implementation of Multipliers for Finite Fields GF (2^m)," *IEEE Transactions on Circuits and Systems*, Vol. 38, No. 7, pp. 796-800, 1991.

[40] N. H. E. Weste, K. Eshraghian, M. J. S. Smith, in Principles of CMOS VLSI Design: A Systems Perspective with Verilog/VHDL Manual, Addison Wesley, 2000.

[41] M74HC86, Quad Exclusive OR Gate, STMicroelectronics,http://www.st.com/stonline/books/pdf/docs/2006.pdf

[42] M74HC08, Quad 2-input AND Gate, STMicroelectronics, http://www.st.com/stonline/books/pdf/docs/1885.pdf

[43] M74HC279, Quad S-R Latch, STMicroelectronics, http://www.st.com/stonline/books/pdf/docs/1937.pdf

[44] M74HC32, Quad 2-input OR Gate, STMicroelectronics, http://www.st.com/stonline/books/pdf/docs/1944.pdf

[45] M74HC11, Triple 3-input AND Gate, STMicroelectronics, http://www.st.com/stonline/books/pdf/docs/1890.pdf

[46] M74AC157, Quad 2 Channel Multiplexer, STMicroelectronics, http://www.st.com/stonline/books/pdf/doce/5144.pdf