Design of High Speed and Area Efficient Finite Field Multiplier Using Factoring Technique for Communication

Shaik Baba Fariddin and Dr. Rahul Mishra
Department of Electronics & Communication Engineering, Dr. A.P.J. Abdul Kalam University, Indore (M.P.) - 452010, India
Corresponding Author Email : sbabafariddin@gmail.com

Article Info
Page Number: 803-811
Publication Issue:
Vol. 70 No. 2 (2021)

Article History
Article Received:
05 September 2021
Revised: 09 October 2021
Accepted: 22 November 2021
Publication: 26 December 2021

Abstract
In this paper, design of high speed and area efficient finite field multiplier using factoring technique for communication is implemented. Data security plays very important role in present generation. Therefore, initially inputs and key are given to S-Box. The main intent of S-Box is to substitute the input data and key. After that input data and key are merged using S-Box merge. This data will be multiplied using finite field multiplier and to improve the performance along with that mix column technique is applied. Factoring technique will increase the speed of operation. After the data performs shift row operation. At last rounding is performed to the obtained data. At last simulation results shows that effective outcome in terms of delay, memory and security.

Keywords— S-Box, Rounding, Factoring Shift Row Operation, Data security, Finite Field Multiplier, Factoring technique, S-Box.

1. Introduction

Arithmetic operations are performed on binary format numbers by digital computers and calculators. The Arithmetic logic unit of a computer performs these operations. In this procedure flip-flops are merged together with logic gates in aarithmetic logic unit in order to perform addition, subtraction, multiplication and division on any numberusing circuits swiftly that are not possible manually [1]. Now we elucidate the circuit performing addition operations which is a major arithmetic operation in computerized system.

Till now most of the circuits used are just capable of executing only multiplications for single digit binary number position. Although this has just a single number that is required to be operated [2]. Logiccircuits basically use two basic methods to perform multiplication of multi-digit numbers. One of these methods is Serial system, and another one is Parallel system.

One bit is executed at once in a constant sequence of time for the serial addition,only a single full adder circuit is utilized [3]. The leastsignificant bit (LSB) is the first series to perform addition that developed the Most Significant Bit (MSB),these values are recorded in registers. A particular amount of data is stored in register which is a short time memory device.

In order to reduce power, many researchers, designers and engineers have come up with many innovative techniques and have patented their ideas. Nevertheless, designers will need

to budget and plan for power dissipation as a factor nearly as important as performance and perhaps more important than area. Low power techniques have been successfully adopted and implemented in designing complex VLSI circuits [4]. As the demand for faster, low cost and reliable products that operate on remote power source performing high end applications keep increasing, there is always a need for new low power design techniques for VLSI.

In various applications like digital signal processing, multiplier plays very important role in present generation. Multipliers are designed using advanced technology by following the targets of high speed, low power, and low area consumptions. Generally, add and shift algorithm is utilized to perform multiplication method. The main parameters used in the operation of parallel multiplier are add and shift method [5]. By using this parameter multiplier performance is determined.

Digital Signal Processing (DSP) applications like fast Fourier transform and filtering will perform arithmetic operations and in that multiplication plays very important role. Earlier parallel multiplier is introduced to perform the high speed operation. But parallel multipliers consume more areas hence in this paper finite tiled multiplier using factoring technique for communication is implemented. This will improve the security and speed of operation. Therefore researchers will concentrate on the efficiency of multiplier operations for designing.

2. Multipliers Strategy

The below shows the different operations of multipliers which are used in DSP applications to improve the speed:

A. Mod m Reducer: Let us consider the combinational mod m for the fixed values of m. mod m multiplier is utilized for value of m as m = 2192 - 264 – 1. Because of this the power will be reduced.

B. Parallel Multiplication Methods:

Partial products are generated using parallel multiplication method. This will perform the entire operation in very effective way. Respectively by using the Full Adder (FA), AND Gate and Half Adder (HA).

Carry Propagate Array Multiplier (CPAM): For the unsigned operand multiplier carry propagate array multiplier is utilized. Because of this the addition operation is performed with carry propagate adders. Partial products are derived by using AND gates in CPAM. Hence in partial products full adders and half adders are utilized for performing addition operation. The below figure (1) shows the architecture of CPAM.

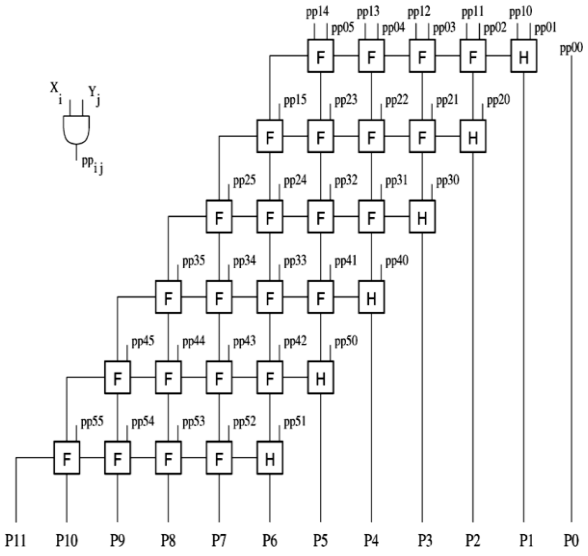

Fig. 1: Carry Propagate Array Multiplier

Carry Save Array Multiplier (CSAM): The below figure (2) shows the structure of CSAM. There are 2 AND gates which are taken as inputs. Carry save adder is utilized to add the products in array. Final product is obtained by adding ripple carry adder. Multiplication is accelerated by performing the operation of carry save adder.

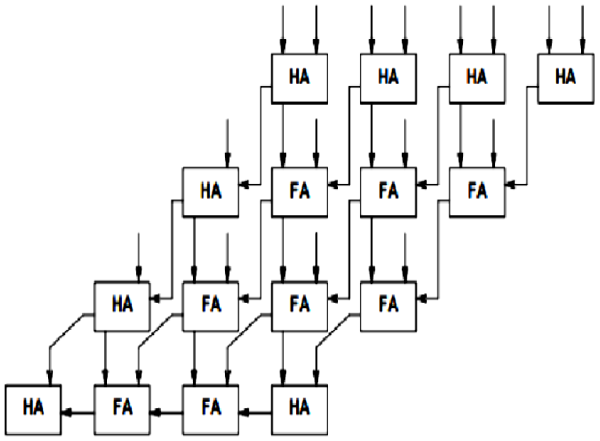

Fig. 2: Carry Save Array Multiplier

Tri-Section Pezaris Array Multiplier (TPAM): This is also called as direct two's complement array multiplication method. In this Tri-Section Pezaris Multiplier is most widely utilized. In the circuits of implementations various types of full adders are utilized. Delay of multiplication process is reduced without the use of complementing stages. Basically it is only used for signed number multiplication process.

Baugh-Wooley Array Multiplier (BWAM):

This multiplier is also equal to theTri-Section Pezar is multiplier. Operands which are used as small number of bits to operate in these applications. This is the most straightforward structure which will perform the two's complement multiplication without the use of parallel

multipliers. Positive values are obtained for performing the addition operation by using all signs. This will allow the structure to implement the addition operation in hardware.

Modified Booth Multiplier (MBM): The delay in addition of partial products like in array multiplier are reduced by some multiplication techniques based on shift and add techniques. The multiplier bit decides whether to shift the partial product or add the multiplicand to the product. Here this will explains how conventional addition is performed. In order to fasten the multiplication procedure custom multiplication process divided into two sections. The first section focuses on producing partial products and the second section focuses on accumulation and addition of the partial products. Before adding of PPs they need to be aligned in their corresponding positions by shifting.

Montgomery Multiplier (MM) multiplication of signed numbers must be observed through the operation to produce the appropriate sign of the result. Whereas in case of unsigned numbers there is no need to think about sign of the operands. If the multiplication of signed 2's complement numbers is performed in the way of positive number multiplication would results in incorrect output. Therefore, booth's algorithm introduced a technique to perform multiplication of signed numbers with the sign protection. In this technique the LSB bits of the multiplier is bi and bi-1 which are tested at every clock cycle. If the two bits are zeros results shifting one bit position of the multiplier to the right. In case of sequence of 1's arithmetic operations like addition and subtraction are need to be performed at the edges of block of ones while changing from 1 to 0 and 0 to 1.

Usually in a multiplication procedure the number of times multiplicand is added to the multiplier relies on the number of 1's in the multiplier. The number of 1's in multiplier decides the speed of operation. To increase the speed the 1's in multiplier are reduced using higher radix representation. The transformation of radix 2 numbers to higher radix significantly compresses the number of 1's in the multiplier. The radix-4 reduces K-bit binary number to K/2 bits in the same way radix-8 changes K-bit binary to K/3 bits. In higher radix notation each bit in multiplier represents two or more bits. This technique gives the ability to add and subtract the multiples in several ways. MBE uses 2's complement of signed numbers while performing multiplication

3. Literature Survey

Tao Luo et al., present an memory Booth multiplier based on racetrack memory to alleviate this problem.Booth's algorithm performs addition if last bits of multiplier encounters '0 1' and subtraction of multiplicand is needed if the LSB bits encounter '1 0'. This method efficiently works for signed numbers also. When multiplier consists of long blocks 1's this algorithm works well and effectively reduces number of additions performed. In b, a, m represents multiplier, multiplicand and product respectively.

Honglan Jiang et al. The Booth multiplier has been widely used for high performance signed multiplication by encoding and thereby reducing the number ofpartial products.The first thing is the left most bit of operands is always a sign bit. This must preserve the sign till the end of the operation. Second thing is to choose which multiplier is and which is multiplicand. If one

of the operands is negative then take its 2'complement as multiplier. In case of two operands are negative then take 2'complement of both numbers and one is chosen as multiplier. Now begin multiplication process by adding n-zeros at the MSB of multiplier making it equal to 2n bits. Then initiate verification of LSB bits of multiplier. In case first step consider extra zero at LSB to test bi and bi-1 positions. These two bit combinations produce four codes each for particular function.

Jiun-Ping Wang et al presents the design of high-accuracy fixed-width modified Booth multipliers.Select an operand between two operands which is having leastdifference amid successive blocks of same numbers. This selected one acts as a multiplier. The LSB and previous LSB bits of multiplier are tested to perform specific operation like shifting, adding or subtracting the multiplicand. If X is a multiplier then the bits xi xi-1 determines the operation to be performed.

RazaidiHussin et al, present the design of an efficient multiplication unit. Assume two operands 2 and -4. The binary representations of operands are 0010 and 1100 (-4 in 2's complement). Between these two operands select a specific operand which is having least difference during successive blocks of same numbers. 0010 has two transitions from 0 to 1 and 1 to 0. But, the -4 has one transition from 1 to 0. So, -4 is taken as multiplier.

Consider the value of X with assigned zeros 0000 1100.

4. Finite Field Multiplier Using Factoring Technique

The below figure (3) shows the block diagram of finite field multiplier using factoring technique.Initially inputs and key are given to S-Box. The main intent of S-Box is to substitute the input data and key. After that input data and key are merged using S-Box merge. This data will be multiplied using finite field multiplier and to improve the performance along with that mix column technique is applied. Factoring technique will increase the speed of operation. After the data performs factoring shift row operation is performed. At last rounding is performed to the obtained data.

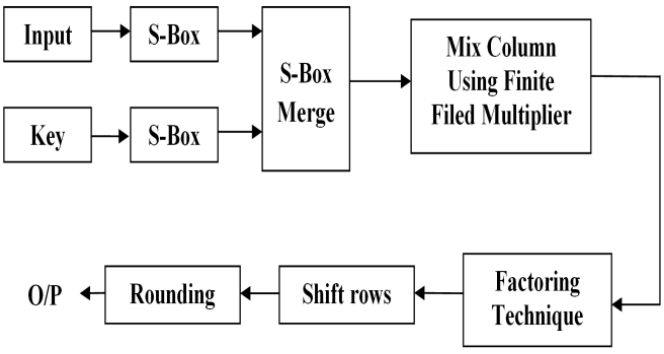

Fig. 3: Block Diagram Of Finite Field Multiplier Using Factoring Technique

Multiplication is one of the most critical arithmetic operations of the digital signal processor. Not only difficult but also consumes huge part of processors area and power. Therefore finite field multiplier is used to decrease the power and area consumption in highly essential processing units. Usually the result of multiplication of two operands of size n-bits requires

2n-bits for their result. In binary number representation MSB (Most Significant Bit) bits contains product value the lower order contains small values.

Some multipliers are developed with fixed size calculates only bits of the multiplication function. Multiplier circuits are model after the “shift and add” algorithm. In this algorithm, one partial product is created for each bit in the multiplier. Each input, partial product digit and result have been given a logical name and these same names are used as signal names in the circuit schematics. By comparing with various circuits, schematics, the behavior of the multiply circuit can be confirmed.

S-box (substitution-box) is a basic component of symmetric key algorithms which performs substitution. In block ciphers, they are typically used to obscure the relationship between the key and the cipher text, thus ensuring Shannon's property of confusion.

Shift rows is the function shifts the bytes in each row of a matrix by a certain offset, determined by the encryption algorithm. Each byte in the second row is shifted one position to the left. Bytes in the third and fourth rows are shifted by offsets of two and three, respectively

Mix column transformation is a word substitution yet it makes utilization of math of GF (2^8). Every segment is worked on separately. Every byte of a segment is charted into another esteem that is a capacity of each of the 4 bytes in the section. This step replaces every byte of a column i.e. one word by a function of all the bytes in the same column.Rounding is a fundamental method to reduce the size of a word, such as arithmetic operations.

The table (1) shows the comparison of parameters of total delay, logic delay, route delay, memory used and accuracy for finite field multiplier and finite field multiplier using factoring technique for communication.

Table. 1: COMPARISON OF PARAMETERS

S.No	Parameter	FFM	FFM - FT
1	Total delay	High	Low
2	Logic delay	High	Low
3	Route delay	High	Low
4	Memory used	High	Low
5	Accuracy	Low	High
6	Security	Low	High

The below figure (4) shows the comparison of total delay, logic delay and route delay for finite field multiplier and finite field multiplier using factoring technique for communication. Compared with finite field multiplier, finite field multiplier using factoring technique for communication reduces the delay in very effective way.

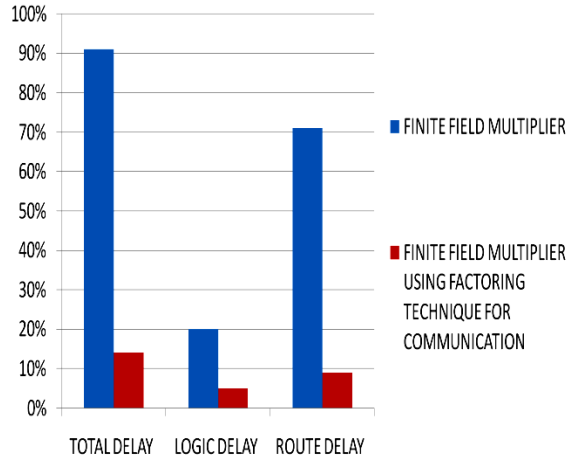

Fig. 4: comparison of total delay, logic delay and route delay

The below figure (5) shows the comparison of accuracy for finite field multiplier and finite field multiplier using factoring technique for communication. Compared with finite field multiplier, finite field multiplier using factoring technique for communication increases the accuracy in very effective way.

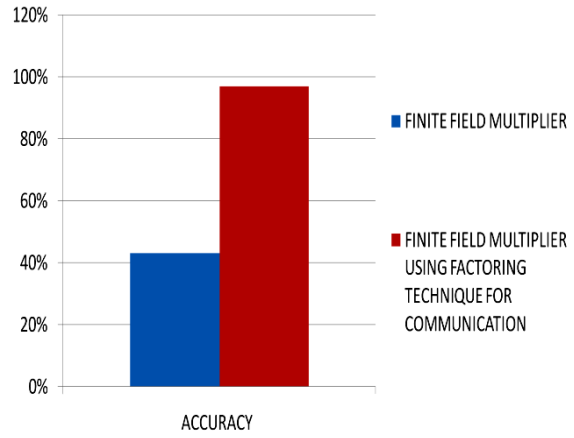

Fig. 5: comparison of accuracy

The below figure (6) shows the comparison of memory used for finite field multiplier and finite field multiplier using factoring technique for communication. Compared with finite field multiplier, finite field multiplier using factoring technique for communication reduces the memory used in very effective way.

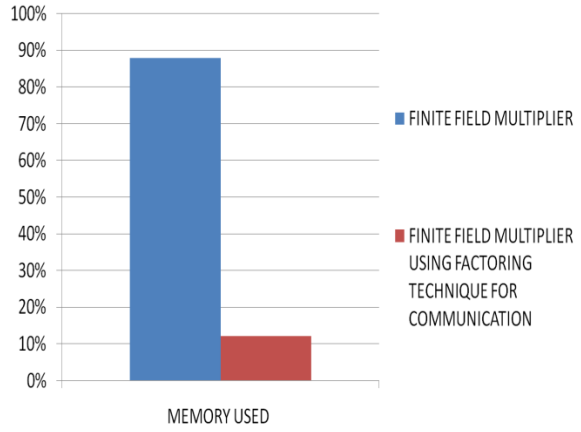

Fig. 6: comparison of memory used

The below figure (7) shows the comparison of security for finite field multiplier and finite field multiplier using factoring technique for communication. Compared with finite field multiplier, finite field multiplier using factoring technique for communication improves the security in very effective way.

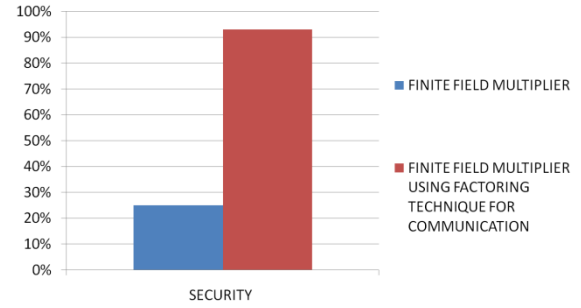

Fig. 7: comparison of security

5. Conclusion

Hence in this paper design of high speed and area efficient finite field multiplier using factoring technique for communication was implemented. In present generation plays very important role in data security applications. S-Box will perform the substitute of data using inputs and key. Factoring technique will increase the speed of operation. After that the data performs shift row operation. Simulation results shows that effective output is obtained in terms of delay, area and security.

References

1. Arvind Nigam, Raghvendra Singh “Comparative Analysis of 28T Full adder with 14T Full adder using 180nm”, Intl J Engg SciAdv Research 2(1):27-32 2016 March

2. Anil Kumar, Kuldeep Singh “A Low-Power 12 Transistor Full adder Design using 3 Transistor XOR Gates”, International Journal of Electronics, Electrical and Computational System, Volume 4, Special Issue September 2015

3. Dayadi Lakshmaiah, Dr. M. V. Subramanyam & Dr. K. Satya Prasad "Design of Low Power 4-Bit CMOS Braun Multiplier based on Threshold Voltage Techniques", Global Journal of Researches in Engineering: Electrical and Electronics Engineering, volume 14, issue 9, version 1.0 Year 2014

4. Ms. Madhu Thakur ,Prof. Javed Ashraf "Design of Braun Multiplier with Kogge Stone Adder & It's Implementation on FPGA", International Journal of Scientific & Engineering Research, Volume 3, Issue 10, October-2012.

5. G.J.V.S.N. Lakshmi Devi and M. Ramesh Kumar – "Design and Implementation of Energy Efficient, Reconfigurable Fir filter using Modified Booth and C.S.A.", Journal of Electrical and Electronics Engineering (JEEE), ISSN: 2250-2424, Vol. 2, Issue 1, Sept 2012 11- 18.

6. B. Ramkumar and Harish M Kittur, " Low-Power and Area Efficient Carry Select Adder", IEEE transactions on very large scale integration (vlsi) systems, vol. 20, no. 2, february 2012

7. Manoj Kumar, Sandeep K. Arya, SujataPandey, "low power cmos Full adder design with 12 transistors", International Journal of Information Technology Convergence and Services (IJITCS) Vol.2, No.6, December 2012.

8. J. Lin, Y. Hwang, M. shew, "Low power 10-T Full adder design based on degenerate pass transistor logic", ISCAS, IEEE, 2012.

9. Sreenivasa Rao. Ijjada , Ayyanna.G , G. Sekhar Reddy , Dr. V. Malleswara Rao, "Performance of different cmos logic styles for low power and high speed", International Journal of VLSI design & Communication Systems (VLSICS) Vol.2, No.2, June 2011.

10. Kumar, R., Singh, J.P., Srivastava, G. (2014). Altered Fingerprint Identification and Classification Using SP Detection and Fuzzy Classification. In: , et al. Proceedings of the Second International Conference on Soft Computing for Problem Solving (SocProS 2012), December 28-30, 2012. Advances in Intelligent Systems and Computing, vol 236. Springer, New Delhi. https://doi.org/10.1007/978-81-322-1602-5_139

11. S. Menon and C. H. Chang, "A reconfigurable multi-modulus modulo multiplier," in Proc. IEEE Asia-Pacific Conf. Circuits Syst., Singapore, Dec. 2006, pp. 1168–1171.

12. Dhireesha Kudithipudi and Eugene John, "Implementation of Low Power Digital Multipliers Using 10 Transistor Adder Blocks", Journal of Low Power Electronics Vol.1, 1–11, 2005

13. C. H. Chang, S. Menon, B. Cao, and T. Srikanthan, "A configurable dual-moduli multi-operand modulo adder," in Proc. IEEE Int. Symp. Circuits Syst., Kobe, Japan, May 2005, vol. 2, pp. 1630–1633.