CREATE A CUSTOMIZABLE, HIGH-SPEED GALOIS FIELD ALGORITHM WITH EFFECTIVE USE OF MOSFETS

[1]Neelima Gottimukkala, [2]Dr.V.Gajendra Kumar, [3] Vemuluri Madhuri, [4]Chakarajamula Naga Malleswarao

[1,3]Assistant Professor, [2]Professor, [4]Student, Dept. of Electronics & Communication Engineering, Newton's Institute of Engineering, Macherla, Andhra Pradesh, India.

ABSTRACT

This study presents the design and implementation of reconfigurable high-speed galois field arithmetic procedures with effective MOSFETS use. The fundamental arithmetic circuits in many of these applications, including digital signal processing, are adders and multipliers (DSP). The adder used by this galois field arithmetic operator restricts the carry propagation. To propagate and create signals, partial products are employed. Sequential logic is used by the galois field arithmetic operator to speed up computation. Outcomes show that the suggested approach produces good results and is put into place utilizing modern techniques.

Key Words: VLSI, Digital signal processing (DSP), Adder, Multiplier, Galois Field Arithmetic Operations.

INTRODUCTION

Basically, finite fields are most frequently utilized in communication systems like error-correcting codes and encryption. The field elements are used for arithmetic operations. Normal basis and polynomial basis are the two basic types typically utilized to design a system. The hardware is implemented on a regular basis, and low cost squaring procedures are carried out. The programmed is implemented using polynomial basis, and in a similar manner, this also executes the low cost squaring operations [1]. In the majority of modern applications, such as image processing and identification, accuracy may be compromised to a certain amount. The fundamental building component of these applications, which entail a lot of mathematical computation, is the multiplier. This leads to a win-win balancing between the energy consumed by the circuit and the required accuracy.

The energy consumed by any system is directly proportional to the multiplication accuracy of those systems. If a system requires high accuracy then it consumes more energy and vice versa. Also, there could be section or module of those systems which needs lesser accuracy than other parts of the system. If the accuracy is kept constant across all such modules it greatly increases the amount of energy consumed by the overall system. However, if the accuracy of the multiplier is characterized to change as per the need of that particular module or section of the entire system, this would have a great impact in reducing the amount of energy consumed by the system [2].

This method of configuring and adjusting the accuracy of a multiplier based on the requirement of the system or application is achieved using different adder sub module of the multiplier module to characterize the accuracy based on the approximation technique. There should be reconfigurable multipliers in various program stages or applications [3]. So, in this paper we designed a multiplier which has an accuracy decided on the go based on the requirement of the application.

Montgomery's multiplier is classified into three types, they are bit-serial, bit-parallel, and digit serial architectures. Bit-parallel shape is rapid; however it's far steeply- priced in phrases of vicinity. Bit-serial structure is region efficient, but it's far too sluggish for plenty packages. The digit- serial structure is flexible which may change the space and velocity, consequently, it achieves a moderate pace, reasonable price of implementation and hence it is most appropriate for practical use. Montgomery presented a technique for figuring modular multiplication productively. He introduced to move the portrayal of numbers from the Zn to an alternate area, called Montgomery Residual portrayal or Montgomery Domain [2-3].

Here for the purpose of security, the computers and communication system brought with a demand from private sector [4]. The Montgomery multiplication is the calculation that permits effectively for registering. The expense of the particular duplication is equivalent to three whole numbers which increases in addition to the

expense of the change in the Montgomery area. Yet, in the event that the large scale task is an exponentiation, at point the changecost is insignificant contrasted with the quantity of augmentations executed in the Montgomery area. In the process of Montgomery multiplication, pre-processingunit and post-processing units are used [5]. The pre-processing unit produces N-Residueoperands and in the same way post processing unit will eliminate the constant factor 2n. Hence to form N-Residue operands in the system, modularexponentiation is used.
Here for the purpose of supplanting division activities, shifting tasks are used. After the shifting process the least critical bits willremain zero. Now to eliminate these bits in the modular multiplication, add products are used. After the process of eliminating thebits, the remaining bits are augmented in the multiplicand. Hence from this it can observe that the process of multiplicand is completed. Now the output is obtained after the subtraction of bits. Here if the bits are increased then Montgomery bits also increases. At last the multiplicand bits are controlled without the use of subtraction calculation.

LITERATURE SURVEY

"An Area and Delay Efficient Logarithmic Multiplier" Multiplication is an ubiquitous operation in growing set of media processing applications (graphics, audio, video, and image). Many of these applications, however, possess an inherent quality of error resilience. Thus the multipliers, that are not very precise but return an approximate value, can be utilized in such applications.
"A review paper on different multipliers based on their different performance parameters".
A processor consumes most of the hardware resources for multiplication process as compared to the other arithmetic operations such as addition and subtraction. Some of the most common parameters like speed, area, power consumption are controlled by topologies like array multiplier, modified booth multiplier, Wallace tree multiplier and modified Wallace tree multiplier.
Comparison of Braun Multiplier andWallace Multiplier Techniques in VLSI",
In this the concept that is used ispower efficient multipliers which are very important part of all VLSI system designwhich provides High speed with low power consumption which are the key requirementsfor any VLSI design. This proposes an efficient implementation of a high speed with low power multiplier using shift and adds methods and this presents the implementation of Braun multiplier andWallace Multiplier using Cadence (Encounter) RTL Complier with simulation which includes creating the Test circuit for each block that is combined together which forms Multiplier.
"A VLSI Architecture for Signed Multipliers",
Multipliers are basically the heart of ALU for any processor. The performance of the DSP processors depends on the computation time of the multipliers. For hardware implementation of DSP basedapplications, we need proper optimization ofadder and multiplier architecture. Also most of the signal processing applications deals with negative data to be processed for accurate result.

PROPOSED SYSTEM

The below figure (1) shows the schematic design of proposed system. While designing this circuit 142 MOSFET's are utilized. 81 total nodes, 71 independent nodes and 10boundary nodes are utilized.

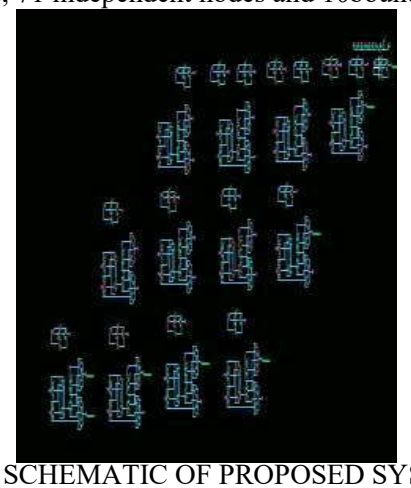

Fig. 1: SCHEMATIC OF PROPOSED SYSTEM

Here firstly, the operands are loaded in the multiplier. The arithmetic operations like addition and multiplication operations are performed. The obtained result of this will be saved in the barrel shifter. Here irreducible polynomial function is not used in the system. The main intent of register multiplier is to store the bit representation and give polynomial output a(t). Here parallel load operation is performed in the most significant bit position. In the same way left shift operations are performed in MSB bit. The multiplicand bit is used b(t) value to store the value in register. The parallel load operation is also applied in the multiplicand. The obtained value is stored in the register. The right shift operation is performed in the multiplicand register block. Crypto core processor is used to transfer the data in multiplicand register.

The barrel shifter consists of root and load mr and this are taken as input to this block. The multiplier register is generally attached to the finite field arithmetic circuit. In the same way, multiplicand register consists of shift, data_in and load_md bits which are taken as input to the barrel shifter. It will shift the data and as well as load the data in effective way. Result register consists of output and saves the entire arithmetic result. Compared to existed system, the proposed system gives effective results.

The result multiplier and multiplicand is saved in the result barrel shifter block. The both a(t) and b(t) values are assigned in the barrel shifter blocks. The obtained values in the barrel shifter block will shift the bits to adder block. This block will perform the addition operation. After performing particular operation, the bits are shifted to the result register. This result register will save the output as product. At last the barrel shifter will perform the parallel operation in effective way.

Partial-Product Multiplication is an alternative method for solving multi-digit multiplication problems. This is a strategy that is based on the distributive (grouping) property of multiplication. The first partial product is created by the LSB of the multiplier, the second partial product is created by the second bit in the multiplier, etc. The final partial products are added with a accurate adder circuit.

SIMULATION RESULTS

The below figure (2) shows the synthesis report of proposed system. In this synthesis report there are utilization of number of MOSFET's, Independent nodes, boundary nodes and total nodes. 81 total nodes are totally utilized in this proposed system while designing, 10 boundary nodes and 71 independent nodes are utilized while designing.

Fig. 2: SYNTHESIS REPORT

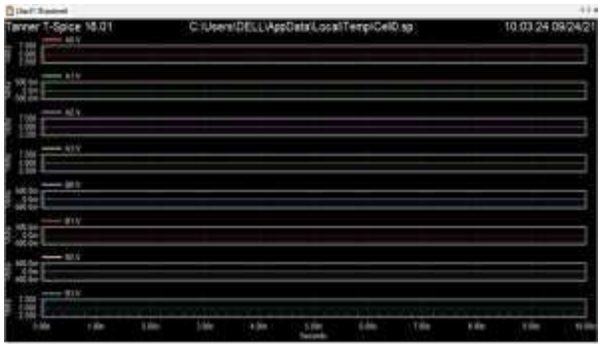

Fig. 3: INPUT WAVEFORM

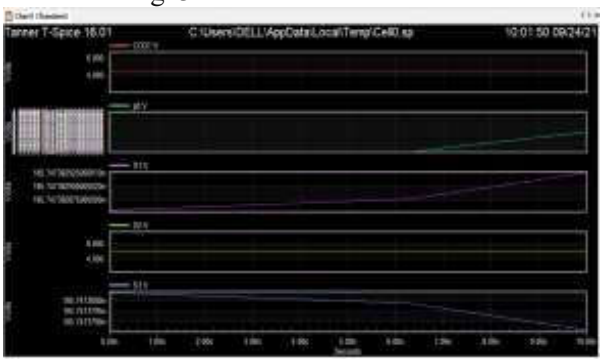

Fig. 4: OUTPUT WAVEFORM

The above figure (4) shows the output waveform of proposed system. In this the overhead delay is reduced up to 0.75 seconds. Set up delay is reduced up to 0.03 seconds and parsing delay is reduced up to 0.10 seconds

CONCLUSION

As a result, in this paper's architecture, high-speed galois field arithmetic was accomplished with effective MOSFETS use. The multiplication is completed quickly by the multiplier. The system that is being presented will lessen the switching activity that the system generates. A partial product unit is introduced to lessen the delay. This system is mostly employed in low-delay and high-speed applications.

REFERENCES

1. Xue Wang, Huiqing Wen, Yinxiao Zhu, "Modeling and Simulation Test for Voltage Multiplier and an LLC Resonant Inverter asa Voltage Equalizer", Downloaded on May 27, 2019 at 06:56:07 UTC from IEEE Xplore.
2. Gunjan Jain, Meenal Jain, Gaurav Gupta,"Design of Radix-4,16,32 Approx Booth Multiplier Using Error TolerantApplication", 978-1-5090-3012-5/17/$31.00 ©2017 IEEE.
3. "Design of area efficient and low power multipliers using multiplexer basedfull adder" S. Murugeswari , S. Kaja Mohideen, Second International Conference on Current Trends In Engineering and Technology - ICCTET 2014.
4. H. Wu, "Bit-parallel finite field multiplier and squarer using polynomial basis," IEEE Trans. Comput., vol. 51, no. 7, pp. 750–758, Jul. 2012.
5. H. Hinkelmann, P. Zipf, J. Li, G. Liu, and M. Glesner, "On the design of reconfigurable multipliers for integer and Galois field multiplication,"Microprocessors Microsyst., vol. 33, no. 1, pp. 2–12, Feb. 2009.
6. "Power-delay-area efficient design of vedic multiplier using adaptable manchester carry chain adder", Raghava Katreepalli , Themistoklis Haniotakis, 2007 International Conference on Communication and Signal Processing (ICCSP).
7. P. K. Meher, "High-throughput hardware-efficient digit-serial architecture for field multiplication over GF(2m),," in Proc. 6th Int. Conf. Inf., Commun. Signal Process. (ICICS), Dec. 2007, pp. 1–5.
8. "Design of area and delay efficient Vedic multiplier using Carry Select Adder", G. R. Gokhale , S. R.

Gokhale, 2005 International Conference on Information Processing (ICIP).

9. "Comparative study of performancevedic multiplier on the basisof adders used", Josmin Thomas , R. Pushpangadan , S Jinesh, 2005 IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE).
10. "Design of high speed multiplier using modified booth algorithm with hybrid carry look-ahead adder" R Balakumaran , E Prabhu, 2004 International Conference onCircuit, Power and Computing Technologies (ICCPCT).
11. "A vertical-MOSFET-based digitalcore circuit for high-speed low-power vectormatching", Yitao Ma , TetsuoEndoh , Tadashi Shibata, 2001 International SoC Design Conference.
12. "Design of ultra low power multipliers using hybrid adders", Thottempudi Pardhu , N.Alekhya Reddy, 2001 International Conference onCommunications and Signal Processing (ICCSP).