Middle-East Journal of Scientific Research 21 (11): 2064-2071, 2014
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2014.21.11.21795

Low Complexity Multiplier for GF (2^m) Based All One Polynomial

M. Anto Bennet, M. Manimaraboopathy, P. Maragathavalli and T.R. Dinesh Kumar

Department of ECE, VELTECH, Chennai-600062, India

Abstract: The area-time-efficient systolic structure for multiplication over GF (2m) based on irreducible all-one polynomial (AOP) and used a novel cut-set retiming to reduce the duration of the critical-path to one XOR gate delay. Basically, this paper is depends on digital electronics(ie.,logic gates)how to reduce the gate count.Finally it is used for what are techniques available in electronics(VLSI advanced technology).Here going to do is to reduce the power consumption,reduce the gate count,and to reduce the critical path in XOR gate in real time application.In input using the technique called register sharing an cut set retiming in that how to reduce the components and to get in area time efficient of systolic structure. The result obtained is in real time application of security purposes for example ATM,etc., to get the area time efficient systolic structure and security purposes in advanced VLSI technology. The application of the paper is mainly for security purposes and for irreducible polynomial of efficient implementation.

Key words: All-One Polynomial · Elliptic Curve Cryptography · System on Chip

INTRODUCTION

Finite Field Multipliers over GF (2^m) have wide applications in Elliptic Curve Cryptography (ECC) and Error Control Coding systems. Polynomial basis multipliers are popularly used because they are relatively simple to design and offer scalability for the fields of higher orders. Efficient hardware design for polynomial-based multiplication is therefore important for real-time applications. All-One Polynomial (AOP) is consists of binary number 0's and 1's considered suitable for systolic multipliers. The circuit complexitycan be reduced by using irreducible algorithm in each stage the number of gates are used that can be reduced at last obtained an single gate. Thereby, To achieve high throughput based on application. Thus the overall circuit complexity is reduced. All-one polynomial (AOP) is one of the classes ofpolynomials considered suitable to be used as irreducible polynomial for efficient implementation of finite field multiplication. Finite Field Multipliers over GF (2^m) have wide applications in Elliptic Curve Cryptography (ECC) and Error Control Coding systems. Polynomial basis multipliers are popularly used because they are relatively simple to design and offer scalability for the fields of higher orders. Efficient hardware design for polynomial-based multiplication is therefore important for real-time applications. The design of systolic arrays is the mapping of the algorithm to the processor array. However, not all algorithms can be systolized. Only highly regular algorithms with the structure of nested loops are suitable for systolic implementation. Systolic implementation of multiplication over GF(2^m) is usually very efficient in area-time complexity, but its latency is usually very large. Thus, two low latency systolic multipliers over GF(2^m) based on general irreducible polynomials and irreducible pentanomials. Systolic arrays have been designed for a wide variety of computationally intensive problems in signal processing, numerical problems, pattern recognition, database and dictionary machines, graph algorithms. Finite Field Multipliers have wide applications in Elliptic Curve Cryptography (ECC) and Error Control Coding systems. Polynomial basis multipliers are popularly used because they are relatively simple to design and offer scalability for the fields of higher orders. Efficient hardware design for polynomial-based multiplication is therefore important for real-time applications.

Literature Survey: BerkSunar (2004) had proposed a multiplier in convolution algorithm. This algorithm technique is to reduce the delay logarithmic in bit length. The advantages are reducing the complexities and area efficiency is high. The disadvantages is space complexity is high [1].Hanho Lee (2003) had proposed an architecture

Corresponding Author: M. Anto Bennet, Department of ECE, VELTECH, Chennai-600062, India.

called high speed Reed-Solomon(RS) decoder architecture using modified algorithm for fiber optic rates. This decoder implements 0.13m CMOS standard technology. The advantage is high speed data processing and detection and correction of errors. The disadvantage is critical path is high at a clock frequency [2].NeethuJohny and Binoy Joseph(2013) had proposed an finite field multipliers over GF (2^m) used in technology like Elliptical Curve Cryptography(ECC) and Error Coding techniques. The advantage is to reduce the critical path in pipelining digital circuits and to reduce the time delay. The disadvantage is area efficient is little bit high [3]. ChiouYng Lee *et al* (2005) had proposed an Booth's algorithm using low complexity in dual basis multipliers. It saves about 9% space complexity. The advantage is parallel reduction of both space and time complexities. The disadvantage is multi bit processing is low in this process [4].Jean Claude *et al* (2010) had proposed an binary field multiplication representation in double polynomial system. It approach Fourier transform to perform reduction. The advantage is to avoid a multiplication required in Montgomery algorithm and in efficient method. The disadvantage is high complexity in this multiplier [5]. Henriquez (2003) had proposed an Galois field GF(2m) generated advantage in a space and time complexities. To reduce the multiplication by using irreducible polynomial in coding techniques. The advantage is to reduce the delay and complexities. The disadvantage is parallel multipliers in multilevel bit is less complexity [6]. YadollahEslami *et al* (2006) had proposed an Cryptography for secure purposes in electronic devices. It occupies small area; consume low power in this algorithm. The advantage is power consumption and less area delay. The disadvantage is multi bit of storage is less [7]. H.W. Leong *et al* (2002) had proposed a micro coded elliptic curve processor in FPGA technology. Using this technology to reduce the chip's i/o requirements. The advantage is control part of processor is micro coded in FPGA processor. The disadvantage is power consumption is high and cost is high [8].CancioMonterio *et al* (2013) had proposed a bit parallel multiplier over Galois field arithmetic algorithm in the circuit architecture. It implements the secure and low power dual logic circuit in bit parallel multiplier. The advantage is using CMOs technology to reduce the power consumption. The disadvantage is better security in high frequency rate [9]. Bimal Kumar Meher (2009) had proposed an finite field in efficient design of elliptic curve cryptography and error coding techniques for digital communication The advantage is security purposes and cost effective is low. The disadvantage is less efficient during communication in elliptic curve cryptography [10]. Ashutosh Kumar Singh *et al* (2009) had proposed an error tolerant hardware efficient in very large scale integration architecture for bit parallel systolic multiplication. The advantage is operate in both dual base and polynomial base in efficient manner. The disadvantage is cost is high effective and space complexity is high [11]. Kazutoshi Wakabayashi *et al* (2000) had proposed an System on Chip (SOC) design method and flow from the view points in electronic application system. The advantage is chip is reduced in electronic devices and power consumption is also reduced. The disadvantage is physical design in Soc of electronic devices is little bit difficult [12].

MATERIALS AND METHODS

Processing Elements (PE[0], PE[1], PE[m+1], Regular PE): The structure of PE [0] is shown in Fig.1. It consists of an AND cell and a BSC. Each XOR cells and AND cells in the PE consists of (m+1) number of gates working in parallel. The regular PE, as shown in Fig.2, consists of three basic cells, e.g., the bit-shift cell (BSC), the AND cell and the XOR cell. The PE[m+1] of the systolic structure in Fig.5.3 consists of only an XOR cell, which performs bit-by-bit XOR operations of its pair of m-bit inputs

Delay Unit: In delay units are using D- Flip flop. The D flip-flop tracks the input, making transitions with match those of the input D. The D stands for "data"; this flip-flop stores the value that is on the data line. It can be thought of as a basic memory cell. A D flip-flop can be made from a set/reset flip-flop by tying the set to the reset through an inverter. The result may be clocked.

AC Unit: Besides, an Addition-Cell (AC) is required to perform the final addition of the outputs of the two systolic arrays, as shown in Fig 4. It performs the XOR operation.

BSC (Bit Shift Cell): The bit shifts are sometimes considered bitwise operations, because it operates only the binary representation of an integer instead of its numerical value; however, the bit shifts do not operate on pairs of corresponding bits and therefore cannot properly be called bit-wise. In these operations the digits are moved, or shifted, to the left or right. The BSC in the PE performs the bit-shift operation according to

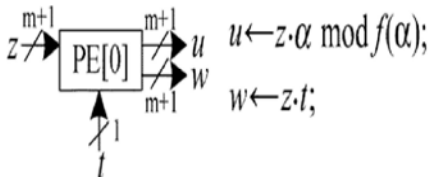

Fig. 1: PE[0]

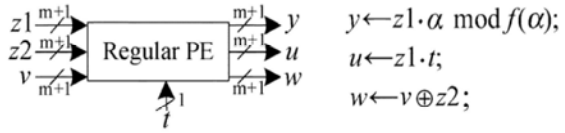

Fig. 2: Regular PE

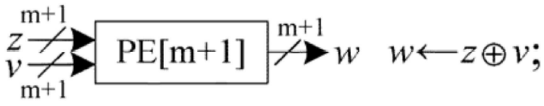

Fig. .3: PE [m+1]

Fig. 4: AC unit

$$A^{i+1}=a_0^{i+1}+a_0^{i+1}+a_1^{i+1}.\alpha+\ldots\ldots\ldots..+a_m^{i+1}.\alpha \quad (1)$$

Systolic Structure: A systolic is said to be reversible if there is a one-to-one and onto mapping between the vectors of inputs and outputs; thus the vector of inputs can be always reconstructed from the vector of outputs. Thus, the number of outputs in a reversible gate or circuits has to be the same as the number of inputs. Output functions of binary reversible logic gates equal to 1 for exactly half their input assignments are called balanced. Logic design of reversible circuits is quite different from designing conventional irreversible logic circuits. In reversible circuits have to use at least one gate is used to duplicate a signal. Moreover, for realization of non balanced Boolean functions with a reversible circuit, it is necessary to add constant signals to input of circuits. A systolic array formed by interconnecting a set of identical data-processing cells in a uniform manner is a combination of an algorithm and a circuit that implements it and is closely related conceptually to arithmetic pipeline.

In a systolic array, data words flow from external memory in a rhythmic fashion, passing through many cells before the results emerge from the array's boundary cell and return to external memory. The external memory connected to the systolic array's boundary cell stores

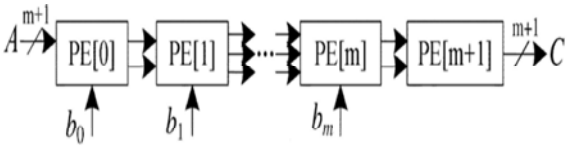

Fig. 5: Systolic Multiplier

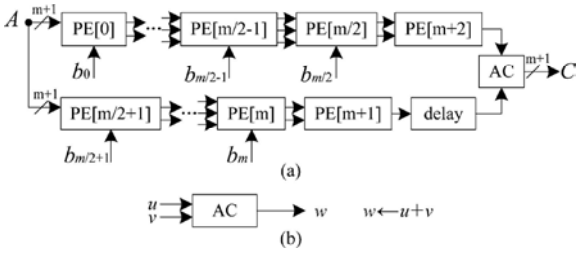

Fig. 6: Low Latency Systolic Multiplier

both input data and results. The underlying principle of systolic array is to achieve massive parallelism with a minimum communication overhead and generally speaking, a systolic array is easy to implement because of its regularity and easy to reconfigure because of its modularity. The classical logic synthesis methods can be used, but they generate too many number of gate output signals, making the circuit extremely complex. The basic design of systolic multiplier thus derived is shown inFig.5. It consists of (m+2) PEs and the functions of the PEs are shown in Fig 5. During each cycle period, the regular PE (from PE [2] to PE [m - 1]) not only performs the modular reduction operation. But also performs the bit-multiplication and bit-addition operations concurrently.

Low Latency Systolic Architecture: For irreducible AOP, m is an even number. Therefore, let l and P be two integers such that (m+1) = lP+r, where r is an integer in the range 0 = r = l. For example, if P=m/2, then l=2, r=1 can be rewritten as

$$C=\sum_{i=0}^{m/2}X_i+\sum_{i=\frac{m}{2}+1}^{m}X_i \quad (2)$$

One of the sum contains [(m/2) +1] partial productswhile the other has m/2 partial products. The systolicstructure of Fig. 6 could be modified to a form shown in Fig. 6(a), which consists of two systolic branches. The upper branch consists of [(m/2) +2]PEs and the lower branch consists of (m/2+1) PEs and a delay cell. Besides, an Addition-Cell (AC) is required to performthe final addition of the outputs of the two systolic arrays, as shown in Fig.6 (b). It is observed that the two systolic

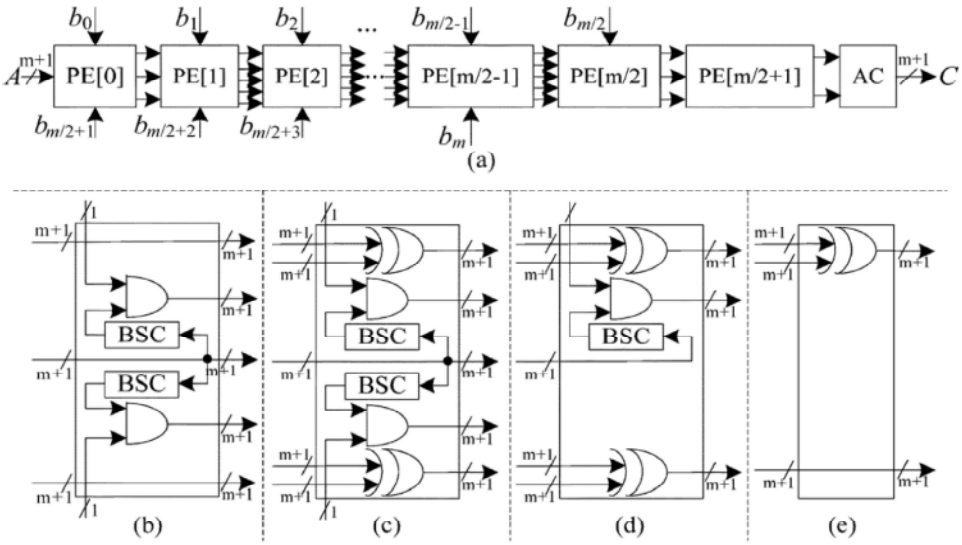

Fig. 7: Low-latency register-sharing systolic structure. (a) The systolic Structure. (b) Structure of PE [1]. (c) Structure of a regular PE (from PE [2] to PE [m/2-1]). (d) Structure of PE [m/2]. (e) Structure of PE [m/2+1].

branches in Fig. 5.6 share the sameinput operand and the PEs in both the branches perform the same operationexcept the last PE in each of the branches.

The proposed structure (Fig.7) requires [(m/2) +2] PEs and one AC. Each of the regular PEs consists of 2(m+1) XOR gates in a pair of XOR cells and 2(m+1) AND gates in a pair of AND cells. Besides, the AC requires (m+1) XOR gates.

These input undergone polynomial multiplication to do polynomial multiplication, the max no. of multipliers are used in order to reduce the no of multipliers by using irreducible algorithm. By this algorithm, No of inbuilt gates to frame an single multiplier have been reduced from 0 to m/2+1 level

RESULTS

The AND operation is used to perform multiplication of two or more inputs. If the inputs are 1,then it produce the result '1'.Otherwise it produce output '0'.is shown in Fig 8.

The Bit Shift Cell is used to shift the input to right by 1 bit position is shown in Fig 9.

The XOR operation is used to produce the result 1 if the inputs are different and produces result 0 if the inputs are same is shown in 0ig 10.

The processing element0 (PE0) produces the corresponding output to the given input and binary digit 0 or 1 by calling the function which is inbuilt in it to perform he specific operation is shown in Fig 11.

The processing element 1 (PE1) produces the corresponding output to the output produced by PE0 and binary digit 0 or 1 by calling the function which is inbuilt in it to perform he specific operation is shown in Fig 12.

The regular PE produces the output to the multiple inputs by comparing it with the binary digit 0 or 1 by calling the function which is inbuilt in it to perform he specific operation corresponding to the input given is shown in Fig 13.

The PE4 produces the corresponding output to the input and binary digit 0 or 1 by calling the function which is inbuilt in it to perform he specific operation and it is added to the additional cell to perform EX-OR operation is shown in Fig 14.

The M=6 systolic structures produces the output to the multiple inputs by comparing it with the binary digit 0 or 1 by calling the function which is inbuilt in it to perform he specific operation corresponding to the input given is shown in Fig 15.

The low latency systolic structure produces the corresponding output to the input and binary digit 0 or 1 by calling the processing element which consists of function which is to be performed is inbuilt in it to perform the specific operation is shown in Fig 16.

The Register Sharing multiplier systolic produces the output to the multiple inputs by comparing it with the binary digit 0 or 1 by calling the function which is inbuilt to perform the specific operation and it is added to the additional cell to perform EX-OR operation.The Register Sharing multiplier mainly used to minimize the register requirement is shown in Fig 17.

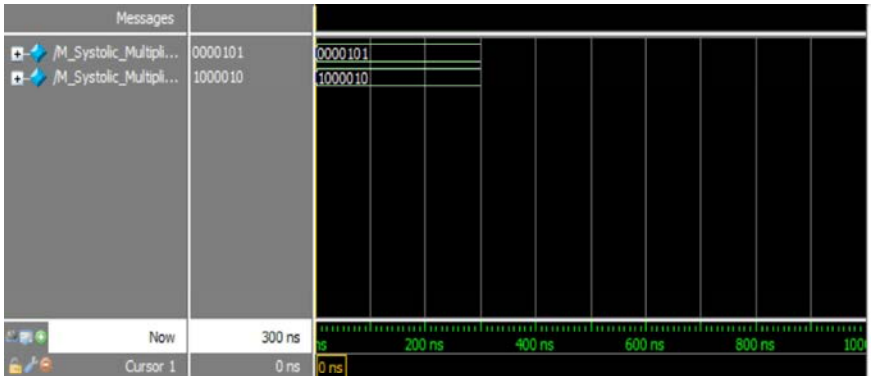

Fig. 8: AND CELL operation

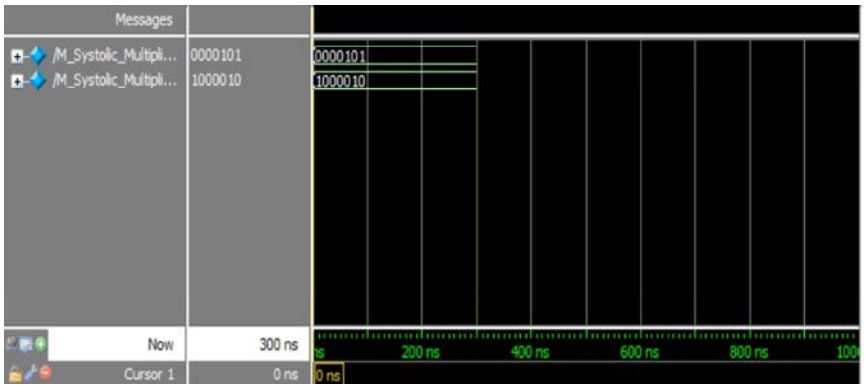

Fig. 9: Bit Shift Cell

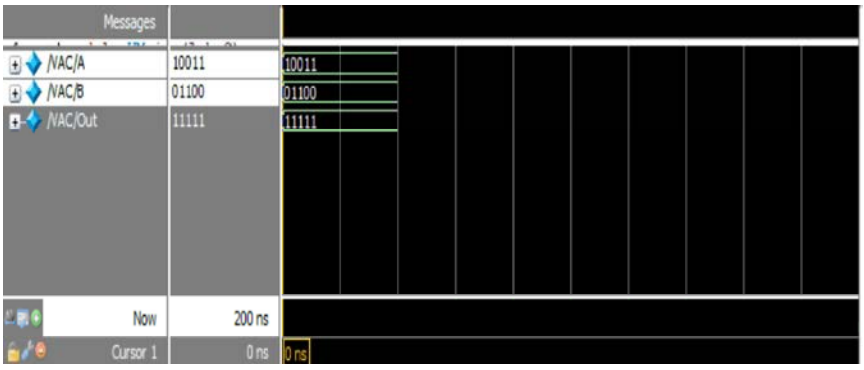

Fig. 10: XOR operation

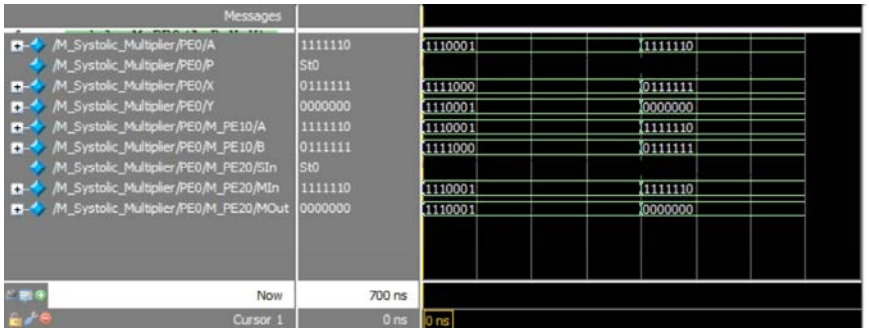

Fig. 11: Processing Element0 (PE0)

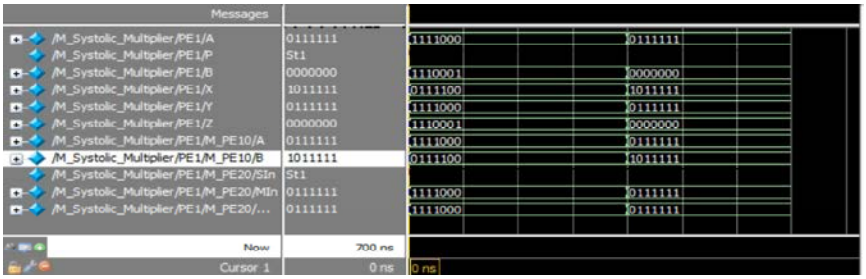

Fig. 12: The Processing Element 1 (PE1)

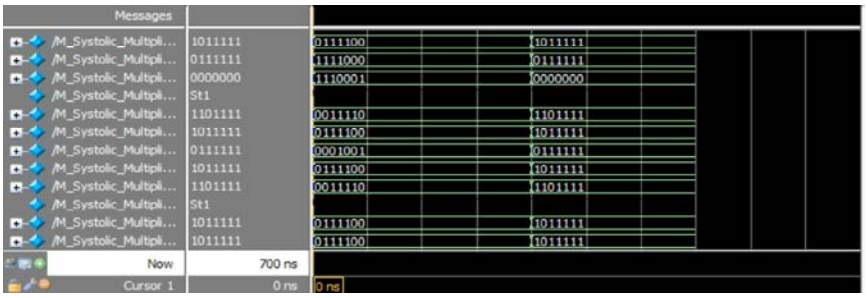

Fig. 13: Regular PE

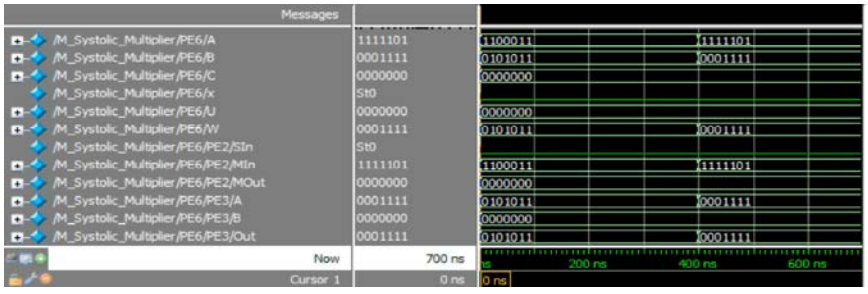

Fig. 14: Processing Element4 (PE4)

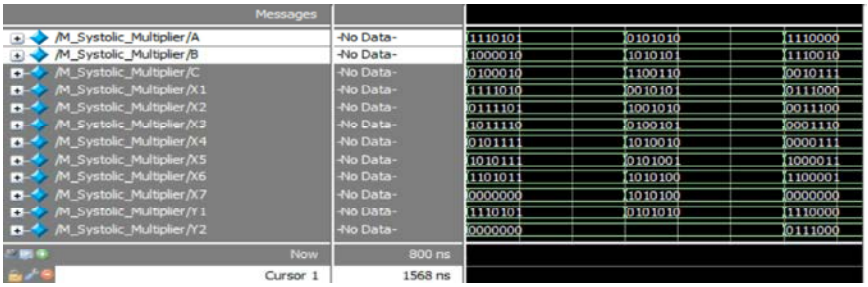

Fig. 15: M=6 systolic structures

In Table No 1,Here mentioned the logic utilization of systolic structure. Basically slices occupied in logic gate very less only because then only reached the area time efficient implementation.The input is number of bonded used Input Output Bank(IOB) for the ports.

In Table No 2,The device ulitization of systolic structure consists of related logic and unrelated logic. In this low latency of systolic array have used additional JTAG gate count for IOBs for reducing the period and latency.In giving the input of look up table for reducing the purpose of slices in fnite field multiplication.

In Table No 3, contains the register sharing technique that is mainly used for reduce the register components in the logic gates. Here the number of slices used for utilization of related logic is 200 i.e., the purpose of reduce the components in the processor, power consumption and get the area time efficiency of finite field implementation.

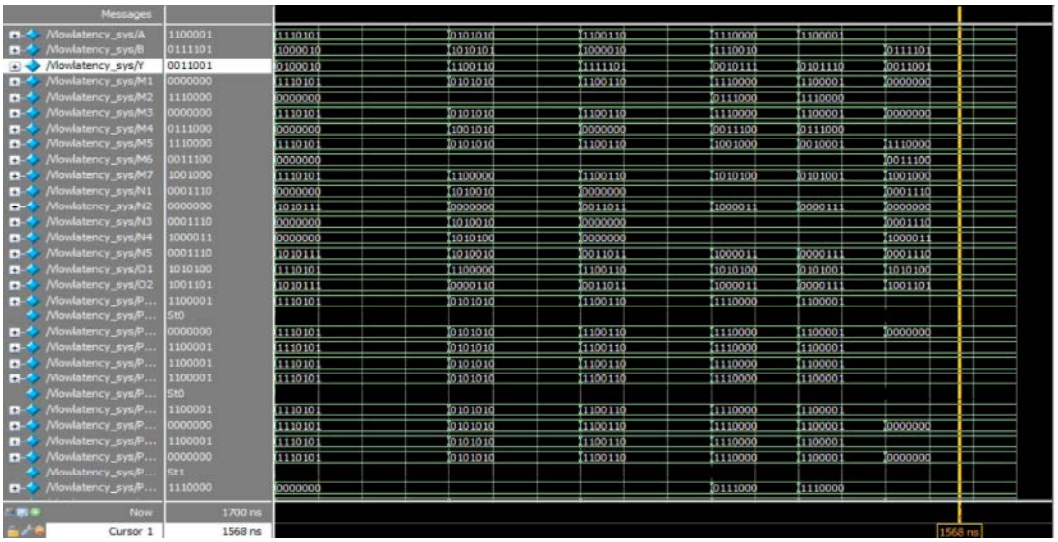

Fig. 16: low latency systolic structure

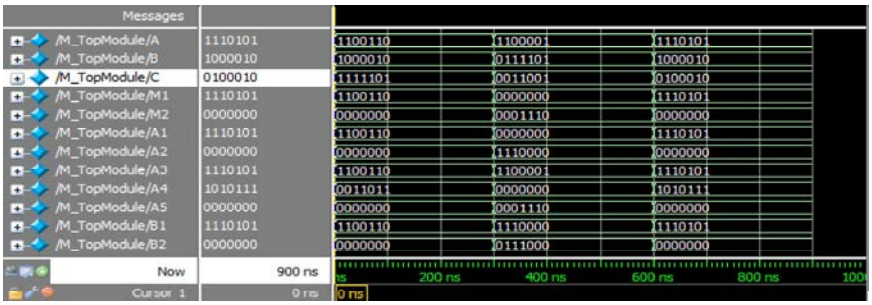

Fig. 17: Register Sharing Multiplier

Table 1: Device Utilization Summary Systolic

Device Utilization Summary				
Logic Utilization	**Used**	**Available**	**Utilization**	**Note(s)**
Number of 4 input LUTs	420	7,168	5%	
Logic Distribution				
Number of occupied Slices	210	3,584	5%	
Number of Slices containing only related logic	210	210	100%	
Number of Slices containing unrelated logic	0	210	0%	
Total Number of 4 input LUTs	420	7,168	5%	
Number of bonded IOBs	63	141	44%	
Total equivalent gate count for design	3,087			
Additional JTAG gate count for IOBs	3,024			

Table 2: Low Latency Systolic Architecture

Device Utilization Summary				
Logic Utilization	**Used**	**Available**	**Utilization**	**Note(s)**
Number of 4 input LUTs	399	7,168	5%	
Logic Distribution				
Number of occupied Slices	200	3,584	5%	
Number of Slices containing only related logic	200	200	100%	
Number of Slices containing unrelated logic	0	200	0%	
Total Number of 4 input LUTs	399	7,168	5%	
Number of bonded IOBs	63	141	44%	
Total equivalent gate count for design	2,835			
Additional JTAG gate count for IOBs	3,024			

Table 3: Register Sharing Low Latency Systolic Architecture

Device Utilization Summary				
Logic Utilization	**Used**	**Available**	**Utilization**	**Note(s)**
Number of 4 input LUTs	399	7,168	5%	
Logic Distribution				
Number of occupied Slices	200	3,584	5%	
Number of Slices containing only related logic	200	200	100%	
Number of Slices containing unrelated logic	0	200	0%	
Total Number of 4 input LUTs	399	7,168	5%	
Number of bonded IOBs	63	141	44%	
Total equivalent gate count for design	2,772			
Additional JTAG gate count for IOBs	3,024			

CONCLUSION

Efficient systolic design for the multiplication over GF (2^m) based on irreducible AOP is proposed.This derived a low-latency bit-parallel 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 lower latency. From ASIC and FPGA synthesis results to find that the proposed design involves significantly less ADP and PDP than the existing designs. Moreover, the proposed design can be extended to further reduce the latency.The usage of Noval Cut-set Retiming reduces the critical path to one XOR gate.thus the complex systolic structure have been spiltted into two or more parallel systolic branches and each one is fed with same input operand and shares same input operand register.thus by using irreducible All One Pollynomialalgorithm,overall circuit complexity is reduced and which can be implemented for cryptography and error control technique.

REFERENCES

1. Berk Suran, 2004. A Generalized Method for constructing subquadratic complexity GF(2^k) Multipliers, IEEE Trans. Computers, 53(9): 1097-1105.
2. Hanho Lee, 2003. High speed VLSI architecture for parallel Reed-Solomon decoder,IEEE Trans. Coputers, 11(2): 288-294.
3. Neethu Johny and Binoy Joseph, 2013. An efficient Systolic multiplier forGF(2m) based on All One Polynomial,journal, Trans. Computers, 1: 2320-2351.
4. Chiou Yng Lee and Che Wun Choiu, 2005. Low complexity bit parallel dual basis multipliers using the modified Booth's algorithm, journal Trans.computers, 31: 444-459
5. Jean Claude, 2010. Subquadratic Space complexity Binary field multiplier using double polynomial representation, IEEE. Trans. Computers, 59(12): 1585-1597.
6. Henriqez, 2003. Parallel Multipliers Based on Special Irreducible pentanomials, IEEE, Trans. Computers, 52(11): 1-7.
7. Yadollah Eslami, 2006. An area efficient Universal cryptography processor for smart cards, IEEE, Trans. Computers, 14(1): 44-51
8. Leong, H.W., 2002. Amicrocoded elliptic curve processor using FPGA technology, IEEE. Trans. Computers, 10(5): 550-559.
9. Cancio Monterio, 2013. Low power bit parallel cellular multiplier implementation in secure dual rail adiabatic logic, IEEE. Trans. Computers, 3(4): 10-19.
10. Bimal Kumar Meher, 2009. A effectiveness of various implementation options of finite field arithmetic on elliptic curve cryptosystem, IEEE. Trans. Computers, 3(4): 1793-8201.
11. Ashutosh Kumar singh, 2009. Error detecting dual basis bit parallel systolic multiplicationar chitectureover GF(2m), Jornals. Trans. Computers, 7(4): 336-342.
12. Kazutoshi Wakabayashi, 2000. C-Based SoC design flow and EDA tools an ASIC andsystemVendor prespctive, IEEE. Trans. Computers, 3(4): 1507-1522.