INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 2794 - 2801
RECEIVED : 05.02.2018 PUBLISHED : 18.03.2018
March 18, 2018

DESIGN AND ANALASIS VLSI ARCHITECTURE FOR MONTGOMERY MODULAR MULTIPLICATION

[1] S .Geetha Rani
[1] M.Tech[ES], RGMCET, Nandyal, geetharani419@gmail.com

Abstract
This project aims at utilizing the modular multiplication (MM) with the large integers is the most critical and time consuming operation. Montgomery multiplication is a fast algorithm to compute the Montgomery product, transforming the result out of Montgomery from yields the classical modular product ab mod N. the proposed multiplier receives and output the data with binary representation and uses only one level carry save adder (CSA) to avoid the carry propagation at each addition operation. This CSA is also used to perform operand pre_ computation and format conversion from the carry save format to the binary representation, leading to a low hardware cost and soft critical path delay at the expense of extra clock cycles for completing one modular multiplication. A new SCS_based Montgomery MM algorithm to reduce the critical path delay of Montgomery multiplier. The multiplier used one level CCSA architecture and skipped the unnecessary carry save addition operations to largely reduce the critical path delay and required clock cycle for completing one MM operation. Montgomery modular multiplier can achieve performance and significant power delay product improvement when compared with previous design.

Index Terms— Carry-save addition, low-cost architecture,
Montgomery modular multiplier, public-key cryptosystem.

1. INTRODUCTION

In many public-key crypto systems, modular multiplication (MM) with large integers is the most critical and time-consuming operation. Therefore, numerous algorithms and hardware implementation have been presented to carry out the MM more quickly, and Montgomery's algorithm is one of the most well-known MM algorithms. Montgomery's algorithm determines the quotient only depending on the least significant digit of operands and replaces the complicated division in conventional MM with a series of shifting modular additions to produce $S=A\times B\times R^{-}1(\mathrm{mod}N)$, where N is the k-bit modulus, $R^{-}1$ is the inverse of R modulo N ,and R = 2k mod N. As a result, it can be easily implemented into VLSI circuits to speed up the encryption/decryption process.

Three-operand addition in the iteration loop of Montgomery's algorithm requires long carry propagation for large operands in binary representation. To solve this problem, several approaches based on carry-save addition were proposed to achieve a significant speedup of Montgomery MM. Based on the representation of input and output operands, these approaches can be roughly divided into semi-carry-save (SCS) strategy and full carry-save (FCS) strategy.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 2794 - 2801
RECEIVED : 05.02.2018 PUBLISHED : 18.03.2018
March 18, 2018

X´Y mod M is the operation to be performed. In which X and Y are the inputs. It is necessary to find the value of mod M, henceforth going for this algorithm. Comparing all previously occurring algorithms, this algorithm will produce the optimized output. There are two cases, semi carry save addition and full carry save addition. In this semi carry save addition, the given inputs are in binary and the inter outputs alone in carry save. Whereas in full carry addition, both inputs and inter outputs are in carry save.

On comparing, it can be seen that semi carry save is the most advantageous one because it has only one carry save and hence it has less area and high speed which is required for designing an VLSI based multipliers. TherebA new method is proposed SCS- based Montgomery MM algorithm to reduce the critical path delay of Montgomery multiplier. In addition, the drawback of more clock cycles for completing one multiplication is also improved while maintaining the advantages of short critical path delay and low hardware complexity.

A. Montgomery Multiplication

The Montgomery modular product S of A and
B can be obtained as $S = A \times B \times R^{-1} \pmod N$,where R^{-1} is the inverse of R modulo N .That is, $R \times R^{-1} = 1 \pmod N$. Note that, the notation Xi the ith bit of X in binary representation. In addition, the notation Xi:j indicates a segment of X from the ith bit to jth bit

B. SCS-Based Montgomery Multiplication

Extension of Montgomery multiplication algorithms in GF(p) are studied and analyzed. The time and space requirements of various state-of-the-art algorithms are presented. We propose Modified Montgomery Modular Multiplication Algorithms that reduces the number of computational operations such as number of additions, memory reads and writes involved in the existing algorithms, thereby, saving considerable time and area for execution.

Many design examples has been solved to prove the theoretical correctness of the proposed algorithms. Complexity analysis shows that Modified Coarsely Integrated Scanning (MCIOS) consume less space and time compared to other modified Montgomery Algorithms.Note that the select signals of multiplexers M1 and M2 in Figure 2 generated by the control part are not shown in Fig. 4 for the sake of simplicity. However, the extra clock cycles for format conversion are dependent on the longest carry propagation chain in SS [k+2]+SC[k+2] and about k/2 clock cycles are required in the worst case because two-level CSA architecture.

2. EXISTED MONTGOMERY MULTIPLICATION

A new SCS-based Montgomery MM algorithm is used to reduce the critical path delay of Montgomery multiplier. In addition, the drawback of more clock cycles for completing one multiplication is also improved while maintaining the advantages of short critical path delay and low hardware complexity.

A. Critical Path Delay Reduction

The critical path delay of SCS-based multiplier can be
reduced by combining the advantages of FCS-MM-2 and SCS MM-2. That is, we can precompute D =B+N and reuse the one-level CSA architecture to perform B+N and the format conversion. Figure 1

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 2794 - 2801
RECEIVED : 05.02.2018 PUBLISHED : 18.03.2018
March 18, 2018

shows the modified SCS-based Montgomery multiplication (MSCS-MM) algorithm and one possible hardware architecture, respectively.

The Zero_D circuit in Figure 4 is used to detect whether SC is equal to zero, which can be accomplished using one NOR operation. The Q-L. The carry propagation addition operations of B+N and the format conversion are performed by the one-level CSA architecture of the MSCS-MM multiplier through repeatedly executing the carry-save addition (SS,SC) = SS+SC+0 until SC =0.

In addition, we also precompute A_i and q_i in iteration i−1 so that they can be used to immediately select the desired input operand from 0, N,B, and D through the multiplexer M3 in iteration i. Therefore, the critical path delay of the MSCS-MM multiplier can be reduced into T MUX4+TFA.

B. Clock Cycle Number Reduction

To decrease the clock cycle number, a CCSA architecture which can perform one three-input carry-save addition or two serial two-input carry-save additions is proposed to substitute for the one-level CSA architecture.

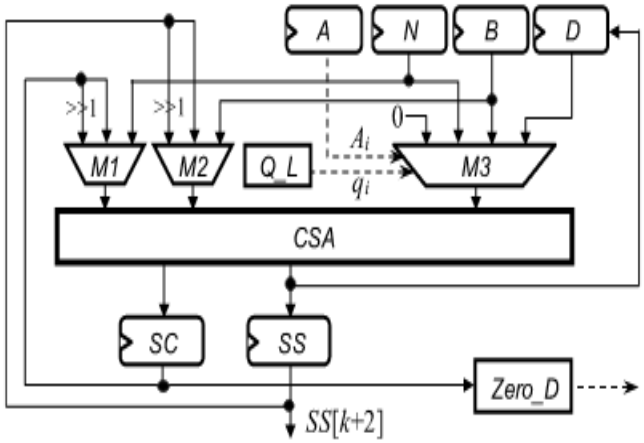

Figure 1:Modified SCS-based MM multiplier

On the bases of critical path delay reduction, clock cycle number reduction, and quotient pre-computation mentioned above, a new SCS-based Montgomery MM algorithm (i.e., SCS-MM-New algorithm shown in Figure 4) using one-level CCSA architecture is proposed to significantly reduce the required clock cycles for completing one MM. As shown in SCS-MM-New algorithm, steps 1–5 for producing ˆ B and ˆD are first performed. Note that because $q_i + 1$ and $q_i + 2$ must be generated in the ith iteration, the iterative index I of Montgomery MM will start from − 1 instead of 0 and the corresponding initial values of ˆq and ˆA must be set to 0.

3. ANALYSIS

In this existing system, carry save addition with semi-carry approach is described. In which all the multiplicands are not recycled, that is whatever the multiplicand is needed to be multiplied at that time alone is used for determining the output. The carry save approach has higher benefits since it is the basic key for operating a Montgomery modular multiplier. In such a way, using this semi carry save type one Ai+1, Ai+2 and qi+1, qi+2 should be known already in order that the unwanted steps in the (i +1)

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 2794 - 2801
RECEIVED : 05.02.2018 PUBLISHED : 18.03.2018
March 18, 2018

iteration can be reduced by determining i iteration. So as to pre compute the quotients. Another method is using skip detector so that it will pre computes the values. And also since the shortest path in this multiplier is lengthened, it has to be minimized. As modulus N is an odd number, it can be used directly for the multiplication. So that time is consumed highly. Ai+1, Ai+2 and qi+1, qi+2 should be known already in order that the unwanted steps in the (i +1) iteration can be reduced by determining i iteration. So as to pre compute the quotients. Another method is using skip detector so that it will pre computes the values. And also since the shortest path in this multiplier is lengthened, it has to be minimized. As modulus N is an odd number, it can be used directly for the multiplication. So that time is consumed highly. carry level adder is implemented which may be two serial half adders or a full adder can be used . The proposed architecture of Montgomery Modular Multiplication using PASTA adder, which consists of one one-level Parallel Self Timed Adder(PASTA) architecture, two 4-to-1 multiplexers (M1 and M2) one simplified multiplier SM3, one skip detector Skip_D, one zero detector Zero_D, and six registers. Zero detector Zero_D is used to detect SC is equal to zero. The Skip_D is composed of four XOR gates, three AND gates, one NOR gate, and two 2-to-1 multiplexers the skip detector is used to detect the unnecessary multiplication operations. Many design examples has been solved to prove the theoretical correctness of the proposed algorithms.

Complexity analysis shows that Modified Coarsely Integrated Scanning (MCIOS) consume less space and time compared to other modified Montgomery Algorithms. To verify the logical correctness, the proposed MCIOS algorithm was implemented in Xilinx Spartan3E FPGA. The total memory for execution of 64 –bit operand is 135484 KB for MCIOS and 140496 KB for existing Coarsely Integrated Scanning (CIOS) method. The proposed algorithm can be changed to be suitable for any arbitrary Galois field size with little modifications. Also the proposed algorithm can be developed as architecture suitable for System on Chip (SoC) implementations of Elliptic curve cryptosystem. Subsequently, the system can

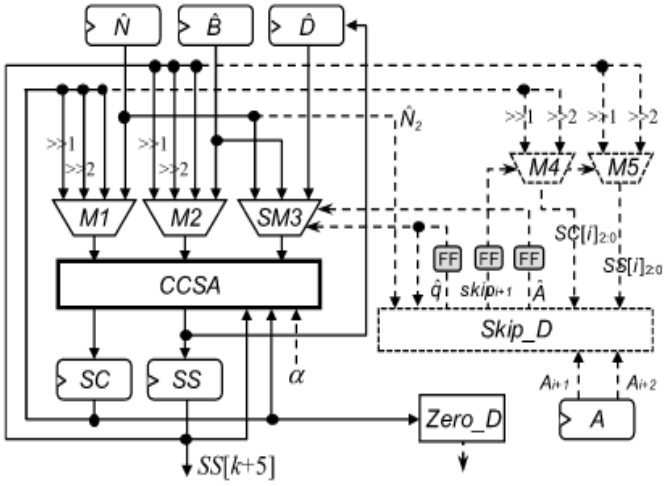

Figure 2: SCS-MM-New multiplier

4. PROPOSED MONTGOMERY MULTIPLICATION

This extend the existing system by replacing the CSA adder block with cmos full adder in fig 3. The proposed architecture of Montgomery Modular Multiplication using PASTA adder, which consists of one one-level Parallel Self Timed Adder(PASTA) architecture, two 4-to-1 multiplexers (M1 and M2) one simplified multiplier SM3, one skip detector Skip_D, one zero detector Zero_D, and six registers.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 2794 - 2801
RECEIVED : 05.02.2018 PUBLISHED : 18.03.2018
March 18, 2018

Zero detector Zero_D is used to detect SC is equal to zero. The Skip_D is composed of four XOR gates, three AND gates, one NOR gate, and two 2-to-1 multiplexers the skip detector is used to detect the unnecessary multiplication operations.

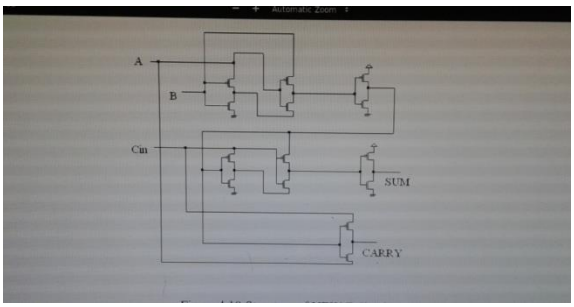

Fig 3:Cmos Full Adder

The circuit of 14T adder is a One bit full adder cell is made of seven cmos inverters that are connected as shown in fig 3. The proposed full adder is proven to have the minimum power consumption and less power delay product.

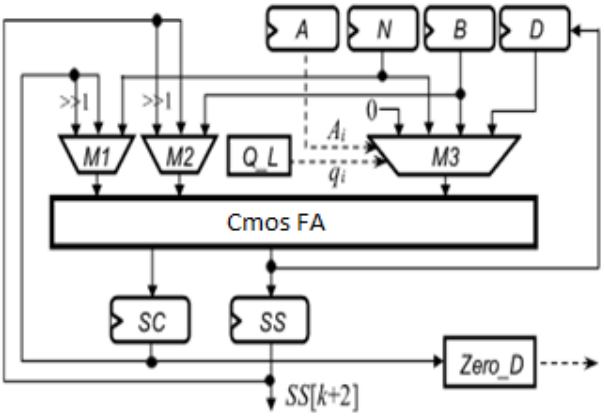

Fig 4: cmos full adder used in MSCS-MM

This partial product is then allowed inside the multiplier. Those partial outputs then enter into configurable carry save adder, where the carry save addition operation is performed. They are stored in the flip flops temporarily. When another partial output is executed, then that will be stored in the flip flop.

The Skip detector will skip the previous multiplication which is not required in the operation so as to reduce the number of clock cycles. The partial product from SM3 is allowed to the multiplexers M4 and

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 2794 - 2801
RECEIVED : 05.02.2018 PUBLISHED : 18.03.2018
March 18, 2018

M5. Later on it allows inside the flip flops for temporary storage, then to the skip detector. The output can be obtained from semi carry. This process is repeated until the output is obtained. The zero detectors can also be used to detect zero in many situations, which is most required. The complexity is very less compared to the previous one

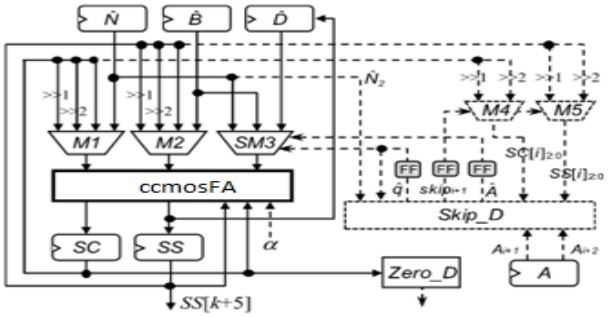

Fig 5: SCS-MM New Multiplier with cmos full adder

5. EXPERIMENTAL RESULTS

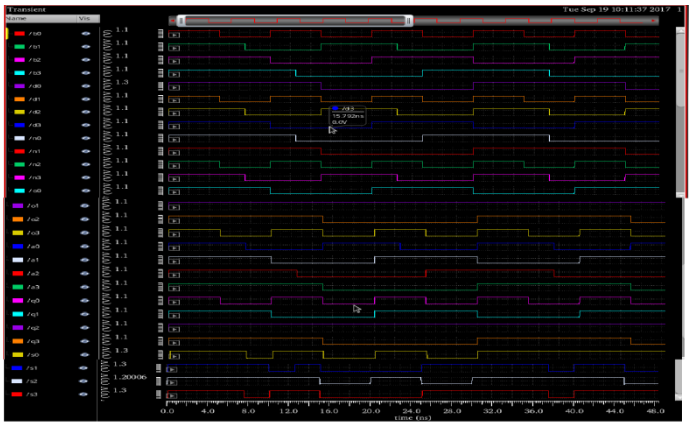

Fig: 4-bit Modified SCS-based MM

The design has been implemented using Xilinx Verilog coding. For further verification, the design can be done using Cadence. It can be clearly understand by the waveform shown below. In the existed architecture disadvantages are carry propagation delay and extra clock cycles. To overcome the disadvantages we go for PASTA adder. The PASTA adder is using in Montgomery Modular Multiplier in these advantages are low hard ware cost short critical path delay and required clock cycles are reduced for completing one MM operation.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 2794 - 2801
RECEIVED : 05.02.2018 PUBLISHED : 18.03.2018
March 18, 2018

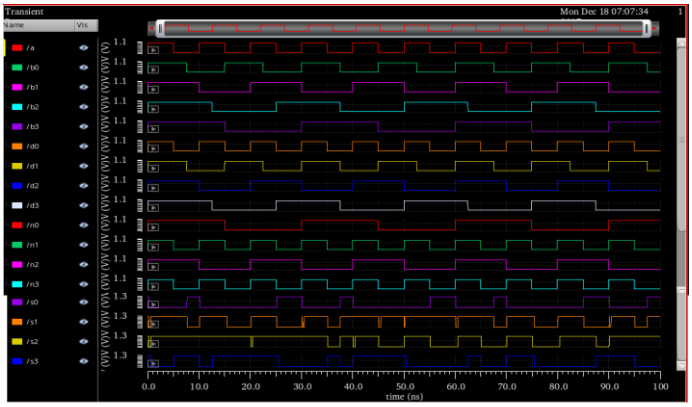

Fig : 4-bit SCS-MM-New multiplier

COMPARISION TABLE

Montgomery Multiplication	Power	Delay	PDP
1bit Mscs-mm	18.23uw	110.6E-12	2.016238E-15
1bit new Scs-mm	37.81uw	60.79E-12	2.2984699E-15
4bit Mscs-mm	219.3uw	77.79E-12	1.70593E-14
4bit new scs-mm	124.4uw	142.6E-12	1.76648E-14
Proposed 1bit Mscs-mm	19.16uw	37.84E-12	0.7250144E-15
Proposed 1bit new scs-mm	53.50uw	45.24E-12	2.22034E-15

The above architecture is the semi-carry save based Montgomery multiplier. In which the loop is reduced on comparing to the existing one. It consists of two multiplexers, one multiplier, one configurable carry save adder, flip-flops, skip detector and zero detector. In order to reduce the critical path delay, the operations in semi carry save and full carry save is performed jointly. The carry save format conversion as well as the binary format should be taken place.

Then pre-computation must be done in order to reuse the multiplicand values. Another method is using zero detectors. SC will produce the output only when the zero is detected. Then the pre computation can be done i-1 iteration.

CONCLUSION

In the proposed method these challenges are tackled by introducing SSC_MM new multiplier. And also a simple and efficient Montgomery multiplication algorithm such that the low-cost and high-performance Montgomery modular multiplier can be implemented. To reduce the extra clock cycles a configurable CSA (CCSA), which could be one full-adder or two serial half-adders is used. In addition, a mechanism that can detect and skip the unnecessary carry-save addition operations in the one-level CCSA architecture while maintaining the short critical path delay is developed.

To further verify the efficiency of the proposed design, we synthesized those Montgomery modular multipliers SCS are used cmos based full adder reduce the power and delay.

REFERENCES

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

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

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

[4] S.-H. Wang, W.-C. Lin, J.-H. Ye, and M.-D. Shieh, "Fast 5scalable radix-4 Montgomery modular multiplier," in Proc. IEEE Int. Symp. Circuits Syst., May 2012, pp. 3049–3052.

[5] A. Miyamoto, N. Homma, T. A oki, and A. Satoh, "Systematic design of RSA processors based on high-radix Montgomery multipliers," IEEE Trans. Very Large Scale Integr. (VLSI) Syst. , vol. 19, no. 7, pp. 1136–1146, Jul. 2011.

[6] G. Perin, D. G. Mesquita, F. L. Herrmann, and J. B. Martins, "Montgomery modular multiplication on reconfigurable hardware: Fully systolic array vs parallel implementation," in Proc. 6th Southern Program. Logic Conf., Mar. 2010, pp. 61–66.

[7] P. Amberg, N. Pinckney, and D. M. Harris, "Parallel high-radix Montgomery multipliers," in Proc. 42nd Asilomar Conf. Signals, Syst., Comput. , Oct. 2008, pp. 772–776.

[8] Y.-Y. Zhang, Z. Li, L. Yang, and S.-W. Zhang, "An efficient CSA architecture for Montgomery modular multiplication," Microprocessors
Microsyst., vol. 31, no. 7, pp. 456–459, Nov. 2007.

[9] H. Zhengbing, R. M. Al Shboul, and V. P. Shirochin, "An efficient architecture of 1024-bits crypto processor for RSA cryptosystem based on modified Montgomery's algorithm," in
Proc. 4th IEEE Int. Workshop Intell. Data Acquisition Adv. Comput. Syst., Sep. 2007, pp. 643–646