International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-5, January 2020

Implementation of High Speed Low Power Systolic Multiplier Based on Irreducible Trinomials

G.Erna, S.Tamilselvan

Abstract: ***This paper presents a high speed low power systolic multiplier based on irreducible trinomials which is implemented using GF (2^M). To calculate a set of d partial products in each Handling Element (HE) during every cycle we suggest multiplication algorithm of digit level. By using the systolic channels independently, operands in the proposed structure will be reduced and accumulated by partial products. Functional verification (Simulation) of the multiplier is done by using Xilinx ISE and synthesis is done by using Xilinx XST. The synthesized design is implemented on Zynq7000 FPGA. After completion of the synthesis, it is found that the proposed multiplier achieved power consumption of 2.9mW. Area and the performance of the multiplier is optimized in the proposed structures.***

Index Terms: Digit-level multiplication, Handling Elements, irreducible trinomials, systolic multiplier.

I. INTRODUCTION

The systolic multipliers have played a vital role. To perform the specific operation some arrays are introduced. by using the parallel integration operation multiply and accumulate operations are performed[2][3]. This operation is mainly used to perform the operation in dynamic programming algorithm. By using trinomials the augmentation is written for expansion.

But the systolic multiplier gives efficient output and calculation compared to digit serial multiplier and finite field multiplier [5]. Every one of the HEs are utilized as completely pipelined way in a systolic exhibit to create a high throughput rate. The basic ways of all the current systolic structures in any case, increment with the digit estimate, bringing about an expansion and this will calculate the time based on the measurement done [6]-[9].

The basic structure is implemented by using the extreme values in the clock time frame work. This will expand the digit time based on the measurement. The measurement of digit d is used in the handling elements. Because of this there will be reduction of elements in the structure. Here parallel operation is performed by using handling elements. (*TA* + *TX* + *TR*) is the transmitted propagation delay which is obtained by adding the registers, and gates).

Manuscript received on January 02, 2020.
Revised Manuscript received on January 15, 2020.
Manuscript published on January 30, 2020.
* Correspondence Author
G. Erna*, Research Scholar, Department of ECE, Pondicherry Engineering College, Puducherry, India – 605014.
S.Tamilselvan, Associate Professor, Department of ECE, Pondicherry Engineering College, Puducherry, India – 605014.

By using limited number of operands in handling element the proposed design is implemented. This is designed using systolic channel based on the collection of incomplete items. The proposed digit serial systolic multiplier gives effective results in terms of area and time.

II. DIGIT-SERIAL MULTIPLIERS

Basically, there are two elements in the finite field multiplication they are represented as A and B. the product of A and B is saved in the C block which is known as result block. By using the binary filed, the digit serial multiplier is introduced by processing the coefficients in effective way. The digit size D defines the number of coefficients that are processed in parallel. By using the degree m-1, the total number of digit size is implemented. Hence the multiplier is given as

$$B = \sum_{i=0}^{f-1} B_i \alpha^{Fi}, \text{ where} \sum_{j=0}^{F-1} b_{Fi+j} \alpha^j; 0 \leq i \leq f\text{-}1 \quad (1)$$

Here B is nothing but a zero coefficient which is shown as most significant bit

III.PROPOSED DIGIT-SERIAL SYSTOLIC MULIPLIER

A. Proposed Algorithm

Let $f(g)$ be an irreducible trinomial of degree m over GF(2) given by

$$f(g) = g^m + g^t + 1 \quad (2)$$

where $1 \leq t \leq m-1$. The product Z of elements X and Y in GF(2^m) can be written as

$$Z = X \cdot Y \bmod f(g) \quad (3)$$

Where $X = \sum_{i=0}^{m-1} x_i g^i$, $Y = \sum_{i=0}^{m-1} y_i g^i$ and $Z = \sum_{i=0}^{m-1} c_i g^i$ for x_i, y_i and $z_i \in G$ (2). Equation (3) can be expressed in the expanded form as

$$Z = \sum_{i=0}^{m-1} x_i \left(Y . g^i \bmod f(g) \right) = \sum_{i=0}^{m-1} G_i \quad (4)$$

Where $G_i = x_i \cdot Y^{\{i\}}$ for $Y^{\{0\}} = Y$, and $Y^{\{i\}} = Y \cdot g^i \bmod f(g)$. Let Q, P, k, and d be integers such that $m = QP + r = Qkd + r$, where $0 \leq r < P$ and d is the digit size.

B. Flow graph Design

From figure 1 the algorithm for digit successive duplication is shown based on the outline stream. It include six sorts of center points, i.e., pre-figuring extension center (PCA center point), estimated move I center (S-I center), detached move II center point (S-II center), increase center point (M center point), development center (A center), and conglomeration center point (AC center point).

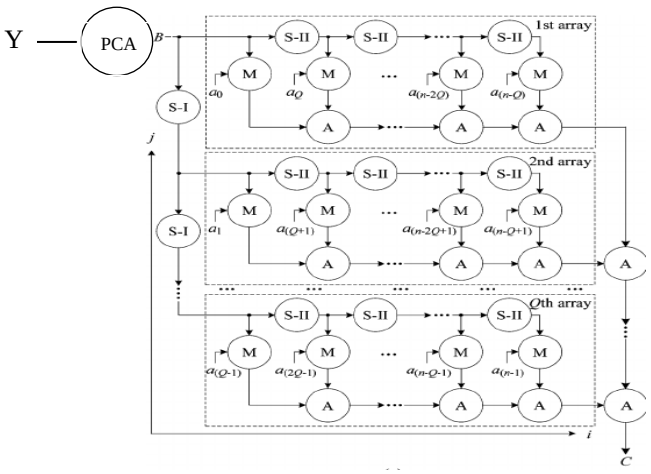

Fig. 1. Flow Graph for multiplication

PCA hub performs expansion activity to infer Y_({E})^({0})from B. for each cycle period, the S-1 hub value is determined to get Y_({E})^({s})(0≤s≤d −1) by using Y_({E})^({s+1}). In the same way S-II hub is determined to get Y_({E})^({(ll+vQ)d})(0≤v ≤k −1) by using Y_({E})^({(l+(v+1)Q)d}). By using the m- bit operands, sequential information is passed through the M hub. This M hub mainly consists of parallel operations. AND task is used to perform the normal operation in M-Hub and XOR operation is used to perform the parallel operation in M-Hub. Hence from figure 2, the block of digit serial systolic multiplier is shown.

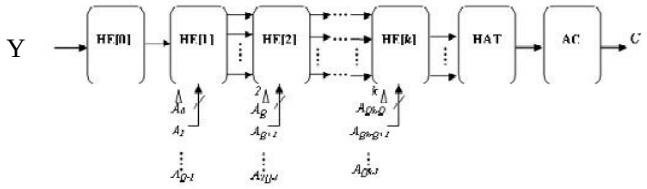

Fig. 2 Structure of Handling elements

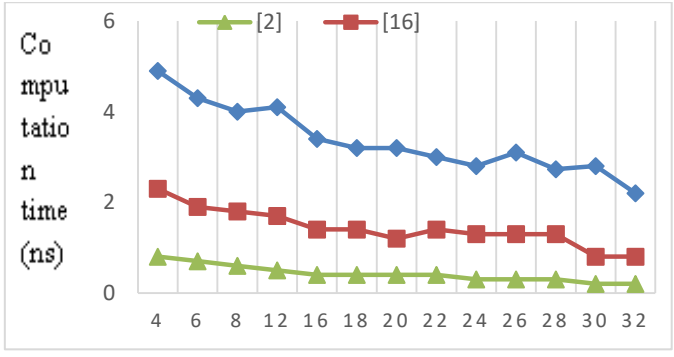

Fig. 3: Comparison of different average computation time

From figure 1 the dull box is recognized based on HE. This figure consists of mainly adder cell and pipelined adder cell. From figure 2 (b)-(h), the cells in the structures are shown separately. By using registers, the pipelined adder cell is fed to the operand B. Y{s+1}{E} is derived by using M-1 cell and after derived {s}{E}(0 ≤s ≤d −1) is obtained. Similarly, B{(l+(v+1)Q)d}{E} is derived to get B {(l+vQ)d}{E}, by using the condition HE[1] to HE[k −1].

Results Analysis – Existing Approach:

	Used	Fixed	Available	Util%
Slice LUTs*	14177	0	53200	26.65
LUT as Logic	14177	0	53200	26.65
LUT as Memory	0	0	17400	0
Slice Registers	24418	0	106400	22.95
Register as Flip Flop	11991	0	106400	11.27
Register as Latch	12427	0	106400	11.68
F7 Muxes	0	0	26600	0
F8 Muxes	0	0	13300	0
Power	3.6 mw			

Result Analysis – Proposed Approach:

Table 1: Comparison Table

	Used	Fixed	Available	Util%
Slice LUTs*	6843	0	53200	12.86
LUT as Logic	6843	0	53200	12.56
LUT as Memory	0	0	17400	0.00
Slice Registers	7763	0	106400	7.30
Register as Flip Flop	3993	0	106400	3.75
Register as Latch	3770	0	406400	3.54
F7 Muxes	0	0	26600	0.00
F8 Muxes	0	0	13300	0.00
Power	2.9 mw			

IV. SUMMARY OF THE MULTIPLIER OPTIONS IMPLEMENTATION RESULTS

Two different architectures are summarized in this section. Table 1 shows the different site types from the FPGA utilized by satisfying the conditions in proposed and existing architectures. The requirement of area is shown from figure 1. Hence the proposed architecture gives small area.

The time required for the existing architecture is high which is shown in figure 3. This graph is drawn between digit size and computations time [12],[13] We have simulated proposed structure and existing structure using Xilinx vivado, I-Sim.

The simulated wave forms of architecture is proposed which is shown in figure 5. We have elaborated the same using Xilinx vivado and the elaborated schematic of the proposed architecture is shown in figure 4. By using Xilinx vivado XST, both proposed and existed structures are implemented and the same is implemented on Zed board (Zync 7000) FPGA. Which is made by 28 nm technology are synthesized.

Fig. 4: Elaborated Schematic

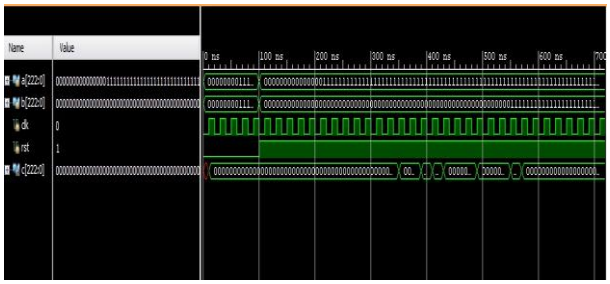

Fig. 5. Simulation results

V. CONCLUSION

The design of high speed low power systolic multiplier Based on Irreducible Trinomials is introduced in this paper. In the proposed system, parallel operation is performed by registering the incomplete items. This system will calculate the speed rate by diminishing the (TNA+ TXN+ TR). From the simulation results, the proposed multiplier produces high speed and low area- time. By using the digit level parallel multiplier, the KA method is stretched. By using the Zyng 7000 FPGA, plan of integration is actualized. The power utilization of proposed multiplier is 2.9Mw.

APPENDIX

By using Xilinx Vivado software the design flow is obtained. By using verilog HDL this software simple digital circuit is created. Bit stream is generated by creating the models, Vivado project, and constant files. By using the Artix-100 based Nexys4 board, the design flow is targeted.

ACKNOWLEDGMENT

I might want to offer exceptional thanks of thanks to my chief just as our head and Doctoral board numbers who gave me the brilliant chance to do this superb Research on the subject which likewise helped me in doing a great deal of Research and I came to thought about such a significant number of new things.

REFERENCES:

1. I. Blake, G. Seroussi, and N. P. Smart, Elliptic Curves in Cryptography. Cambridge, U.K.: Cambridge Univ. Press, 1999, ser. London Mathematical Society Lecture Note Series.
2. N. R. Murthy, and M. N. S. Swamy, “Cryptographic applications of brahmaqupta- bhaskara equation,” IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 53, no. 7, pp. 1565–1571, Jul. 2006.
3. J. Xie, P. K. Meher, and J. He, “Low-complexity multiplier for based onall-one polynomials,” IEEE Trans. VLSI Syst., vol. 21, no. 1, pp. 168–173,Jan. 2013.[4] L. Song and K. K. Parhi, “Low-energy digit-serial/parallel finite field multipliers,” J. VLSI Signal Process. Syst. Signal, Image Video Technol.,vol. 19, no. 2, pp. 149–166, Jul. 1998.
4. P. K. Meher, “On efficient implementation of accumulation in finite fieldover GF(2M) and its applications,” IEEE Trans. VLSI Syst., vol. 17,no. 4, pp. 541–550, Apr. 2009.
5. NIST. Boulder, CO. [Online]. Available: http://www.csrc.nist.gov/publications
6. C.-Y. Lee, J.-S.Horng, I.-C.Jou, and E.-H. Lu, “Low-complexity bit parallel systolic montgomery multipliers for special classes of GF(2m),”IEEE Trans. Compute., vol. 54, no. 9, pp. 1061–1070, Sep. 2005.
7. P. K. Meher, “Systolic and super-systolic multipliers for finite field GF(2M) based on irreducible trinomials,” IEEE Trans. Circuits Syst. I,Reg. Papers, vol. 55, no. 4, pp. 1031–1040, May, 2008.
8. S. Kumar, T. Wollinger, and C. Paar, “Optimum digit serial GF(2m) multipliers for curve-based cryptography,” IEEE Trans. Circuits Syst. I,Reg. Papers, vol. 55, no. 10, pp. 1306–1311, Oct. 2006.
9. S. Talapatra, H. Rahaman, and S. K. Saha, “Unified digit serial systolic montgomery multiplication architecture for special classes of polynomials over GF(2M),” in Proc. Euromicro Conf. Digital Syst. Des., Archit.,Meth.
10. Tools, 2010, pp. 427–432.
11. C. H. Kim, C. P. Hong, and S. Kwon, “A digit-serial multiplier for finite field GF(2m),” IEEE Trans. VLSI Syst., vol. 13, no. 4, pp. 476–483,Apr. 2005.
12. J-S. Pan, C-Y .Lee, and P. K. Meher, Low-latency digit-serial and digit parallel systolic multipliers for large binary extension fields,” IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 60, no. 12, pp. 3195–3204, Dec. 2013.
13. A. Hariri and A. R.Masoleh, “Bit-serial and bit-parallel Montgomery multiplication and squaring over GF(2m),” IEEE Trans. Comput., vol. 58,no. 10, pp. 1332–1345, Oct. 2009.
14. J. Imana and J. Sanchez, “Bit parallel finite field multipliers for irreducible trinomials,” IEEE Trans. Comput., vol. 55, no. 5, pp. 520–533,May 2006.
15. K. K. Parhi, VLSI Digital Signal Processing Systems: Design and Implementation. New York, NY, USA, Wiley, 1999.
16. A. Karatsuba and Y. Of man, “Multiplication of multi digit numbers on automata,” Soviet Phys.-Doklady (English Translation), vol. 7, no. 7,pp. 595–596, Jul. 1963.
17. P. L. Montgomery, “Five, six, and seven-term Karatsuba-like formulae, ”IEEE Trans. Comput., vol. 54, no. 3, pp. 362–369, Mar. 2005.
18. Nan Gate Standard Cell Library.[Online]. Available: http://www.si2.org/openeda.si2.org/projects/nangatelib/

AUTHORS PROFILE

G.Erna, M.Tech, MISTE, Reaserch scholar, Dept. of ECE, Pondicherry Engineering College, Puducherry-605014. Publishedd Austrialian journal (Scopus) and Academic science,Various UGC Journals and Attended International Conference in India.Research work on VLSI and System design.In 2011 Faculty Eligible Test Qulified by JNTU - Hyderabad

Dr. S. TAMILSELVAN B.E., M.Tech. Ph.D MISTE, ASSOCIATE PROFESSOR/ECE, Pondicherry Engineering College, Puducherry-605014. He has Published various SCI and Scopus journals. Attendded more than five IEEE Conferences in various parts of India. His Research areas are Wireless Communication, VLSI Design and Solid Stae Devices. He is presently guiding 7 Research Scholars.