Efficient Designs for AOP-Based Field Multiplication over GF(2^m)

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

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

[2] Department of Computer Information and Network Engineering,
Lunghwa University of Science and Technology,
Taoyuan 333, Taiwan
chiouyng@yahoo.com.tw

Received 15 July 2011; Revised 20 August 2011; Accepted 24 September 2011

Abstract. In this paper, we present an efficient recursive formulation and systolic implementation of polynomial basis finite field multiplication over GF(2^m) based on irreducible all-one-polynomials (AOP). Using the property of irreducible AOP we have obtained a scheme of computation-free modular-reduction up to degree *m*, where reduction of degree is achieved by cyclic-left-shift operations. In the proposed systolic architecture, the cyclic-left-shift has been achieved by appropriate reordering of input lines in the processing elements (PEs). Compared with the previously existing systolic structures, the proposed one is found to involve significantly less number of registers and requires nearly half the area-time complexity. It is shown that the proposed structure requires nearly the same number of gates as those of the existing bit-parallel structures. Unlike the existing bit-parallel designs, it does not require rewiring of input lines, and critical path of proposed structure does not increase with the field order m. For $m > 17$ (which is required in most practical cases), the proposed systolic design is found to have significantly less area-time complexity compared with the existing bit-parallel structures.

Keywords: Finite field, galois field, finite field multiplication, elliptic curve cryptography, error-control-coding, systolic array, VLSI

References

[1] R. Lidl and H. Niederreiter, Eds., Introduction to Finite Fields and their Applications, NY: Cambridge University Press, New York, 1986.

[2] [Online]. Available: http://www.csrc.nist.gov/publications

[3] L. Song and K. K. Parhi, "Efficient Finite Field Serial/Parallel Multiplication," in *Proceedings of 1996 International Conference on Application-Specific Systems, Architectures, and Processors*, Chicago, IL, USA, pp. 72-82, 1996.

[4] S. K. Jain, L. Song, K. K. Parhi, "Efficient Semisystolic Architectures for Finite-field Arithmetic," *IEEE Transactions on Very Large Scale Integration Systems*, Vol. 6, No. 1, pp. 101-113, 1998.

[5] P. K. Meher, "Systolic Formulation for Low-complexity Serial-parallel Implementation of Unified Finite Field Multiplication over GF(2^m)," in *Proceedings of IEEE International Conference on Application-Specific Systems, Architectures and Processors*, Montréal, Québec, Canada, 2007.

[6] F. Rodriguez-Henriguez and C. K. Koc, "Parallel Multipliers based on Special Irreducible Pentanomials," *IEEE Transactions on Computers*, Vol. 52, No. 12, pp. 1535-1542, 2003.

[7] J. L. Ima~na, J. M. Sanchez, F. Tirado, "Bit-parallel Finite Field Multipliers for Irreducible Trinomials," *IEEE Transactions on Computers*, Vol. 55, No. 5, pp. 520-533, 2006.

*Correspondence author

[8] A. Reyhani-Masoleh and M. A. Hasan, “Low Complexity Bit Parallel Architectures for Polynomial Basis Multiplication over GF(2^m),” *IEEE Transactions on Computers*, Vol. 53, No. 8, pp. 945-959, 2004.

[9] W. Tang, H. Wu, M. Ahmadi, “VLSI Implementation of Bit-parallel Word-serial Multiplier in GF(2^{233}),” in *Proceedings of IEEE International Conference on New Circuits and Systems*, Québec, Canada, pp. 399-402, 2005.

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

[11] C. K. Koc 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.

[12] C. H. Kim, S. Oh, J. Lim, “A New Hardware Architecture for Operations in GF(2^n),” *IEEE Transactions on Computers*, Vol. 51, No. 1, pp. 90-92, 2002.

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

[14] C.Y. Lee, E.H. Lu, J.Y. Lee, “New Bit-parallel Systolic Multipliers for a Class of GF(2^m),” in *Proceedings of IEEE International Symposium on Circuits and Systems*, Sydney, Australia, pp. 578-581, 2001.

[15] C.Y. Lee, E.H. Lu, J. Yien, “High-speed Bit-parallel Systolic Multipliers for a Class of GF(2^m),” in *Proceedings of International Symposium on VLSI Technology, Systems, and Applications*, Hsinchu, Taiwan, pp. 291-294, 2001.

[16] K.Y. Chang, D. Hong, H.S. Cho, “Low Complexity Bit-parallel Multiplier for GF(2^m) Defined by All-one Polynomials Using Redundant Representation,” *IEEE Transactions on Computers*, Vol. 54, No. 12, pp. 1628-1630, 2005.

[17] I. S. Hsu, T. K. Truong, L. J. Deutsch, I. S. Reed, “A Comparison of VLSI Architecture of Finite Field Multipliers Using Dual, Normal, or Standard Bases,” *IEEE Transactions on Computers*, Vol. 37, No. 6, pp. 735-739, 1988.

[18] S. Y. Kung, VLSI Array Processors. Prentice Hall, Inc. Upper Saddle River, NJ, USA, 1987.