Design of Polynomial Basis Multiplier over GF(2^m) for Resisting Fault-Based Cryptanalysis and Off-Line Testing

Che-Wun Chiou[1, *], Wen-Tzeng Huang[2], Chi-Hsiang Chang[3], Chiou-Yng Lee[4], Jim-Min Lin[5], and Yun-Chi Yeh[6]

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

[2] Department of Computer Science and Information Engineering,
Minghsin University of Science and Technology,
Hsinchu 304, Taiwan
wthuang@must.edu.tw

[3] Institute of Computer and Communication,
National Taipei University of Technology,
Taipei 106, Taiwan
garychang0706@gmail.com

[4] Department of Computer Information and Network Engineering,
Lunghwa University of Science and Technology,
Taoyuan 333, Taiwan
PP010@mail.lhu.edu.tw

[5] Department of Information Engineering and Computer Science,
Feng Chia University,
Taichung 407, Taiwan
jimmy@fcu.edu.tw

[6] Department of Electronic Engineering,
Ching Yun University,
Jhong-Li 320, Taiwan
yunchi@cyu.edu.tw

Received 12 June 2011; Revised 5 August 2011; Accepted 6 September 2011

Abstract. There are two popular approaches for designing polynomial basis (PB) multiplier over GF(2^m) with concurrent error detection (CED) capability to resist fault-based cryptanalysis, i.e., the parity checking and the REcomputing with Shifted Operands (RESO) approaches. The RESO approach is suited to VLSI chips. However, the systolic PB multiplier using the RESO approach will unavoidably break the regular structure when detecting errors occurred on feedback lines. The parity checking method for single parity bit can be easily extended to the one with multiple parity bits. However, the drawback of a parity checking method is the dependence on multiplier architectures, and can detect only odd number of errors. To overcome these problems, we present a novel approach, termed self-checking alternating logic (SCAL) approach, to detect errors in a systolic PB multiplier. The proposed SCAL systolic PB multiplier can keep the regular structure and takes less time overhead than existing PB multipliers with CED also. Moreover, the proposed one has the self-testing property which can ensure that there is at least one input can detect the occurred fault.

Keywords: Information security, elliptic curve cryptosystem, fault attacks, finite fields, polynomial basis multiplication, error detection, alternating logic

*Correspondence author

References

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

[2] N. Koblitz, "Elliptic Curve Cryptosystems," *Mathematics of Computation*, Vol. 48, pp. 203-209, 1987.

[3] V. S. Miller, "Use of Elliptic Curves in Cryptography," *Advances in Cryptology Crypto'85*, pp. 417-426, 1986.

[4] E. R. Berlekamp, "Bit-Serial Reed-Solomon Encoder," *IEEE Transactions on Information Theory*, Vol. IT-28, No. 6, pp. 869-874, 1982.

[5] R. E. Blahut, Fast Algorithms for Digital Signal Processing, Boston: Addison-Wesley Longman Publishing Company Press, 1985.

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

[7] T. C. Bartee and D. I. Schneider, "Computation with Finite Fields," *Information and Computing*, Vol. 6, No. 2, pp. 79-98, 1963.

[8] E. D. Mastrovito, "VLSI Designs for Multiplication over Finite Field GF(2^m)," in *Proceedings of the 6th International Conference, on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, Rome, Italy, pp. 297-309, 1988.

[9] Ç. K. Koç and B. Sunar, "Low-Complexity Bit-Parallel Canonical and Normal Basis Multipliers for a Class of Finite Fields," *IEEE Transactions on Computers*, Vol. 47, No. 3, pp. 353-356, 1998.

[10] T. Itoh and S. Tsujii, "Structure of Parallel Multipliers for a Class of Fields GF(2^m)," *Information and Computation*, Vol. 83, No. 1, pp. 21-40, 1989.

[11] M. A. Hasan, M.Z. Wang, V. K. Bhargava, "Modular Construction of Low Complexity Parallel Multipliers for a Class of Finite Fields GF(2^m)," *IEEE Transactions on Computers*, Vol. 41, No. 8, pp. 962-971, 1992.

[12] C.Y. Lee, E.H. Lu, J.Y. Lee, "Bit-Parallel Systolic Multipliers for GF(2^m) Fields Defined by All-One and Equally-spaced Polynomials," *IEEE Transactions on Computers*, Vol. 50, No. 5, pp. 385-393, 2001.

[13] C. Paar, P. Fleischmann, P. Roelse, "Efficient Multiplier Architectures for Galois Fields GF(2^{4n})," *IEEE Transactions on Computers*, Vol. 47, No. 2, pp. 162-170, 1998.

[14] 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. 1-3, pp. 161-178, 2006.

[15] C.Y. Lee, C.W. Chiou, A.W. Deng, J.M. Lin, "Low-Complexity Bit-Parallel Systolic Architectures for Computing $A(x)B^2(x)$ over GF(2^m)," *IEE Proceedings-Circuits, Devices and Systems*, Vol. 153, No. 4, pp. 399-406, 2006.

[16] S. S. Erdem, T. Yanlk, Ç. K. Koç, "Polynomial Basis Multiplication over GF(2^m)," *Acta Applicandae Mathematicae*, Vol. 93, No. 1-3, pp. 33-55, 2006.

[17] J. L. Massey and J. K. Omura, "Computational Method and Apparatus for Finite Field Arithmetic," U.S. Patent Number 4,587,627, 1986.

[18] C.C. Wang, T.K. Truong, H.M. Shao, L. J. Deutsch, J. K. Omura, I. S. Reed, "VLSI Architectures for Computing Multiplications and Inverses in GF(2^m)," *IEEE Transactions on Computers*, Vol. 34, No. 8, pp. 709-717, 1985.

[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] H.N. Fan and Y.Q. Dai, "Key Function of Normal Basis Multipliers in GF(2^n)," *IEE Electronics Letters*, Vol. 38, No. 23, pp.1431-1432, 2002.

[21] 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)," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science*, Vol. E88-A, No. 11, pp. 3169-3179, 2005.

[22] H.P. 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] H.P. Wu and M. A. Hasan, "Low Complexity Bit-Parallel Multipliers for a Class of Finite Fields," *IEEE Transactions on Computers*, Vol. 47, No. 8, pp. 883-887, 1998.

[24] S. T. J. Fenn, M. Benaissa, D. Taylor, "GF(2^m) Multiplication and Division over the Dual Basis," *IEEE Transactions on Computers*, Vol. 45, No. 3, pp. 319-327, 1996.

[25] C.C. Wang, "An Algorithm to Design Finite Field Multipliers Using a Self-Dual Normal Basis," *IEEE Transactions on Computers*, Vol. 38, No. 10, pp. 1457-1460, 1989.

[26] S. T. J. Fenn, M. Benaissa, D. Taylor, "Dual Basis Systolic Multipliers for GF(2^m)," *IEE Proceedings Computer and Digital Techniques*, Vol. 144, No. 1, pp. 43-46, 1997.

[27] M. Wang and I. F. Blake, "Bit Serial Multiplication in Finite Fields," *SIAM Journal on Discrete Mathematics*, Vol. 3, No. 1, pp. 140-148, February 1990.

[28] M. Diab and A. Poli, "New Bit-Serial Systolic Multiplier for GF(2^m) Using Irreducible Trinomials," *IEE Electronics Letters*, Vol. 27, No. 13, pp. 1183-1184, 1991.

[29] D. Boneh, R. DeMillo, R. Lipton, "On the Importance of Checking Cryptographic Protocols for Faults," in *Proceedings of the 20th Annual International Cryptology Conference on Advances in Cryptology - EUROCRYPT'97*, Konstanz, Germany, pp. 37-51, 1997.

[30] I. Biehl, B. Meyer, V. Müller, "Differential Fault Attacks on Elliptic Curve Cryptosystems," in *Proceedings of the 20th Annual International Cryptology Conference on Advances in Cryptology*, Santa Barbara, California, USA, Vol. 1880, pp. 131-146, 2000.

[31] M. Ciet and M. Joye, "Elliptic Curve Cryptosystems in the Presence of Permanent and Transient Faults," *Designs, Codes and Cryptography*, Vol. 36, No. 1, pp. 33-43, 2005.

[32] J. Blömer, M. Otto, J. P. Seifert, "Sign Change Fault Attacks on Elliptic Curve Cryptosystems," *Fault Diagnosis and Tolerance in Cryptography*, Vol. 4231, pp. 36-52, 2006.

[33] M. Joye, A. K. Lenstra, J. J. Quisquater, "Chinese Remaindering Based Cryptosystems in the Presence of Faults," *Journal of Cryptology*, Vol. 12, pp. 241-245, 1999.

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

[35] S. Fenn, M. Gossel, M. Benaissa, D. Taylor, "On-Line Error Detection for Bit-Serial Multipliers in GF(2^m)," *Journal of Electronic Testing: Theory and Applications*, Vol. 13, No. 1, pp. 29-40, 1998.

[36] 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*, CA, USA, pp. 515-528, 2003.

[37] A. Reyhani-Masoleh and M. A. Hasan, "Fault Detection Architectures for Field Multiplication Using Polynomial Bases," *IEEE Transactions on Computers*, Vol. 55, No. 9, pp. 1089-1103, 2006.

[38] 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: Theory and Applications*, Vol. 21, No. 5, pp. 539-549, 2005.

[39] S. Bayat-Sarmadi and M. A. Hasan, "On Concurrent Detection of Errors in Polynomial Basis Multiplication," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, Vol. 15, No. 4, pp. 413-426, 2007.

[40] W. Chelton and M. Benaissa, "Concurrent Error Detection in GF(2^m) Multiplication and Its Application in Elliptic Curve Cryptography," *IET Circuits, Devices & Systems*, Vol. 2, No. 3, pp. 289-297, 2008.

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

[42] C.Y. Lee, C.W. Chiou, J.M. Lin, "Concurrent Error Detection in a Polynomial Basis Multiplier over GF(2^m)," *Journal of Electronic Testing: Theory and Applications*, Vol. 22, No. 2, pp. 143-150, 2006.

[43] 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 Science*, Vol. E89-A, No. 2, pp. 566-574, 2006.

[44] C.W. Chiou, C.C. Chang, C.Y. Lee, T.W. Hou, J.M. Lin, "Concurrent Error Detection and Correction in Gaussian Normal Basis Multiplier over GF(2^m)," *EEE Transactions on Computers*, Vol. 56, No. 6, pp. 581-587, 2009.

[45] C.W. Chiou, C.Y. Lee, J.M. Lin, T.W. Hou, C.C. Chang, "Concurrent Error Detection and Correction in Dual Basis Multiplier over GF(2^m)," *IET Circuits, Devices & Systems*, Vol. 3, No. 1, pp. 22-40, 2009.

[46] 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.

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

[48] A. Bark and C. Kinne, "The Application of Pulse Position Modulation to Digital Computers," in *Proceedings of National Electronics Conference*, pp. 656-664, 1953.

[49] H. Yamamoto, T. Watanabe, Y. Urano, "Alternating Logic and Its Application to Fault Detection," in *Proceedings of IEEE International Computing Group Conference*, Washington, D.C., pp. 220-228, 1970.

[50] D. A. Reynolds and G. Metze, "Fault Detection Capabilities of Alternating Logic," *IEEE Transactions on Computers*, Vol. C-27, No. 12, pp. 1093-1098, 1978.

[51] S. E. Woodard, "Design of Digital Systems Using Self-Checking Alternating Logic," Ph.D. Thesis, University of Illinois at Urbana-Champaign, U.S.A., 1977.

[52] C.W. Chiou, "Self-Checking Array Multiplier in GF(2^m) Fields Using Alternating Logic," in *Proceedings of 2003 Conference on Electronic Communication and Applications*, Penghu, Taiwan, R.O.C, pp. 270-274, 2003.

[53] C.W. Chiou, W.Y. Liang, H.W. Chang, J.M. Lin, C.Y. Lee, "Concurrent Error Detection in Semi-Systolic Dual Basis Multiplier over GF(2^m) Using Self-Checking Alternating Logic," *IET Circuits, Devices & Systems*, Vol. 4, No. 5, pp. 382-391, 2010.