iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** IV **Month of publication:** April 2019

DOI: https://doi.org/10.22214/ijraset.2019.4505

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

VLSI Architecture for Systolic-Like Modular Multipliers over GF (2^m) Build on Irreducible All-One Polynomials

Soumya. M[1], Ganesan P[2], Annapurna. G[3]
[1]PG Scholar, [2]Professor, [3]Asst.Professor, Department of E.C.E, Vidya Jyothi Institute of Technology, Hyderabad, India.

Abstract: By using irreducible AOP, an effective recursive formulation is proposed implies systolic implementation of these finite field multiplications over GF (2^m). Here, a recursive algorithm derived for the multiplication and used it in designing a systematic and localized bit-linear dependence graph for computing systolic multiplication. This dependence graph is altered to a fine-grained dependence graph (DG) by using node splitting method. This parallel systolic architecture is mapped from fine-grained DG. Compared to other structures, it doesn't include any global communication for reducing the modules. The proposed architecture has same time compared to other existent bit-parallel systolic structure and includes registers to a lesser extent. This proposed structure has an ascendable latency of l+ [$log_2 s$] +1 cycles which is minimum compared with existing designs. This structure is proposed specifically for hardware complexity in the structure and throughput scalability to meet the area-time tradeoff by maintaining the overall latency in resource-constrained application.
Keywords: All-One Polynomial, Finite Field multiplication, error control systems, VLSI architecture, Systolic Design.

I. INTRODUCTION

With the rapid expansion of the Internet and wireless communications, more and more digital systems are becoming increasingly equipped with some form of cryptosystems to provide various kinds of data security. Many such cryptosystems rely on computations in very large finite fields and it requires fast computation. Finite fields arithmetic multiplication over GF (2^m) has gained very high importance to obtain secure communication by integrating elliptical curve cryptography (ECC) and error control systems. Among the different basis of multipliers polynomial basis are relatively easy to design, and subjects to scalability for the higher order fields. The real-time applications are hard-ware efficient with polynomial-based multiplication [1].Multipliers with different basis of representations are normal basis, dual basis and polynomial basis used for several applications in earlier cases. Based on a number of significant classes, irreducible polynomials for the field are all-one polynomials can be defined [4]. 1-equally spaced polynomials (or) All-one polynomials (AOP) form a special class, which can be used for simpler and more efficient implementation compared to trinomials and pentanomial-based multipliers. The AOP-based representations of elements are expected to have potential application in elliptic curve cryptosystems and error control coding procures efficient hardware implementation. The first multiplier for GF (2^m) generated by AOP which was followed by some bit-parallel architectures[8].The bit-parallel designs are useful for low-latency realization, but due to their large critical path, they cannot provide high throughput rate and involve high average computation time which increases rapidly with the field order m.

II. PROPOSED DESIGN

The proposed finite field multiplication over GF(2^m) over an irreducible all-one polynomial is outlined as follows,

A. Algorithm for Multiplication

1) *Step-1:* Multiplication is performed for bit b_0 with input operand A, which results $b_0 \cdot A$. Initialize the first (m−1) bits of a finite field accumulator by ($b_0.a_i$), for $0 \le i \le (m-1)$ according to $Y_0=b_0.P_{-1}$,P_{-1}=(0&A). The last bit m^{th} location (i.e., the MSB) of the finite field accumulator initialize to zero.
2) *Step-2:* For i = 1 to (m – 1) which performs cyclic left-shift operation of the polynomial $P_{i-2\alpha}$ of degree (m + 1) to reduce its degree by one to obtain the operand P_{i-1} of degree m. Firstly, to perform bit-level multiplication of bi with P_{i-1} to obtain Y_i according to $Y_i= b_i . P_{i-1}$, for $1 \le I \le$ (m-1). (1) Secondly, Add Y_i to the content of the FFA to obtain the partial result of degree m, $Y=\sum_{i=0}^{m-1} Y_i$ (2)

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

3) *Step-3:* To perform the modular reduction of Y and to reduce the degree from m to (m − 1) according to C=Y mod Q(z) $=(y_0 \oplus y_m)+(y_1 \oplus y_m)\propto+(y_2 \oplus y_m)$.Type equation here.$^2+\ldots\ldots.+(y_{m-1} \oplus y_m).\propto^{m-1}$ (3)

This results in product value. Note **:** STEP-1 is considered as pre-processing step, STEP-2 carries the recursive operations of the proposed algorithm, while STEP-3 is considered as a post-processing step.

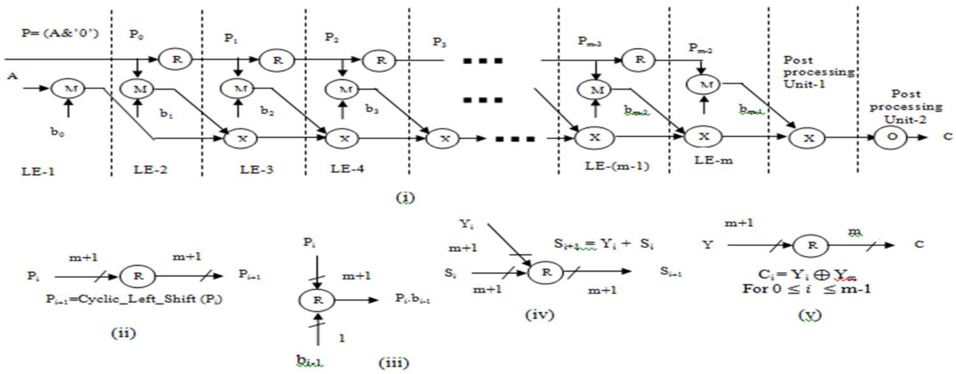


Fig. 1. The dependence graph (DG) for recursive formulation of the finite field multiplication based on irreducible AOP over GF(2^m). (i) The dependence graph. (ii) structure of reduction node R. (iii) Functional sorting of bit-multiplication node M. (iv) Structural description of the Addition node X. (v) Functional description of the output reduction node O.

This exaggerates two major disadvantages .Firstly, since latency of the DG is m (field order).Secondly, the combinational circuit complexity has overtaken the register complexity since neighboring PE receives transferred bits by three registers. To avoid these problems, we derive here a parallel structure of multipliers for GF(2^m) based on irreducible AOP with low register complexity. Moreover, for hardware-efficient realization we have proposed a time-multiplexed structure, where throughput can be traded-off against area with moderate increase in latency.

B. Parallel Systolic Structure

We project to partition the one-dimensional DG by LUs and rearrange the LUs into a two-dimensional parallel systolic array. for a finite field of order m, we generally have m = ls – r. (5) where r is an integer in the range of [0,l]. When r > 0, the multiplicands are padded with r-bit zeros. The construction of a two-dimensional dependence graph for m = 56 is shown in Fig. 2 we pick out l = 7,s = 4, and r = 0 for the proposed design.

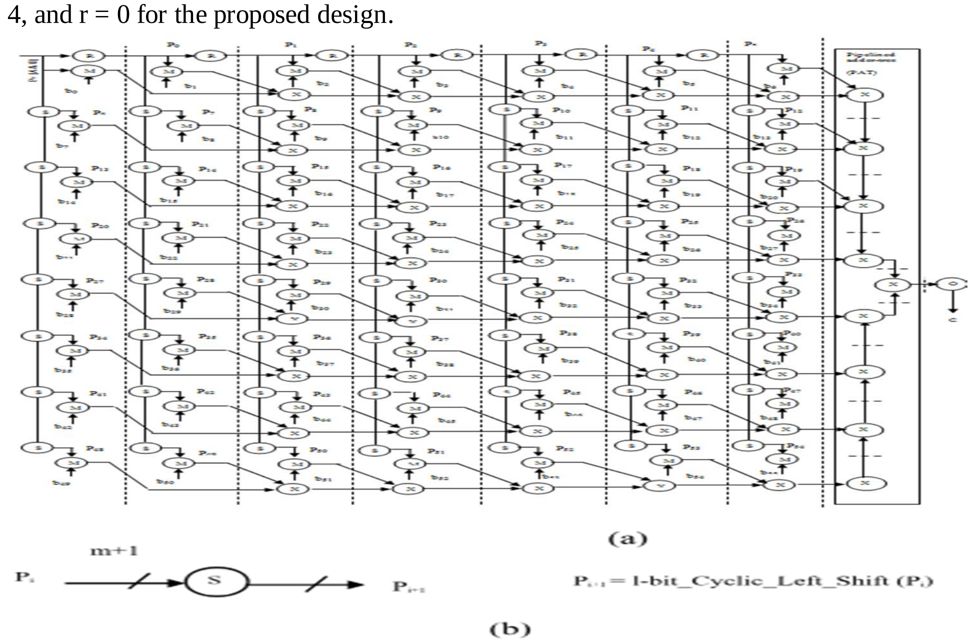


Fig. 2. The Regularized Dependence Graph (DG) for the Finite Field Multiplication over G F(2m) for Irreducible AOP. (a) The DG. (b) Function Description of Multi-Reduction Node S.

From fig 3, It perform the function of 4 multiplication nodes M. Each of the other PEs (the regular PEs: PE-3 to PE-7) consists of four AND cells and four XOR cells to perform the functions of multiplication nodes and Addition nodes. Except the last PE, all other PEs require one reduction cell to implement the function of node R. The reduction nodes are implemented by rewiring of bits, which do not require combinational resources. The last PE or PE-7 does not require the operation of reduction node R, otherwise its function is the same as other regular PEs. Total latency of this structure is 10 cycles (7 cycles in PEs, 2 cycles in PAT and 1 cycle for ORC), and it produces one product word in each cycle once the pipeline is filled-in during the latency period. The duration of cycle period T = T_X, where T_X is the delay of an XOR gate.

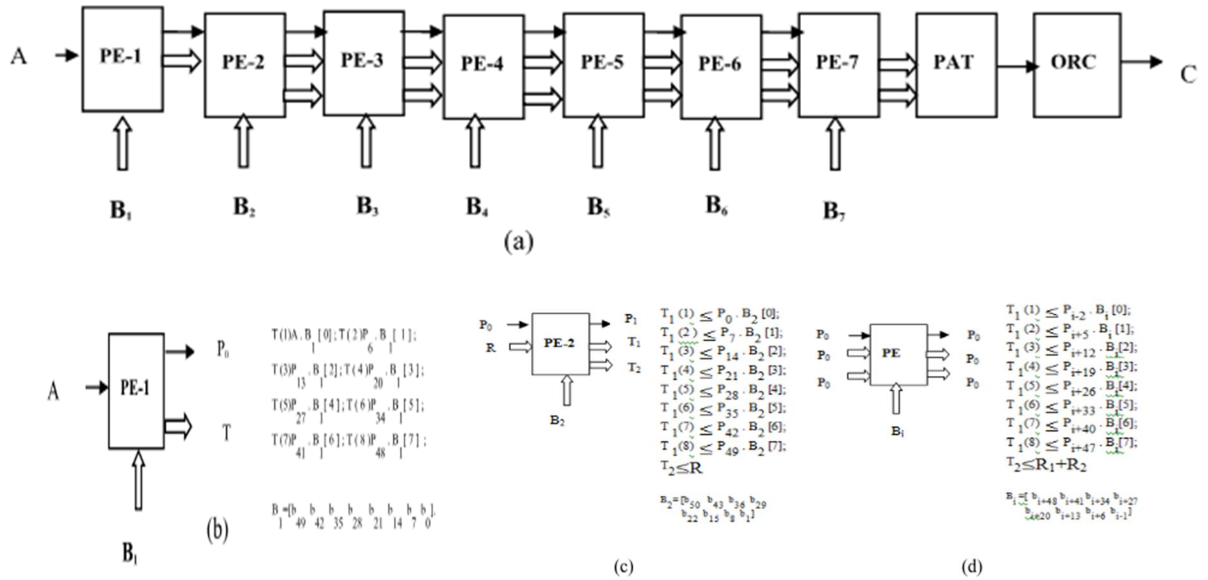
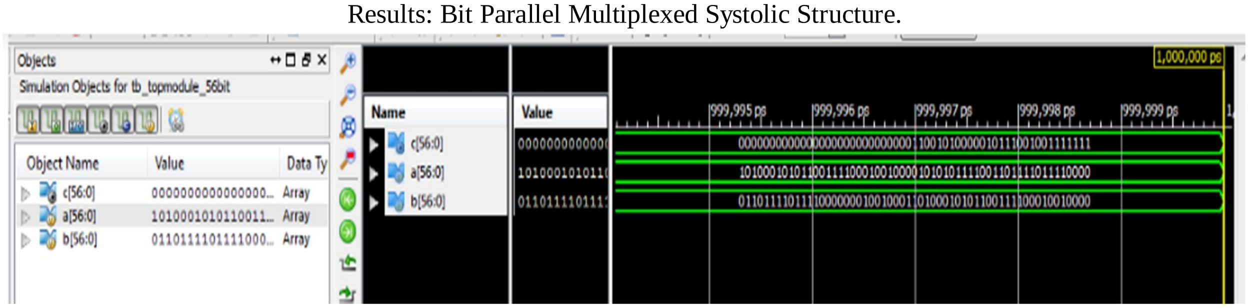


Fig. 3. The Proposed Parallel Systolic-Like Array for the Finite Field Multiplication over G F (2^m) based on Irreducible AOP. (a) The Linear Array Structure. (b) Function of PE-1. (c) Function of PE-2. (d) Function of the ith regular PEs (PE-3 to PE-7).

Table I: Comparison of Bit parallel Systolic Structure with Existing Structures

Performance parameter	Bit parallel systolic structure m=56	Bit parallel systolic structure m=28
No. of slices	737/8672	189/8672
No. of LUTs	1367/1920	5/1920
Delay (ns)	3.213	6.067
Power consumption (mw)	0.081	0.158
Fan-out	29	72
Net delay (ns)	1.436	2.328
Gate delay (ns)	1.218	2.185
Throughput (mbps)	4616	5216

Results: Bit Parallel Multiplexed Systolic Structure.



C. Time-Multiplexed Systolic Structure

To obtain an hardware-efficient implementation, the procedure of the rows of logical units (LU) of the 2-D dependence graph in Fig. 2 can be time-multiplexed. The adder tree in Fig. 2 could be implemented by a finite field accumulator (FFA). The TM-1 structure of multiplier for G F (2^m) based on irreducible AOP is shown in Fig. 4 for m = 56. It performs the reduction of degree of Y from m to (m −1) to produce the desired product word C according to (3). The input operand A is appended with a zero, and the (m + 1) bit word P−1 thus generated is fed to PE-1 through a multiplexer, while the first 7 bits of operand B are fed to the seven PEs of the structure in a staggered manner. After 7 cycles PE-7 produces the output.

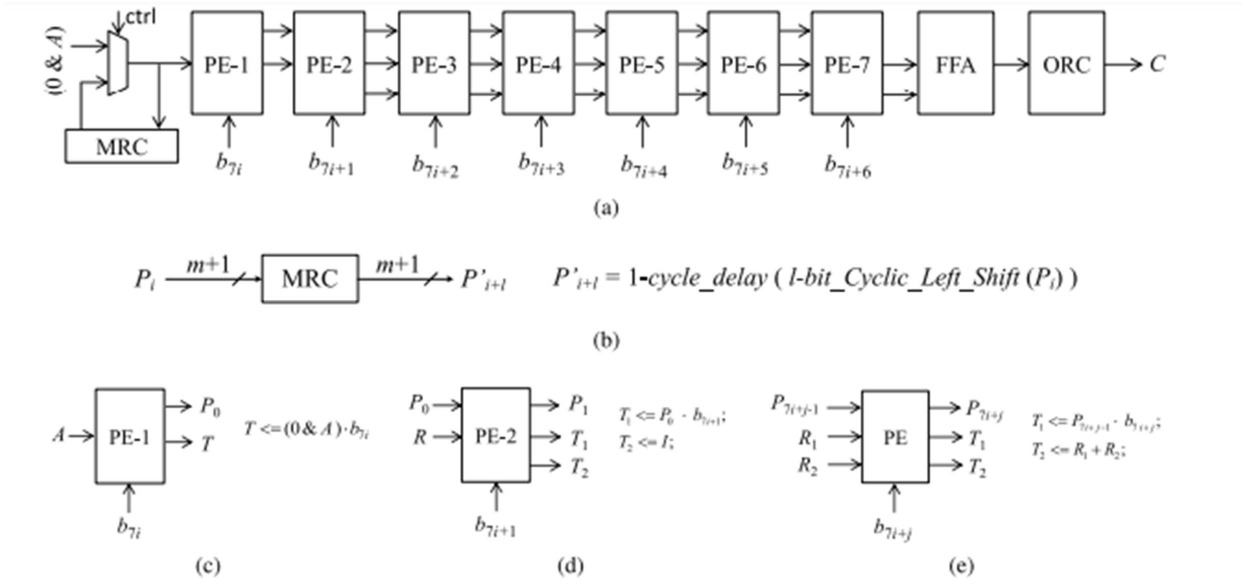


Fig. 4. Projecting the Time-Multiplexed Systolic-Like Array (TM-1) for the Finite Field Multiplication over G F (2^m) based on Irreducible AOP. (a) The Linear Array Structure. (b) Function of MRC. (c) Function of PE-1. (d) Function of PE-2. (e) Function of the ith regular PEs (PE-3 to PE-7).

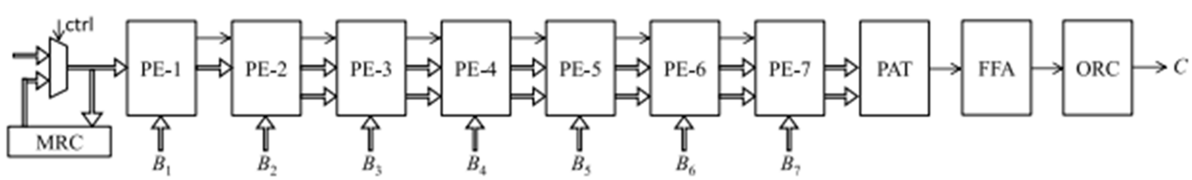


Fig. 5. Time-multiplexed systolic-like array (TM-n) for the Finite Field Multiplication over G F (2^m) based on Irreducible AOP.

The multiple-reduction cell (MRC) is used to implement the function of nodes S from fig.5. It reduces the input operand by order 7 in each cycle iteratively to generate successive input operands for the systolic array. The output of PE-7 is fed to the finite field accumulator (FFA) to implement the function of the pipeline-adder-tree in a sequential manner.

Table II: Comparison of Existing Time Multiplexed Systolic Structure

Performance parameter	Time multiplexed systolic structure	Time multiplexed systolic structure
	m=56	m=28
No. of slices	566/8672	189/8672
No. of LUTs	772/1920	5/1920
Delay (ns)	4.052	6.067
Power consumption (mw)	0.081	0.087
Fan-out	36	78
Net delay (ns)	0.482	1.226
Gate delay (ns)	0.591	1.106
Throughput (mbps)	4616	5216

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

Results:Time Multiplexed Systolic Structure

III. CONCLUSIONS

Systolic multiplication over GF (2^m) outcomes with an efficient recursive algorithm which reduced the latency of the structure using irreducible AOP. The reduction of critical path to one XOR gate delay obtained by novel cut-set retiming by sharing of registers for the input operands in the PEs, we have derived a low-latency bit parallel and time multiplexed systolic multiplier. Compared with the existing systolic structures for bit-parallel realization of multiplication over GF (2^m), the proposed one is found to involve less area, shorter critical-path and less latency. From FPGA synthesis results we find that the proposed design involves significantly less than the existing designs. Moreover, our proposed design can be extended to further reduce the latency.

REFERENCES

[1] Jiafeng Xie, Pramod Kumar Meher, and Jianjun He, “Low-Complexity Multiplier for GF (2^m) Based on All-One Polynomials”, IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 21, No. 1, January 2013.

[2] P. K. Meher, “Systolic formulation for low-complexity serial-parallel implementation of unified finite field multiplication over GF(2^m),” in Proc. 18th IEEE Int. Conf. Appl.-Specific Syst., Archit. Process. (ASAP), Jul. 2007, pp. 134–139.

[3] R. Katti and J. Brennan, “Low complexity multiplication in a finite field using ring representation,” IEEE Trans. Comput., vol. 52, no. 4, pp.418–427, Apr.2003.

[4] A. Reyhani-Masoleh and M. A. Hasan, “Low complexity bit parallel architectures for polynomial basis multiplication over *GF(2m)*,” IEEE Trans. Comput., vol. 53, no. 8, pp. 945–959, Aug. 2004.

[5] A. Reyhani-Masoleh and M. A. Hasan, “A new construction of Massey–Omura parallel multiplier over GF (2^m),” IEEE Trans Comput., vol. 51, no. 5, pp. 511–520, May 2002.

[6] C. H. Kim, C.-P. Hong, and S. Kwon, “A digit-serial multiplier for finite field GF (2^m),” IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 13, no. 4, pp. 476–483, 2005.

[7] C. Paar, “Low complexity parallel multipliers for Galois fields GF ((2^m) 4) based on special types of primitive polynomials,” in Proc. IEEE Int. Symp. Inform. Theory, 1994, p. 98.

[8] Z.-H. Chen, M.-H. Jing, J.-H. Chen, and Y. Chang, “New viewpoint of bit-serial/parallel normal basis multipliers using irreducible all-one polynomial,” in Proc. IEEE Int. Symp. Circuits Syst. (ISCAS), May 2006, p. 4.

[9] S. Fenn, M.G. Parker, M. Benaissa, and D. Taylor, “Bitserial multiplication in GF (2^m) using all-one polynomials,” IEE Proc. Com. Digit. Tech., vol. 144, no. 6, pp. 391–393, 1997.

[10] K.-Y. Chang, D. Hong, and H.-S. Cho, “Low complexity bit-parallel multiplier for GF (2^m) defined by allone polynomials using redundant representation,” IEEE Trans. Computers, vol. 54, no. 12, pp. 1628–1629, Dec. 2005.

[11] H.-S. Kim and S.-W. Lee, “LFSR multipliers over GF (2^m) defined by all-one polynomial,Integr” VLSI J., vol. 40, no. 4, pp. 571–578, 2007.