Low-Complexity Parallel Systolic Architectures for Computing Multiplication and Squaring over GF(2^m)

Chiou-Yng Lee*

Department of Computer Information and Network Engineering

Lunghwa University of Science and Technology

Taoyuan, Taiwan

PP010@mail.lhu.edu.tw

Received 19 November 2008; Revised 10 December 2008 ; Accepted 20 December 2008

Abstract. Recently, cryptographic applications based on finite fields have attracted much interest. This paper presents a unified systolic multiplier under the method of the multiply-by-x^2 and the folded technique. This circuit is particularly suitable for implementing multiplication and squaring in GF(2^m). The results show that our proposed multiplier saves up to 75% space complexity and 50% latency as compared to the traditional multipliers proposed by Yeh et al. and Wang-Lin. Also, the proposed squarer saves about 45% space complexity as compared to the traditional squarer presented by Guo and Wang.

Keywords: finite field, polynomial basis, systolic architecture, MSB-first multiplication algorithm

References

[1] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, Amsterdam: North-Holland, 1977.

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

[3] R.E. Blahut, *Fast algorithms for digital signal processing*, Reading, Mass.: 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. IT-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. 25, No. 1, pp.78-86, 1976.

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

[7] C.S. Yeh, S. Reed, and T.K. Truong, "Systolic Multipliers for Finite Fields GF(2^m)," *IEEE Transactions on Computers*, Vol. 33, pp. 357-360, 1984.

[8] C.L. Wang and J.L. Lin, "Systolic Array Implementation of Multipliers for GF(2^m)," *IEEE Transactions on Circuits and Systems II*, Vol. 38, pp. 796-800, 1991.

[9] B.B. Zhou, "A New Bit-Serial Systolic Multiplier over GF(2^m)," *IEEE Transactions on Computers*, Vol. 37, No. 6, pp. 749-751, 1988.

[10] J.H. Guo and C.L. Wang, "A New Systolic Squarer and Its Application to Compute Exponentiations in GF(2^m)" *Proceedings of 1997 IEEE International Symposium on Circuits and Systems*, Vol. 3, pp.2044-2047, 1997.

[11] C.L Wang and J.H. Guo, "New Systolic Arrays for AB^2+C, Inversion, and Division in GF(2^m)," *IEEE Transactions on Computers*, Vol. 49, No. 10, pp.1120-1125, 2000.

* Correspondence author

[12] C.Y. Lee, E.H. Lu, and 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.Y. Lee, E.H. Lu, and L.F. Sun, "Low-Complexity Bit-Parallel Systolic Architecture for Computing AB^2+C in a Class of Finite Field GF(2^m)," *IEEE Transactions on Circuits and Systems II*, Vol. 50, No. 5, pp. 519-523, May 2001.

[14] C.Y. Lee, "Low-Complexity Bit-Parallel Systolic Multiplier over GF(2^m) Using Irreducible Trinomials," *IEE Computers and Digital Techniques*, Vol. 144, No. 1, pp. 39-42, 2003.

[15] C.Y. Lee, J.S. Horng and I.C. Jou, "Low-Complexity Bit-Parallel Systolic Montgomery Multipliers for Special Classes of GF(2^m)," *IEEE Transactions on Computers*, Vol. 54, No. 9, pp. 1061-1070, 2005.

[16] C.Y. Lee, "Low-Latency Bit-Parallel Systolic Multiplier for Irreducible x^m+x^n+1 with gcd(m,n)=1," *IEICE Transactions on Fundamentals*, Vol.E86-A, No.11, pp. 2844-2852, 2003.

[17] S. Kwon, C.H. Kim and C.P. Hong, "A Systolic Multiplier with LSB First Algorithm over GF(2^m) Which Is As Efficient As the One with MSB First Algorithm," *Proceedings of the 2003 International Symposium on Circuits and Systems*, Vol. 5, pp.V-633-636, 2003.

[18] C.L. Wang, "Bit-Level Systolic Array for Fast Exponentiation in GF(2^m)," *IEEE Transactions on Computers*, Vol. 43, No. 7, pp.838-841, 1994.

[19] C.L. Wang and J.L. Lin, "A Systolic Architecture for Computing Inverses and Divisions in Finite Fields GF(2^m), " *IEEE Transactions on Computers*, Vol. 42, No. 9, pp. 1141-1146, 1993.

[20] G. Seroussi, "Table of Low-Weight Binary Irreducible Polynomials," *Visual Computing Dept., Hewlett Packard Laboratories*, Aug. 1998. Available at: http://www. hpl.hp.com /techreports/98/ HPL-98-135.html.

[21] W. Stahnke, "Primitive Binary Polynomials," *Mathematics of Computation*, Vol.27, pp. 977-980, 1973.

[22] S.Y. Kung, *VLSI Array Processors*, Englewood Cliffs, NJ: Prentice-Hall, 1988.

[23] N. Weste and K. Eshraghian, *Principles of CMOS VLSI Design: a System Perspective*, Addison-Wesley, Reading, MA, 1985.