A Novel Digit-Serial Dual Basis Systolic Karatsuba Multiplier over GF(2^m)

Ying Yan Hua[1] Jim-Min Lin[2,*] Che Wun Chiou[3] Chiou-Yng Lee[4] Yong Huan Liu[1]

[1]College of Electronics and Information Engineering, Tongji University
NO.4800, Cao'an Hwy, Shanghai201804, China
{hippocrene814@hotmail.com , liuyonghuan@tongji.edu.cn}

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

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

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

Received 18 January 2012; Revised 15 June 2012 ; Accepted 21 June 2012

Abstract. Multiplication is one of the most important finite field arithmetic operations in cryptographic computations. Dual basis multipliers over GF(2^m) are widely applied in this kind of computations due to its advantage of small chip area. However, up to date, there are only few methods that can keep balance of low space complexity and low time complexity at the same time. To achieve such an efficient aim, this study presents a novel digit-serial dual basis multiplier that is different from existing ones with a modified cut-set method using Karatsuba algorithm. Though this kind of multiplier will lose some throughput, it needs only a small number of transistors so that it is particularly suitable for some hand held devices that equipped only limited resources. The proposed digit-serial dual basis multiplier saves 54% space complexity and 30% time complexity as compared to existing similar studies with NIST suggested values for elliptic curve cryptosystem.

Keywords: public-key cryptosystem, elliptic curve cryptosystem, finite field multiplication, digit-serial multiplier, Karatsuba algorithm.

Acknowledgment

The authors would like to thank anonymous referees and the editor for carefully reading the paper and for their great help in improving the paper.

References

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

[2] R.E. Blahut, *Fast Algorithms for Digital Signal Processing*, Addison-Wesley, Reading, Mass., 1985.

[3] E.R. Berlekamp, “Bit-serial Reed-solomon Encoder,” *IEEE Transactions on Information Theory*, Vol. IT-28, pp. 869-874, 1982.

[4] 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. IT-35, No.6, pp. 1177-1183, 1989.

[*] Correspondence author.

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

[6] V.S. Miller, "Use of Elliptic Curves in Cryptography," in *Proceedings of Crypto 85, LNCS 218*, pp. 417-426, 1986.

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

[8] N. Koblitz, "A Family of Jacobians Suitable for Discrete Log Cryptosystems," In *Advances in Cryptology, Proc. Crypto'88*, pp. 94-99, 1988.

[9] R. Dutta, R. Barua, P. Sarkar, "Pairing-based Cryptographic Protocols: A Survey," *Cryptology ePrint Archive*, Report 064/2004, 2004.

[10] T.C. Bartee and D.J. Schneider, "Computation with Finite Fields," *Information and Computing*, Vol. 6, pp. 79-98, Mar. 1963.

[11] E.D. Mastrovito, "VLSI Architectures for Multiplication over Finite Field GF(2^m)," in *Proceedings of Sixth International Conference on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes (AAECC-6)*, pp. 297-309, Jul. 1988.

[12] 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, Mar. 1998.

[13] T. Itoh and S. Tsujii, "Structure of Parallel Multipliers for A Class of Fields GF(2^m)," *Information and Computation*, Vol. 83, pp. 21-40, 1989.

[14] 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, May 2001.

[15] 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, Feb. 1998.

[16] H. Wu, "Bit-parallel Finite Field Multiplier and Squarer Using Polynomial Basis," *IEEE Transactions on Computers*, Vol. 51, No. 7, pp. 750-758, Jul. 2002.

[17] H. Fan and M.A. Hasan, "A New Approach to Subquadratic Space Complexity Parallel Multipliers for Extended Binary Fields," *IEEE Transactions on Computers*, Vol. 56, No. 2, pp. 224-233, Feb. 2007.

[18] J.H. Guo and C.L. Wang, "Digit-serial Systolic Multiplier for Finite Fields GF(2^m)," *IET Computers & Digital Techniques*, Vol. 145, No. 2, pp. 143-148, May 1998.

[19] C.H. Kim, C.P. Hong, S. Kwon, "A Digit-serial Multiplier for Finite Field GF(2^m)," *IEEE Transactions on Very Large Scale Integration Systems*, Vol. 13, No. 4, pp. 476-483, Apr. 2005.

[20] S. Kumar, T. Wollinger, C. Paar, "Optimum Digit-serial GF(2^m) Multipliers for Curve-based Cryptography," *IEEE Transactions on Computers*, Vol. 55, No. 10, pp. 1306-1311, Oct. 2006.

[21] S. Talapatra, H. Rahaman, J. Mathew, "Low Complexity Digit Serial Systolic Montgomery Multipliers for Special Class of GF(2^m)," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, Vol. 18, No. 5, pp. 847-852, May 2010.

[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, Nov. 1998.

[23] 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, Mar. 1996.

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

[25] 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, Nov. 2005.

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

[27] 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. C-34, No. 8, pp. 709-717, Aug. 1985.

[28] A. Reyhani-Masoleh, "Efficient Algorithms and Architectures for Field Multiplication Using Gaussian Normal Bases," *IEEE Transactions on Computers*, Vol. 55, No. 1, pp. 34-47, Jan. 2006.

[29] 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.

[30] G.B. Agnew, R.C. Mullin, I.M. Onyszchuk, S.A. Vanstone, "An Implementation for A Fast Public-key Cryptosystem," *Journal of Cryptology*, Vol. 3, pp. 63-79, 1991.

[31] M.A. Hasan, M.Z. Wang, V.K. Bhargava, "A Modified Massey-Omura Parallel Multiplier for A Class of Finite Fields," *IEEE Transactions on Computers*, Vol. 42, No. 10, pp. 1278-1280, Oct. 1993.

[32] S. Kwon, "A Low Complexity and A Low Latency Bit Parallel Systolic Multiplier over GF(2^m) Using An Optimal Normal Basis of Type II," in *Proceedings of the 16th IEEE Symposium on Computer Arithmetic*, pp. 196-202, 2003.

[33] H. Fan and M.A. Hasan, "Subquadratic Computational Complexity Schemes for Extended Binary Field Multiplication Using Optimal Normal Bases," *IEEE Transactions on Computers*, Vol. 56, No. 10, pp. 1435-1437, Oct. 2007.

[34] A. Karatsuba and Y. Ofman, "Multiplication of Many-digital Numbers by Automatic Computers," in *Proceedings of the USSR Academy of Sciences*, pp. 293-294, 1962.

[35] B. Sunar, "A Generalized Method for Constructing Subquadratic Complexity GF(2^k) Multipliers," *IEEE Transactions on Computers*, Vol. 53, No. 9, pp. 1097-1105, Sep. 2004.

[36] F. Rodriguez-Henriquez and C.K. Koc, "On Fully Parallel Karatsuba Multipliers for GF(2^m)," in *Proceedings of the International Conference on Computer Science and Technology*, pp. 405-410, May 19-21, 2003.

[37] H. Fan and M.A. Hasan, "Alternative to the Karatsuba Algorithm for Software Implementations of GF(2^n) Multiplications," *IET Information Security*, Vol. 3, No. 2, pp. 60-65, 2009.

[38] Y. Li, G.L. Chen, J.H. Li, "Speeding of Bit-parallel Karatsuba Multiplier in GF(2^m) Generated by Trinomials," *Information Processing Letters*, Vol. 111, No. 8, pp. 390-394, Mar. 2011.

[39] A. Weimerskirch and C. Paar, "Generalizations of the Karatsuba Algorithm for Efficient Implementations," Cryptology ePrint Archive: Report 2006/224, http://eprint.iacr.org/2006/224.

[40] L.H. Chen, P.L. Chang, C.Y. Lee, Y.K. Yang, "Scalable and Systolic Dual Basis Multiplier over GF(2^m)," *International Journal of Innovative Computing*, Vol. 7, No. 3, pp. 1193-1208, Mar. 2011.

[41] P.L. Chang, L.H. Chen, C.Y. Lee, "Low-complexity Dual Basis Digit Serial GF(2^m) Multiplier," *ICIC Express Letters*, Vol.3, No.4, pp. 1113-1118, Dec. 2009.

[42] N. Weste and K. Eshraghian, *Principles of CMOS VLSI Design: A System Perspective*, Reading, Mass.: Addison-Wesley, 1985.

[43] "M74HC86, Quad Exclusive OR Gate," STMicroelectronics, 2001, *http://www.st.com/stonline/books/pdf/docs/2006.pdf*

[44] "M74HC08, Quad 2-Input AND Gate," STMicroelectronics, 2001, *http://www.st.com/stonline/books/pdf/docs/1885.pdf*

[45] "M74HC279, Quad $\overline{S}-\overline{R}$ Latch," STMicroelectronics, 2001, *http://www.st.com/stonline/books/pdf/docs/1937.pdf*

[46] M74AC1157, "2 to 1 multiplexer, 2001 STMicroelectronics," *http://www.st.com/stonline/books/pdf/docs/5144.pdf*