High-Throughput Finite Field Multipliers Using Redundant Basis for FPGA and ASIC Implementations

Shaik.Sooraj, Jabeena shaik,,M.Tech
Department of Electronics and communication Engineering
Quba College of Engineering & Technology,Venkatachalam
(JNTU Anantapur)

Abstract: Redundant basis (RB) multipliers over Galois Field($GF2^m$) have gained huge popularity in elliptic curve cryptography (ECC) mainly because of their negligible hardware cost for squaring and modular reduction. In this paper, we have proposed a novel recursive decomposition algorithm for RB multiplication to obtain high-throughput digit-serial implementation. Through efficient projection of signal-flow graph (SFG) of the proposed algorithm, a highly regular processor-space flow-graph (PSFG) is derived. By identifying suitable cut -sets, we have modified the PSFG suitably and performed efficient feed-forward cut-set retiming to derive three novel multipliers which not only involve significantly less time-complexity than the existing ones but also require less area and less power consumption compared with the others. Both theoretical analysis and synthesis results confirm the efficiency of proposed multipliers over the existing ones. The synthesis results for field programmable gate array (FPGA) and application specific integrated circuit (ASIC) realization of the proposed designs and competing existing designs are compared. It is shown that the proposed high-throughput structures are the best among the corresponding designs, for FPGA and ASIC implementation. It is shown that the proposed designs can achieve up to 94% and 60% savings of area-delay-power product (ADPP) on FPGA and ASIC implementation over the best of the existing designs, respectively

Keywords: ASIC, digit-serial, finite field multiplication, FPGA, high-throughput, redundant basis.

1. INTRODUCTION

.

F INITE FIELD multiplication over Galois Field ($GF(2^m)$) is a basic operation frequently encountered in modern cryptographic systems such as the elliptic curve cryptography (ECC) and error control Moreover, multiplication over a finite field can be used further - over $GF(2^m)$ can be implemented on a general purpose machine, but it is expensive to use a general purpose ma-chine to implement cryptographic systems in cost-sensitive consumer products. Besides, a low-end microprocessor cannot meet the real-time requirement of different applications since word length of these processors is too small compared with the order of typical finite fields used in cryptographic systems. Most of the real-time applications, therefore, need hardware implementation of finite field arithmetic operations for the benefits like low-cost and high-throughput rate.

The choice of basis to represent field elements, namely the polynomial basis, normal basis, triangular basis and redundant basis (RB) has a major impact on the performance of the arithmetic circuits .The multipliers based on have gained significant attention in recent years due to their several advantages. Not only do they offer free squaring, as normal basis does, but also involve lower computational complexity and can be implemented in highly regular computing structures

Several digit-level serial/parallel structures for RB multiplier over $GF(2^m)$ have been reported in the last years after its introduction by this. An efficient serial/parallel multiplier using redundant representation has been presented. A bit-serial word-parallel (BSWP) architecture for RB multiplier has been reported by Naming. Several other RB multipliers also have been developed by the same authors in for reducing the complexity of implementation and for high-speed realization. We find that the hardware utilization efficiency and throughput of existing structures of can be improved by efficient design of algorithm and architecture.

In this paper, we aim at presenting efficient digit-level serial/parallel designs for high-throughput finite field multiplicand-

over $GF(2_m)$ based on RB. We have proposed an efficient recursive decomposition scheme for digit-level RB multiplication, and based on that we have derived parallel algorithms for high throughput digit-serial multiplication. We have mapped the algorithm to three different high-speed architectures by mapping the parallel algorithm to a regular 2-dimensional signal-flow graph (SFG) array, followed by suitable projection of SFG to 1-dimensional processor-space flow graph (PSFG), and the choice of feed -forward cut-set to enhance the throughput rate. Our proposed digit-serial multipliers involve significantly less area-time-power complexities than the corresponding existing designs. Field programmable gate array (FPGA) has evolved as a mainstream dedicated computing platform. FPGAs however do not have abundant number of registers to be used in the multiplier. Therefore, we have modified the proposed algorithm and architecture for reduction of register-complexity particularly for the implementation of RB multipliers on FPGA platform.

III. 2. DERIVATION OF PROPOSED HIGH-THROUGHPUT STRUCTURES FOR RB MULTIPLIERS

In this section, we derive the proposed multipliers from the SFG of the proposed Algorithm 1. For efficient realization of a digit-serial RB multiplier, we can perform feed-forward cut-set retiming in a regular interval in the PSFG as shown in Fig. 3. As a result of cut-set retiming of the Fig. 3, the minimum duration of each clock period is reduced to (T_A+T_X), where T_A and T_X denote the delay of an AND gate and an XOR gate, respectively.

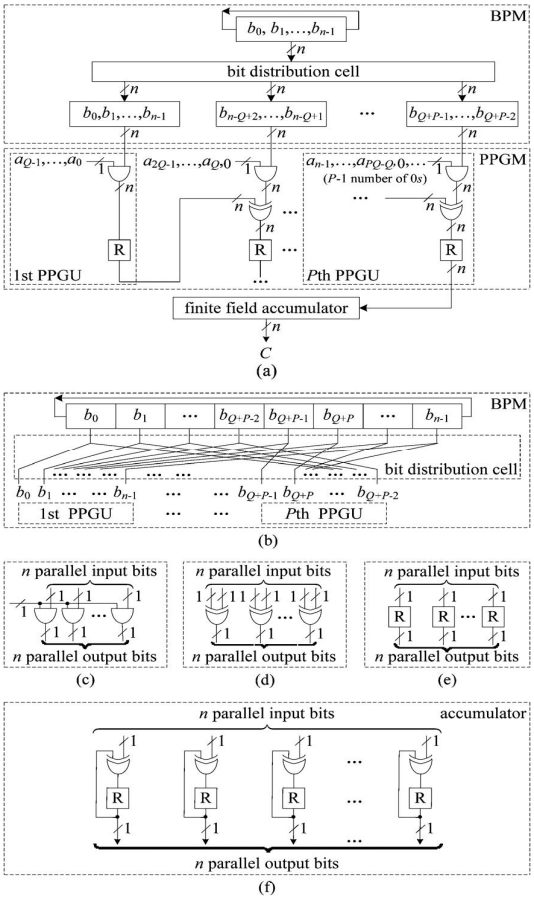


Fig. 4. Proposed structure-I (PS-I) for RB multiplier, where "R" denotes a register cell. (a) Detailed structure of the RB multiplier. (b) Structure of the bit-per-mutation module (BPM). (c) Structure of the AND cell in the partial product generation module (PPGM). (d) Structure of the XOR cell in the PPGM. (e) Structure of the register cell in the PPGM. (f) Structure of the finite field accumulator.

The finite field accumulator module. The BPM of Fig. 4 per-forms rewiring of bits of operand B to feed its output to P partial product generation units (PPGU)s according to the S nodes of PSFG of Fig. 3, as shown in Fig. 4(b). The AND cell, XOR cell and register cell of PPGM perform the function of M node, A node and delay imposed by the retiming of PSFG of system.

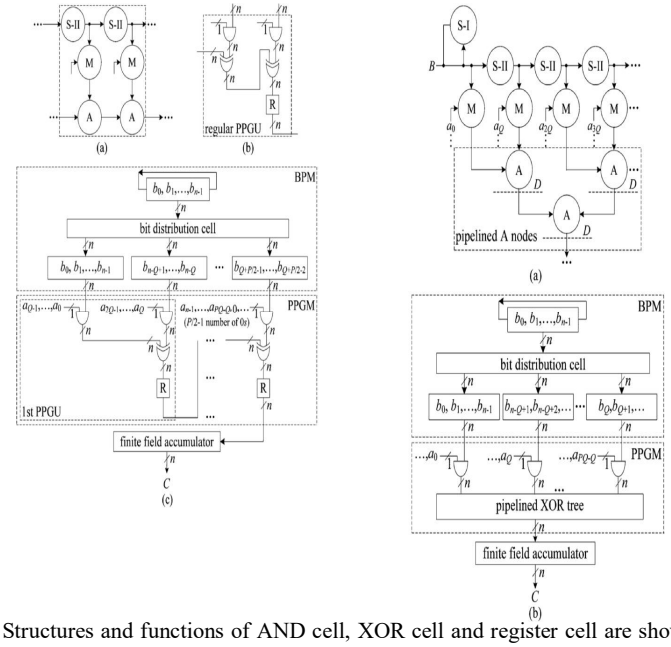


Fig. 3, respectively. Structures and functions of AND cell, XOR cell and register cell are shown in Fig. 4(c), (d), and (e), respectively. The input operands are fed to PPGU in staggered manner to meet the

B. Modification of Proposed Structure-I

For any integer value of P, we can have $(P=kd+l)$, where $0\leq l<d$ and $d<P$. Without loss of generality, for simplicity of discussion, we can assume $l=0$. The approach proposed here for $l=0$ however can be easily extended to the cases where $l\neq 0$. Define $0\leq h\leq k-1$, and $0\leq f\leq d-1$, such that (13) can be rewritten as

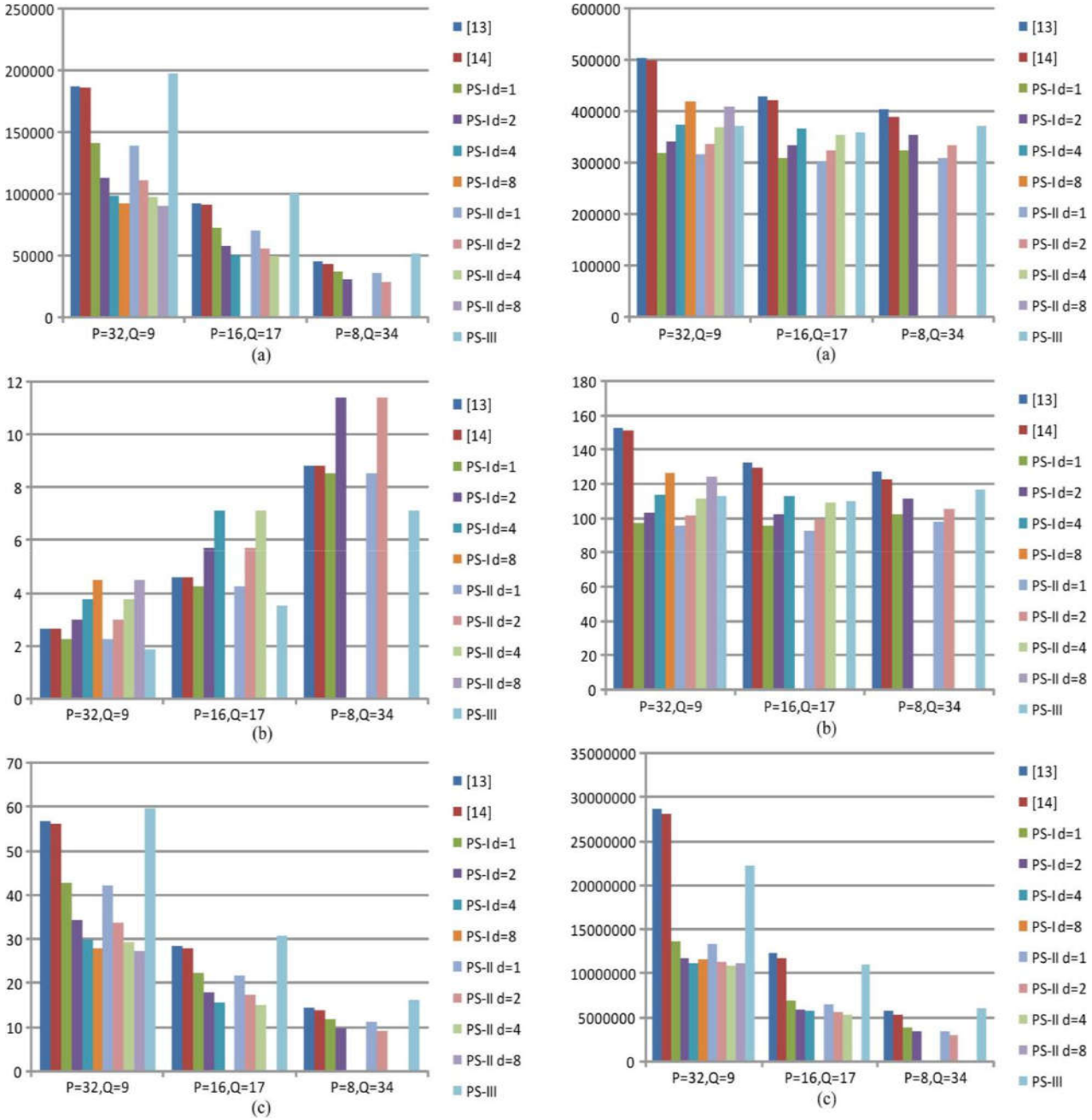
$$C_u = \sum_{h=0}^{k-1}\sum_{f=0}^{d-1} B^{u+fk} a_{u+fk} \qquad (14)$$

Based on (14), we can modify the retiming of PSFG of Fig. 3 to derive suitable digit- level architecture for RB multiplier over $GF(2^m)$. For example, to obtain the proposed structure for $d=2$, a pair of S nodes, a pair of M nodes and a pair of A nodes of the PSFG of Fig. 3 can be merged to form a macro- node as shown within the dashed-lines in Fig. 5. Each of these macro-nodes can be implemented by a new PPGU to obtain a PPGM of $P/2$ PPGUs. Accordingly, two regular PPGUs in the structure of Fig. 4 can be emerged into a new regular PPGU as shown in Fig. 5(b), which consists of two AND cells and two XOR cells (the first PPGU requires only one XOR cell). The functions of AND cell, XOR cell and register cell are the same as those described

F. Design Selection

From Figs. 8, 9, 10, and 11, we find that PS- I and PS-II out-perform the other structures in both FPGA and ASIC platforms in terms of area, time and power complexities. Besides, because of their low area-time-power complexities and high throughput rate, PS-I and PS-II can be used in various real time applications. Especially for FPGA implementation, it is suggested to use either

PS-I/II (for $1 < d < P$) based on the area constraint and speed requirement of applications. For ASIC implementation, PS-I and PS-II of Figs. 4 and 6 or PS-III of Fig. 7 are preferred for their efficiency in area-time-power complexities.



V. CONCLUSION

We have proposed a novel recursive decomposition algorithm for RB multiplication to derive high-throughput digit-serial mul-tipliers. By suitable projection of SFG of proposed algorithm and identifying suitable cut-sets for feed-forward cut-set retiming, three novel high-throughput digit -serial RB multipliers are de-rived to achieve significantly less area-time -power complexities than the existing ones. Moreover, efficient structures with low register-count have been derived for area-constrained implemen-tation; and particularly for implementation in FPGA platform where registers are not abundant. The results of synthesis show that proposed structures can achieve saving of up to 94%

REFERENCES

[1] I. Blake, G. Seroussi, and N. P. Smart, *Elliptic Curves in Cryptography*, ser. London Mathematical Society Lecture Note Series.. Cambridge, U.K.: Cambridge Univ. Press, 1999.

[2] N. R. Murthy and M. N. S. Swamy, "Cryptographic applications of brahmaqupta-bha skara equation," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 53, no. 7, pp. 1565–1571, 2006.

[3] L. Song and K. K. Parhi, "Low-energy digit-serial/parallel finite field multipliers," *J. VLSI Digit. Process.*, vol. 19, pp. 149–C166, 1998.

[4] P. K. Meher, "On efficient implementation of accumulation in finite field over $GF2_m$ and its applications," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 17, no. 4, pp. 541–550, 2009.

[5] L. Song, K. K. Parhi, I. Kuroda, and T. Nishitani, "Hardware/(softw)are codesign of finite field datapath for low-energy Reed-Solomn codecs," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 8, no. 2, pp. 160–172, Apr. 2000.

[6] G. Drolet, "A new representation of elements of finite fields $GF2_m$ yielding small complexity arithmetic circuits," *IEEE Trans. Comput.*, vol. 47, no. 9, pp. 938–946, 1998.

[7] C.-Y. Lee, J.-S. Horng, I.-C. Jou, and E.-H. Lu, "Low-complexity bit-parallel systolic montgomery multipliers for special classes of $GF2_m$," *IEEE Trans. Comput.*, vol. 54, no. 9, pp. 1061–1070, Sep. 2005.

[8] P. K. Meher, "Systolic and super-systolic multipliers for finite field ( ) based on irreducible trinomials," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 55, no. 4, pp. 1031–1040, May 2008.

[9] J. Xie, J. He, and P. K. Meher, "Low latency systolic montgomery mul-tiplier for finite field $GF2_m$ based on pentanomials," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 21, no. 2, pp. 385–389, Feb. 2013.

[10] H. Wu, M. A. Hasan, I. F. Blake, and S. Gao, "Finite field multiplier using redundant representation," *IEEE Trans. Comput.*, vol. 51, no. 11, pp. 1306–1316, Nov. 2002.

[11] A. H. Namin, H. Wu, and M. Ahmadi, "Comb architectures for finite field multiplication in F_{2m}," *IEEE Trans. Comput.*, vol. 56, no. 7, pp. 909–916, Jul. 2007.

[12] A. H. Namin, H. Wu, and M. Ahmadi, "A new finite field multiplier using redundat representation," *IEEE Trans. Comput.*, vol. 57, no. 5, pp. 716–720, May 2008.

[13] A. H. Namin, H. Wu, and M. Ahmadi, "A high-speed word level finite field multiplier in F_{2m} using redundant representation," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 17, no. 10, pp. 1546–1550, Oct. 2009.

[14] A. H. Namin, H. Wu, and M. Ahmadi, "An efficient finite field multi-plier using redundant representation," *ACM Trans. Embedded Comput. Sys.*, vol. 11, no. 2, Jul. 2012, Art. 31.

[15] North Carolina State University, *45 nm FreePDK wiki* [Online]. Avail-able: http://www.eda.ncsu.edu/wiki/FreePDK45:Manual

[16] P. K. Meher, "Systolic and non-systolic scalable modular designs of finite field multipliers for Reed-Solomon Codec," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 17, no. 6, pp. 747–C757, Jun. 2009.

[17] K. K. Parhi, *VLSI Digital Signal Processing Systems: Design and Implementation*. New York: Wiley, 1999.

[18] J. L. Massey and J. K. Omura, "Computational method and apparatus for finite field arithmetic," U.S. patent application, 1984.

[19] S. Gao and S. Vanstone, "On orders of optimal normal basis genera-tors," *Math. Comput.*, vol. 64, no. 2, pp. 1227–1233, 1995.

[20] A. Reyhani-Masoleh and M. A. Hasan, "Efficient digit-serial normal basis multipliers over $GF2_m$," *IEEE Trans. Comput.*, vol. 52, no. 4, pp. 428–439, Apr. 2003.

[21] A. Reyhani-Masoleh and M. A. Hasan, "Low complexity word-level sequential normal basis multipliers," *IEEE Trans. Comput.*, vol. 54, no. 2, pp. 98–C110, Feb. 2005.

[22] A. H. Namin, H. Wu, and M. Ahmadi, "A word-level finite field mul-tiplier using normal basis," *IEEE Trans. Comput.*, vol. 60, no. 6, pp. 890–895, Jun. 2011.