Design of Low Register all One Polynomial Multipliers Over GF (2^m) on FPGA

M Srilatha, M Lavanya, M Saritha, M Suguna

***Abstract:** This paper presents All-one-polynomial (AOP)-based systolic multipliers over GF (2m) need aid as a rule not acknowledged for useful execution for cryptosystems for example, elliptic bend cryptography (ECC) because of security motivations. Also that, systolic AOP multipliers typically suffer from those issue from the secondary register-complexity, particularly alongside field programmable gate array (FPGA) platforms the place the register assets need aid not that abundant. This paper however, we have demonstrated that those AOP-based systolic multipliers could effortlessly accomplish low register-complexity usage and the recommended architectures could be utilized concerning illustration calculation cores with infer efficient usage from the systolic Montgomery multipliers In view of trinomials, which need aid recommended by the National institute of standard and technology (NIST) for cryptosystems. This paper, first we recommend a novel information television plan alongside which the register-complexity included inside existing AOP based systolic multipliers may be significantly decreased.*

We have found crazy that to useful usage, the modified AOP-based systolic structure can a chance to be stuffed concerning illustration a standard calculation core.

Now we propose the novel Montgomery multiplication algorithm that can fully employ the proposed AOP based computation core.

"The proposed architectures are then implemented by Xilinx ISE 14.1 and it is shown that compared with the existing designs, the proposed designs achieve at least 70.0% and 47.6% less "area-delay product (ADP) and power-delay product (PDP) than the best of competing designs", respectively". Those suggested architectures are at that point actualized by Xilinx ISE 14. 1 and it may be demonstrated that compared for the existing designs, the suggested outlines accomplish in any event 70.0% and 47. 6% less "area-delay Product (ADP) and power-delay product" (PDP) over those best about contending designs, separately.

***Key Words:** Finite field multiplication, systolic structure, low complexity, Montgomery algorithm, irreducible trinomials.*

Revised Manuscript Received on October 22, 2019.

M Srilatha, Dept. of ECE, AAR Mahaveer Engineering college, Hyderabad, India

M Lavanya, Dept. of ECE, Institute of Aeronautical Engineering, Hyderabad, India.

M Saritha, Dept. of ECE, Institute of Aeronautical Engineering, Hyderabad, India

M Suguna, Dept. of ECE, Institute of Aeronautical Engineering, Hyderabad, India

I. INTRODUCTION

Finite field multiplication through GF (2m) will be broadly utilized within elliptic curve cryptography (ECC) frameworks. The national institute of standard and technology (NIST) need recommended two trinomials for ECC usage. Therefore, a number from works meets expectations need been suggested in the expositive expression for productive multiplication in GF (2m) In view of irreducible trinomials..

Around at these works, digit-serial systolic multipliers have picked up more excellent consideration as of late. Not best do they give adjusted tradeoff the middle of region unpredictability and period intricacy as well as they have features for example, such that modularity, regularity, Furthermore neighborhood interconnections. Every last one of PEs on a systolic exhibit will be fully pipelined to prepare a higher throughput rate.

In recent years, the Finite Field algorithm as one of the high efficiency and low complexity algorithms have already been used in various fields, such as error-control codes, information theory and "elliptic curve cryptography" (ECC). It can be used in various devices, such as wearable devices, key agreement and bank account systems. On one side, cryptographic system and algorithm should be high resistible to reduce the potential attacks, on the other side, the complexity of the cryptographic system shall be reduced. Basically, there are two bases, polynomial basis and normal basis, which can be selected to represent the field operation. Nevertheless, in hardware realization, polynomial basis multipliers are more widely used compared to normal basis multipliers.

All-one-polynomials (AOPs) also trinomials need aid two of the imperative irreducible polynomials constantly utilized. Those AOP-based multipliers might make utilized for the almost AOP, which Might make utilized to effective acknowledgment about cryptosystems. The AOP-based structures might be utilized concerning illustration An portion out to field exponentiation, inversion, and more division architectures, same time trinomial based multipliers are more prevalent over AOP-based ones, Similarly as two trinomials need been proposed by the "National institute of standard and technology (NIST) to ECC usage". However, due to those intricacy differences, AOPs and trinomials are not generally recognized together to useful field multiplication usage.

II. LITERATURE REVIEW

There are essentially two sorts for structures to multipliers through GF (2m): systolic plan and more non-systolic configuration. Systolic multipliers again GF (2m) In light of irreducible polynomials would favored Previously, high-octane provisions because of their features for example, modularity and normality. Systolic structures likewise have high register-complexity since know “processing elements (PEs)” in the systolic show necessity to utilize registers to pipelining, same time non-systolic outlines generally bring down multifaceted nature with bigger critical-path delay. For useful applications, particularly in “field-programmable gate array (FPGA) platforms”, the place the register-resources are not the individual’s abundant, low register-complexity systolic structures are required. A number deliberations need been showed up for diminish those register-complexity over systolic multipliers In view of irreducible AOPs and more trinomials.

In this we combine low register-complexity and Montgomery multiplication algorithm together to speed up the multiplication process.

2.1 AOP Systolic Multiplier Based on Trinomial

There are some designs about finite field systolic multiplier based on trinomial have been reported. Most of these designs focus on the way to design the PEs inside of multiplier based on the critical-path. In this, we have two kinds of structure with critical paths of $T_A + T_X$ and $_{MAX}\{T_A; T_X\}$, where the duration of each cycle period is $T_A + T_X$ (T_A and T_X refer to the delay of an AND gate and a XOR gates respectively). The critical-path of the second structure is shorter than the first one, so it has lower latency. But the second multiplier needs more registers.

The efficiency of multiplier will be limited if we only use one algorithm. So the main contribution needs to combine another novel Montgomery Algorithm together to improve the overall efficiency. Inside of the structure, we can apply the strategies of registers sharing and parallel-array pipelining to decompose the linear systolic design into several parallel arrays. According to the characteristics of one the inputs matrix, we can observe that each two adjacent columns have mostly the same elements. Correspondingly, every two adjacent PEs can share the same input operands. In this way, we not only can decrease the latency and amount of registers but also can decrease the number of XOR gates. In order to confirm the design, we choose m = 233 which has been recommended by NIST.

As we all know, the NAND gate is usually faster than the AND gate, so we use NAND to instead all AND in original structures. In order to satisfy the logic functions, we also need to change the XOR gate to XNOR. Besides that, there is a need to redesign the wire connections between each shift unite. After changing these components, we can realize the same function with lower latency and lower register-complexity circuits.

III. PROPOSED SYSTOLIC STRUCTURE

The efficiency of multiplier will be limited if we only use one algorithm. So the main contribution of this thesis needs to combine another novel Montgomery Algorithm together to improve the overall efficiency. Inside of the structure, we can apply the strategies of registers sharing and parallel-array pipelining to decompose the linear systolic design into several parallel arrays. According to the characteristics of one the inputs’ matrix, we can observe that each two adjacent columns have mostly the same elements. Correspondingly, every two adjacent PEs can share the same input operands. In this way, we not only can decrease the latency and amount of registers but also can decrease the number of XOR 2gates. In order to confirm the proposed design, we choose m=233 which has been recommended by NIST [15].

As we all know, the NAND gate is usually faster than the AND gate, so we use NAND2 to instead all AND2 in original structures. In order to satisfy the logic functions, we also need to change the XOR2 gate to XNOR2. Besides that, there is a need to redesign the wire connections between each shift unite. After changing these components, we can realize the same function with lower latency and lower register-complexity circuits. We use an example which m=162 to test the proposal in this work.

3.1 Polynomial basis multiplication over $GF\ (2^m)$

Assume there has field F, and the elements $a_n,a_{n-1},a_{n-2}...,a_1,a_0$ belong to field F.Then the expression with the form of $f\,(x) = a_nx^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} ... + a_2x^2 + a_1x + a_0$is calledapolynomialwithdegreenoverF.Theelement$a_i$iscalledthecoefficientofx^iin f(x), and $a_n \neq 0$. Depend on the each power of X and corresponding co-efficient we can justify if this two polynomials are equal or not.

Polynomial ring R[X] is a ring which can be formed by these to f polynomial sin one or more variables (such as x) with coefficients in another ring R (or field). Such as in X over a field P is defined as the set of expressions with the form $f(x)=a_nx^n+a_{n-1}x^{n-1}+ a_{n-2}x^{n-2}... + a_2x^2+ a_1x + a_0$, where a_n, a_{n-1}, a_{n-2}..., a_1, $a_0$are the coefficients which are the elements of field P, then these coefficients can form a ring, called polynomial ring P[x]. Polynomials can be equipped with arithmetic cooperation’s. Two standard operations for polynomials are addition and multiplication. Here is an example. Let $A(x)=x^4+3x^2+2$and $B(x) = 3x^2+ x + 4$ be elements of polynomial ring $R_4[x]$. The multiplications and addition of this two polynomials are:

$$A(x) \cdot B(x) = 3x^6+ x^5+ x^4+ 3x^3+ 2x^2+ 2x + 4$$

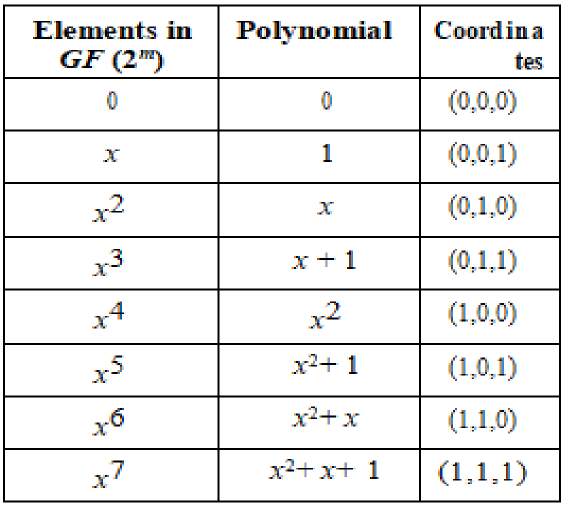
$$A(x) + B(x) = x^4+ 2x^2+ x + 2$$

3.2 Polynomial basis representation over

GF (2^m)

The way to use polynomial basis representation to construct binary field *GF*(2^m) means the elements of *GF* (2^m) are binary polynomials with the degree at most m −1. In this condition the polynomials' coefficients are in the field of *GF* (2). Such as, for finite field *GF*(2^m),the elements in this field are the polynomials$\{0,1,x,x+1,x^2,x^2+1,...,x^{m-1}+ x^{m-2}+ ... + x + 1\}$, where the x is a root of an irreducible polynomial $f(\alpha)$ over *GF* (2), and the polynomial coefficients are *GF* (2) = {0, 1}, where $f(x)$ =0.

We can use an example to show the exactly elements for finite field based on polynomials. The elements of finite field *GF* (2^3) are as follows



Elements in *GF* (2^m)	Polynomial	Coordinates
0	0	(0,0,0)
x	1	(0,0,1)
x^2	x	(0,1,0)
x^3	$x + 1$	(0,1,1)
x^4	x^2	(1,0,0)
x^5	$x^2+ 1$	(1,0,1)
x^6	$x^2+ x$	(1,1,0)
x^7	$x^2+ x+ 1$	(1,1,1)

Table.1. elements of finite field *GF* (2^3)

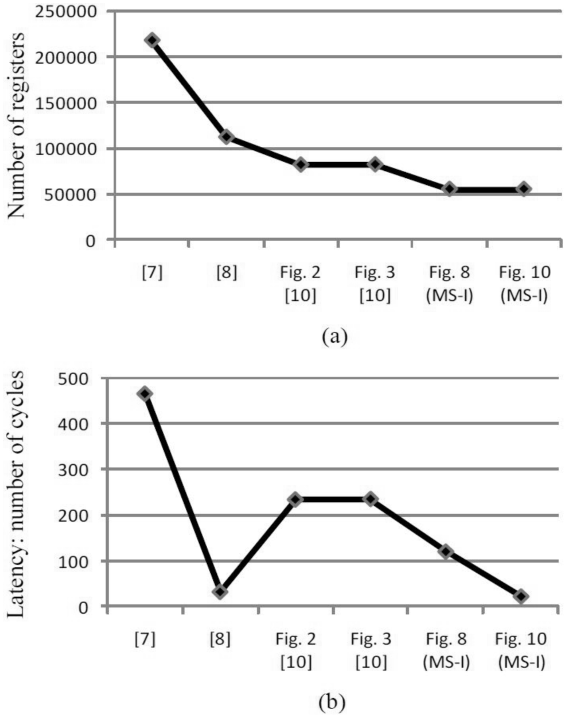
3.3 AOP based structures with FPGA implementation

We have additionally executed these AOP-based systolic structures will confirm the efficiency for suggested structures. We need synthesized these outlines utilizing Xilinx ISE14. 1onVirtex 6 crew gadget for k = 162. The comes about As far as area-time-power unpredictability are indicated to table II. It might a chance to be seen that the recommended structures beat those existing ones, particularly for area-complexity. Since there is just minor difference the middle of critical- ways about TNA+ TXN and more TXN on FPGA platforms, the recommended MS-II doesn't bring significant point over existing ones. Therefore, those recommended MS-I might a chance to be utilized more generally over MS-II in commonsense requisitions.

3.4 Area and Time Complexities

The area and time through complexities as far as rationale entryway count, register count, latency, and critical-path of the suggested structures also existing structures.

The recommended outlines beat those existing designs, particularly in the register check. The recommended plans need more level area-time multifaceted nature over ×the outline about [7]. When compared with the low-latency super×systolic structure of [8], those suggested configuration (Fig. 5. 4) need shorter inactivity (if we decide e = m) Furthermore less registers. At contrasted with the two later outlines over [9] and [10], the suggested plans not main need bring down register count, as well as include significantly easier inactivity.



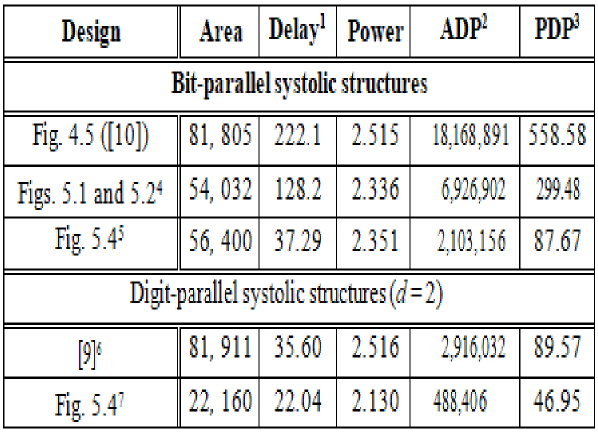
(a)

(b)

Figure.1. Comparison of register count and latency of various bit parallel structures based on trinomial $f(x) = x^{233}+ x^{74}+ 1$. A) Comparison of number of registers required by various designs. B) Comparison latency

IV. SIMULATION RESULTS

Shown the below table as comparison of various complexities



Design	Area	Delay[1]	Power	ADP[2]	PDP[3]
Bit-parallel systolic structures					
Fig. 4.5 ([10])	81, 805	222.1	2.515	18,168,891	558.58
Figs. 5.1 and 5.2[4]	54, 032	128.2	2.336	6,926,902	299.48
Fig. 5.4[5]	56, 400	37.29	2.351	2,103,156	87.67
Digit-parallel systolic structures ($d = 2$)					
[9][6]	81, 911	35.60	2.516	2,916,032	89.57
Fig. 5.4[7]	22, 160	22.04	2.130	488,406	46.95

Table.2. Comparison of area time complexities of various designs based on trinomial $f(x) = x^{233}+ x^{74}+ 1$

Unit for Area: number of slice register; Unit for delay: *ns*; Unit for power: W (power is estimated at 100MHz).

[1]: Delay = Latency.

[2]: ADP: Area-delay product = Area Delay.

[3]: PDP: Power-delay product = Power Delay.

[4]: based on structure of MS-I with $e = 2$.

[5]: based on structure of MS-I with $e = 16$ and $d = 1$.

[6]: structure here has 16 parallel systolic arrays ($d = 2$).

[7]: based on structure of MS-I with $e = 16$ and $d = 2$.

V. CONCLUSION

This design focuses on finite field trinomial multiplier with AOP core, and also use Mont gomery algorithm to improve the speed of the multiplier. The speed and complexity are two main points of hardware. There are multiple structures and algorithm which had been developed depending on the previous designs. In this thesis, our design focuses on finite field which can reduce the complexity of arithmetic.

VI. FUTURE SCOPUE

After finishing this thesis, we know that if we want to design a better circuit, we need to combine using new algorithm and optimizing structure. Only try to decrease the components based on the structure without applying new algorithm has its limitation. Montgomery algorithm act an important role this paper. Similar strategy can be used in some new algorithms, such as Karatsnba algorithm or TMVP. Using different algorithm can get totally different structures which can change the latency and area significantly

REFERENCES

1. Pingxiuqi Chen, Shaik Nazeem Basha,Member, IEEE, and Jiafeng Xie, “FPGA Realization of low register Systolic AOP Multipliers Over GF(2^m) and Their Apllications in Trinomial Multipliers,” IEEE Trans.
2. I. F. Blake, G. Seroussi, and N. Smart, Elliptic Curves in Cryptography (London Mathematical Society Lecture Note Series). Cambridge, U.K.: Cambridge Univ. Press, 1999.
3. N. R. Murthy and M. N. S. Swamy, “Cryptographic applications of Brahmagupta–Bhˇaskara equation,” IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 53, no. 7, pp. 1565–1571, Jul. 2006.
4. M. Sun et al., “eButton: A wearable computer for health monitoring and personal assistance,” in Proc. 51st Design Autom. Conf., 2014, pp. 1–6.
5. D. Schinianakis and T. Stouraitis, “Multifunction residue architectures for cryptography,” IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 61, no. 4, pp. 1156–1169, Apr. 2014.
6. K. K. Parhi, VLSI Digital Signal Processing Systems: Design and Implementation. New York, NY, USA: Wiley, 1999.
7. C.-Y. Lee, J.-S. Horng, I.-C. Jou, and E.-H. Lu, “Low-complexity bitparallel systolic Montgomery multipliers for special classes of G F(2m),” IEEE Trans. Comput., vol. 54, no. 9, pp. 1061–1070, Sep. 2005.
8. P. K. Meher, “Systolic and super-systolic multipliers for finite field G F(2m) based on irreducible trinomials,” IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 55, no. 4, pp. 1031–1040, May 2008.
9. J. Xie, P. K. Meher, and J. He, “Low-latency area-delay-efficient systolic multiplier over G F(2m) for a wider class of trinomials using parallel register sharing,” in Proc. IEEE Int. Sym. Circuits Syst., May 2012, pp. 89–92.