Error-Correcting Codes for Concurrent Error Correction in Bit-parallel Systolic and Scalable Multipliers for Shifted Dual Basis of GF(2^m)

Chiou-Yng Lee[1, *], Pramod Kumar Meher[2], and Yung-Hui Chen[1]

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

[2] Department of Embedded Systems,
Institute for Infocomm Research,
Singapore, 138632
pkmeher@i2r.a-star.edu.sg

Received 15 May 2011; Revised 20 July 2011; Accepted 30 August 2011

Abstract. This work presents a novel bit-parallel systolic multiplier for the shifted dual basis of GF(2^m). The shifted dual basis multiplication for all trinomials can be represented as the sum of two Hankel matrix-vector multiplications. The proposed multiplier architecture comprises one Hankel multiplier and one (2*m*-1)-bit adder. The algebraic encoding scheme based on linear cyclic codes is adopted to implement the multiplications with concurrent error correction (CEC). The latency overhead is analytically demonstrated to require extra four clock cycles than as compared by the multiplier without CEC. The block Hankel matrix-vector representation is used to derive a CEC scalable SDB multiplier. In the binary field GF(2^{84}), the space overhead of the proposed bit-parallel architecture using cyclic code is around 22.8%. The proposed CEC scalable multiplier given by seven or fewer injection errors can correct nearly 99.6% of error correction. Unlike the existing concurrent error detection multipliers that apply the parity prediction scheme, the proposed architectures have multiple error-detection capabilities.

Keywords: Fault-based attack, finite field multiplication, linear cyclic code, concurrent error correction

References

[1] IEEE Standard 1363-2000, IEEE standard specifications for public-key cryptography.

[2] C.Y. Lee, "Concurrent Error Detection in Digit-Serial Normal Basis Multiplication over GF(2^m)," in *Proceedings of International Conference Advanced Information Networking and Applications Workshops (AINA2008)* , Okinawa, Japan, pp. 1499-1504, 2008.

[3] 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.

[4] J. Mathew, A. Costas, A. M. Jabir, M. Rahaman, H. D. K. Pradhan, "Single error correcting finite field multipliers over GF(2^m)," in *Proceedings of 21st International Conference VLSI Design*, Hyderabad, India, pp. 33-38, 2008.

[5] R. Karri, G. Kuznetsov, M. Goessel, "Parity-based concurrent error detection of substitution-permutation network block ciphers," in *Proceeding of CHES 2003, Springer LNCS 2779*, Cologne, Germany, pp. 113-124, 2003.

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

[7] D. Boneh, R. A. DeMillo, R. J. Lipton, "On the Importance of Eliminating Errors in Cryptographic Computations," *Journal of Cryptography*, Vol. 14, pp. 101-119, 2001.

[*] Correspondence author

[8] C.Y. Lee, "Low-complexity Parallel Systolic Montgomery Multipliers Over GF(2^m) using Toeplitz Matrix-vector Representation," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, Vol. E91-A, No. 6, pp. 1470-1477, 2008.

[9] C.Y. Lee and C.W. Chiou, "New Bit-parallel Systolic Architectures for Computing Multiplication, Multiplicative Inversion and Division in GF(2^m) under the Polynomial Basis and Normal Basis Representations," *Journal of VLSI Signal Processing Systems*, Vol. 52, No. 3, pp. 313-324, 2008.

[10] C.Y. Lee, "Low-complexity Bit-parallel Systolic Multipliers Over GF(2^m)," *Integration – The VLSI Journal*, Vol. 41, No. 1, pp. 106-112, 2008**.**

[11] C.Y. Lee, C.W. Chiou, J.M. Lin, C.C. Chang, "Scalable and Systolic Montgomery Multiplier over GF(2^m) Generated by Trinomials," *IET Circuits, Devices & System*, Vol. 1, No. 6, pp. 377-484, 2007**.**

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

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

[14] C.Y. Lee, "Concurrent Error Detection Architectures for Gaussian Normal Basis Multiplication over GF(2^m)," *Integration – The VLSI Journal*, Vol. 43, No. 1, pp. 113-123, 2010.

[15] 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.

[16] S. Bayat-Sarmadi and M. A. Hasan, "On Concurrent Detection of Errors in Polynomial Basis Multiplication," *IEEE Transactions on VLSI Systems*, Vol. 15, No. 1, pp. 413-426, 2007.

[17] C.Y. Lee, P. K. Meher, J.C. Patra, "Concurrent Error Detection in Bit-serial Normal Basis Multipliers Over GF(2^m)," *IEEE Transactions on VLSI Systems*, Vol. 18, No. 8, pp. 1234-1238, 2010.

[18] W. Hamming, "Error Detecting and Error Correcting Codes," *Bell Systems Technical Journal*, pp. 147-160, 1950.

[19] K. K. Parhi, "Eliminating the Fanout Bottleneck in Parallel Long BCH Encoders," *IEEE Transactions on Circuits and Systems-I*, Vol. 51, No. 3, pp. 512-516, 2004.

[20] T. Kasiimi, T. Takata, T. Fujiwara, S**.** Lin, "Trellis Diagram Construction for Some BCH Codes," in *Proceedings of IEEE International Conference on Information Theory and Applications***,** Honolulu, HI, 1990.

[21] C.Y. Lee, P.K. Meher, W.Y. Lee, "Fault-Tolerant Bit-Parallel Multiplier for Polynomial Basis of GF(2^m)," in *Proceedings of IEEE Circuits and Systems International Conference on Testing and Diagnosis (ICTD'09),* Chengdu , China, pp. 1-4, 2009.

[22] H. Fan and Y. Dai, "Fast Bit-parallel GF(2^n) Multiplier for All Trinomials," *IEEE Transactions on Computers,* Vol. 54, No. 4, pp. 485-490, 2005.

[23] S. Bayat-Saramdi and M. A. Hasan, "Run-time Error Detection in Polynomial Basis Multiplication using Linear Codes," in *Proceedings of IEEE International Conference on Application-specific Systems, Architectures and Processors*, Québec, Canada, pp. 204-209, 2007.