IMPLEMENTATION OF VARIBLE WIDTH MONTGOMERY MODULAR MULTIPLICATION FOR FPGAS

SHAIK.APSAR[1], I.V.PRAKASH[2]

1 P.G Student, Department of Electronics and Communication Engineering

2 Associate Professor, Department of Electronics and Communication Engineering, Siddhartha Institute of Technology and Sciences.

(E-mail: apsarappu143@gmail.com)

Abstract— This paper proposes an efficient Montgomery multiplication where a new multiplier is designed. The proposed multiplier accepts and outputs the data with binary representation and uses only one-level configurable carry-save adder (CCSA). Which could be used as full adder or serial half adder this reduces the extra clock cycles for operand pre-computation and format conversion by half? We also use a mechanism that can detect and skip the unnecessary carry save addition operations. But the area complexity and critical path delay are high. So a new multiplier is designed by Implementing modified carry save adder (MCSA) where the carry can be predicted at initial stage and only sum is computed in the full adder stage. This is the modified version of existing CCSA. This result in reduction of time required for computation resulting in higher throughput.

Keywords—CCSA, MCSA, Cryptography, Modular Multiplication.

I. INTRODUCTION

Cryptography is a technique for putting away and transmitting information in a specific frame, with the goal that those whom it is planned just can read and process the information. Cryptography is exceptionally fundamental for security reason in information transmission. For its equipment execution Montgomery measured Multiplication calculations is utilized. For the most part in Public Key Cryptography this rationale is utilized as a part of information encryption process. Montgomery calculation can be ordered into two sorts in view of its task. They are Full-Carry-Save Montgomery secluded Multiplication (FCS-MM) and Semi-Carry-Save Montgomery particular increase (SCS-MM1) shapes. In FCS-MM both the got convey and aggregate are considered as yields. In SCS-MM just the entirety which was acquired is considered as yield. At the point when contrasted with FCS-MM, SCS-MM is having a low zone on account of less number of snake levels in the fundamental calculation. In this paper we talk about the Modified SCS-MM2 engineering and break down it for 128-piece inputs. In SCS-MM calculation it has three information A, B, N, and S as entirety yield .A will be a Multiplicand, B is multiplier and N is modulus. There are a few principles for thinking about the sources of info. They are length of the sources of info ought to be same. Modulus esteem ought to be constantly more noteworthy than the multiplicand and multiplier.

II. LITERATURE SURVEY

The design of accurate multipliers which were applied in image processing has many applications and they lead to less delay and power compared with the logarithm. Appropriate accuracy-configurable multiplier architecture [2] was proposed for many applications. DRUM6[3] which is having the segment size has 6 helps in the comparison of relative error and pass rates where rounding based accurate multiplier has the best results compared with it. The accuracy of the multipler is compared with the DSM8 [4] where it more accurate than the multiplier and has relative error smaller than 2%. Many of the error tolerant multipliers are been proposed by two parts one for the appropriate result and the other was for the accurate results. A 32-bit signed appropriate multiplier was designed which were used in many pipelined processors [5] DRUM6 and DSM8 are some of the accurate multiplier compared with the ROBA multiplier which yields in poor results in almost in all the cases. So, the design of MROBA helps in securing better results and with this MROBA MAC unit is been designed

III. EXISTING SYSTEM

Consider the modulus N to be a k-bit odd number and an extra factor R is to be defined as 2k mod N, where $2k-1 \leq N < 2k$. Given two integers a and b, where a, b,

$$A = a \times R \pmod N \quad (1)$$

$$B = b \times R \pmod N \quad (2)$$

Based on equation (1), the Montgomery modular product Z of A and B can be obtained as

$$Z = A \times B \times R-1 \pmod N \quad (3)$$

In this existing system, convey spare expansion with semi-convey approach is portrayed. In which every one of the multiplicands are not reused, that is whatever the multiplicand is should have been increased around then alone is utilized for deciding the yield. The convey spare approach has higher advantages since it is the fundamental key for working a Montgomery secluded multiplier. In such a way, utilizing this semi convey spare compose just a single convey level snake is executed which might be two serial half adders or a full viper can be utilized in view of the prerequisite. It in this way lessens the quantity of clock cycles and consequently less postponement. So the yield will be streamlined and it can be actualized utilizing Verilog coding.

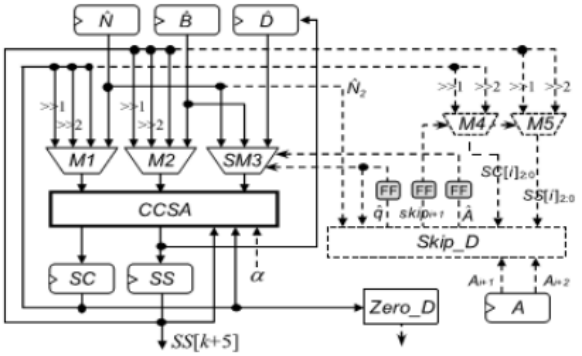

Fig.1. Block diagram of Montgomery Modular Multiplication using CCSA

The above engineering is the semi-convey spare based Montgomery multiplier. In which the circle is decreased on contrasting with the current one. It comprises of two multiplexers, one multiplier, one configurable convey spare snake, flip-flops, skip indicator and zero finder.

Fig. 1 outlines the square chart of proposed semi convey spare multiplier. It is first used to precompute the four-to-two convey spare increases. At that point the required duplication can be performed. The modulus N and information sources will be permitted inside the two multiplexers. This halfway item is then permitted inside the multiplier. Those fractional yields at that point go into configurable convey spare viper, where the convey spare expansion activity is performed. They are put away in the flip flounders briefly. At the point when another halfway yield is executed, at that point that will be put away in the flip tumble. The Skip finder will avoid the past increase which isn't required in the activity in order to lessen the quantity of clock cycles. The halfway item from SM3 is permitted to the multiplexers M4 and M5. Later on it permits inside the flip failures for transitory capacity, at that point to the skip identifier. The yield can be acquired from semi convey. This procedure is rehashed until the point that the yield is acquired. The zero identifiers can likewise be utilized to recognize zero by and large, which is generally required. The multifaceted nature is less contrasted with the past one.

IV. PROPOSED SYSTEM

To increase the Speed of Operation we are replacing the CSA with PASTA (Parallel self timed adder) in the proposed architecture. Montgomery multiplication is to perform fast modular multiplication(MM).PASTA adder using in Montgomery modular multiplication is to reduced area and clock cycles.To outline a basic and proficient radix-2 Montgomery Modular augmentation with Parallel Self Timed Adder (PASTA).The plan of PASTA is utilizes half adders (HAs) alongside multiplexers requiring insignificant interconnections.

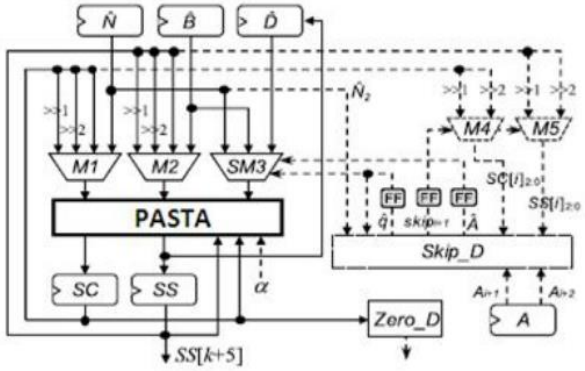

Fig.2. Montgomery Modular Multiplication

The determination contribution for two-input multiplexers compares to the Request handshake flag and will be a solitary 0 to 1 progress indicated by SEL. It will at first select the genuine operands amid SEL=0and will change to input/convey ways for ensuing emphasess utilizing SEL=1. The input way from the HAs empowers the different cycles to proceed until the point that the fulfillment when all convey signs will expect zero qualities are appear in Fig .2.

In the current SCS-MM-New engineering (as appeared in Fig. 3), every last way in that multiplier will be broke down through RTL. Reenactment through coding or RTL see, the way having the most extreme most pessimistic scenario postponement will be discovered. In that way, extra cushions, for example, registers or flip-failures will be presented and the clock is synchronized to lessen the most pessimistic scenario delay. The idea of pipelining will be presented and henceforth effectiveness increments. Working recurrence is contrarily proposed to basic way. Consequently streamlining will be done on Area, Power and Speed. Henceforth the proposed multiplier appeared in Fig. 6 builds the speed and lessens the postpone contrasting with the past existing SCS-MM-New multiplier.

The proposed engineering of Montgomery Modular Multiplication utilizing PASTA snake, which comprises of one-level Parallel Self Timed Adder(PASTA) design, two 4-to-1 multiplexers (M1 and M2) one rearranged multiplier SM3, one skip identifier Skip_D, one zero finder Zero_D, and six registers. Zero identifier Zero_D is utilized to distinguish SC is equivalent to zero. The Skip_D is made out of four XOR entryways, three AND doors, one NOR entryway, and two 2-to-1 multiplexers the skip identifier is utilized to identify the pointless increase tasks.

SIMULATION RESULTS

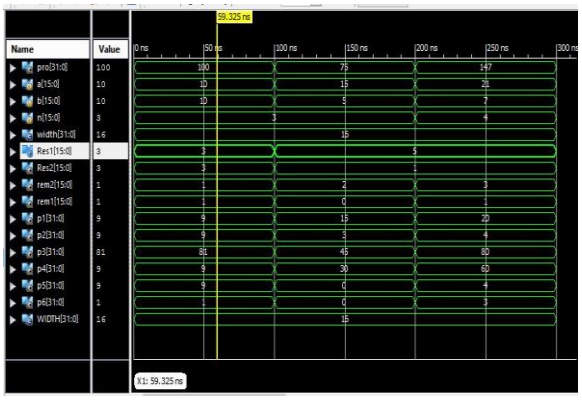

Fig.4. Simulation results of new semi-carry skip Montgomery multiplier

The above Fig. 4 depicts the simulation results for the multiplication of two input numbers by using Xilinx 14.2 ISE software. Here I have taken two input numbers denoted as 'a' and 'b' with an input width of size 32 and modulus value can be denoted by 'n' which can be used to perform the modular multiplication between the input numbers(a * b) and storing the output value into the variable denoted as 'pro'.

Table 1. Synthesis result of New Semi-Carry Skip modular multiplier (SCS-MM)

Device Utilization Summary (estimated values)			
Logic Utilization	Used	Available	Utilization
Number of Slice LUTs	4046	41000	9%
Number of fully used LUT-FF pairs	0	4046	0%
Number of bonded IOBs	80	300	26%
Number of DSP48E1s	2	240	0%

Table 1 shows the synthesis result of new semi-carry skip modular multiplier, in which the design occupies 4046 number of slice LUT's (look up tables) of 41000 available hence the utilization is 9%. Also design uses 0 number of fully used LUT-FF pairs of available 4046 with a utilization of 0% and 80 number of bonded IOB's of available 300 IOB's with a utilization of 26%. And 2 number of DSP-48E1s of available 240 with a utilization of 0%.

V. CONCLUSION

FCS-based multipliers keep up the information and yield operands of the Montgomery MM in the convey skip arrangement to escape from the configuration change, prompting less clock cycles yet bigger region than SCS-based multiplier. To upgrade the execution of Montgomery MM while keeping up the low equipment many-sided quality, this task has adjusted the SCS-based Montgomery augmentation calculation and proposed an ease and elite Montgomery measured multiplier. The proposed multiplier utilized one-level CCSA design and avoided the superfluous convey skip expansion activities to a great extent diminish the basic way delay and required clock cycles for finishing one MM task. Trial comes about demonstrated that the proposed approaches are to be sure equipped for upgrading the execution of radix-2 CSA-based Montgomery multiplier while keeping up low equipment many-sided quality.

VI. REFERENCES

[1] Shiann-Rong Kuang,Member, IEEE, Kun-Yi Wu, and Ren-Yao Lu, "Minimal effort High Performance VLSI Architecture for Montgomery Modular Multiplication," IEEE Trans. Large Scale Integr. (VLSI) Syst., 2015.

[2] S.- R. Kuang, J.- P. Wang, K.- C. Chang, and H.- W. Hsu, "Vitality proficient high-throughput Montgomery secluded multipliers for RSA cryptosystems," IEEE Trans. Large Scale Integr. (VLSI) Syst., vol. 21, no. 11, pp. 1999– 2009, Nov. 2013.

[3] J. Han, S. Wang, W. Huang, Z. Yu, and X. Zeng, "Parallelization of radix-2 Montgomery duplication on multicore stage," IEEE Trans. Large Scale Integr. (VLSI) Syst., vol. 21, no. 12, pp. 2325– 2330,Dec. 2013.

[4] S.- H. Wang, W.- C. Lin, J.- H. Ye, and M.- D. Shieh, "Quick versatile radix-4 Montgomery secluded multiplier," in Proc. IEEE Int. Symp. Circuits Syst., May 2012, pp. 3049–3052.

[5] A. Miyamoto, N. Homma, T. Aoki, and A. Satoh, "Systematicdesign of RSA processors in view of highradix Montgomery multipliers,"IEEE Trans. Large Scale Integr. (VLSI) Syst., vol. 19, no. 7,pp. 1136– 1146, Jul. 2011.

[6] J. C. Neto, A. F. Tenca, and W. V. Ruggiero, "A parallel k-segment strategy to perform Montgomery duplication," in Proc. IEEE Int. Conf. Appl.- Specific Syst., Archit., Processors, Sep. 2011, pp. 251– 254.

[7] G. Sassaw, C. J. Jimenez, and M. Valencia, "High radix usage of Montgomery multipliers with CSA," in Proc. Int. Conf. Microelectron., Dec. 2010, pp. 315– 318.

[8] G. Perin, D. G. Mesquita, F. L. Herrmann, and J. B. Martins, "Montgomery measured duplication on reconfigurable equipment: Fully systolic cluster versus parallel execution," in Proc. sixth Southern Program. Rationale Conf., Mar. 2010, pp. 61– 66.

[9] D. Bayhan, S. B. Ors, and G. Saldamli, "Examining and contrasting the Montgomery augmentation calculations for their capacity utilization," in Proc. Int. Conf. Comput. Eng. Syst., Nov. 2010, pp. 257– 261. [10] P. Amberg, N. Pinckney, and D. M. Harris, "Parallel high-radix Montgomery multipliers," in Proc. 42nd Asilomar Conf. Signs, Syst., Comput., Oct. 2008, pp. 772– 776.