Implementation of VLSI Architecture for Montgomery Modular Multiplier

Shobana Priya M S, Priyanka R, Manikandan T, Joshua Kumaresan S, Satheesh Kumar S

Abstract*: The paper proposes a Montgomery Modular Multiplier (MMM) using a simple and efficient Montgomery multiplication algorithm. Here a modification in the form of using hybrid full adders in the Carry Save adder is proposed. The hybrid full adder is designed using a conventional Complementary Metal Oxide Semiconductor and transmission gate logic. There is about 54% and 55% reduction of area (no. of components) in Radix 2 MMM and Semi-Carry-Save (SCS) based MMM with hybrid full adders. There is significant reduction in the power dissipation of 52% for Radix 2 MMM and 46% of SCS based MMM when hybrid adders are used instead of C-CMOS Full-Adders. The delay is also reduced by 47% in SCS based MMM as compared to that of Radix 2 MMM. The software used are Xilinx ISE 14.2 and Mentor Graphics Pyxis Schematic in 180-nm technology.

Keywords: **MMM, C-CMOS, SCS, Hybrid full adder.**

I. INTRODUCTION

Traditionally, cryptography is used for military and diplomatic services to provide secure communication, in which the parties involved in communication share a secret key in secured ways. All cryptographic operations are done in finite fields, which map to modular multiplication in the digital world. The Montgomery modular multiplication, more commonly referred to as Montgomery multiplication, will be made use to construct these cryptography applications. This multiplication paves way for performing fast modular multiplication.

This Montgomery Multiplication Algorithm has the advantage of replacing division operations by bit shift operations. If the least significant bits to be shifted out are not zero, Montgomery's algorithm adds multiples of modulus to clear these bits before shifting them out. In conventional modular multiplication, the multiplicand are processed for all the bits and modulus is repeatedly subtracted from the result till the result obtained is less than the modulus. In Montgomery multiplication, bits are shifted out as each bit of the multiplicand is processed, leaving no need for the subtractions. Thus, reducing the overall execution time when there are many multiplications to be done with the same modulus and with the same number of multipliers is achieved using Montgomery Modular Multiplier.

Revised Manuscript Received on November 12, 2019.

M.S.Shobana Priya, M.E.,(Ph.D), Assistant Professor, Department of ECE, Saveetha School of Engineering, Mail id: shobanapriyams.sse@saveetha.com

R.Priyanka M.E.,(Ph.D), Assistant Professor, Department of ECE, Saveetha School of Engineering, Mail id: priyankar.sse@saveetha.com

Dr. T.Manikandan, Professor, Department of ECE, Rajalakshmi Engineering College, Mail id: manikandan.t@rajalakshmi.edu.in

Dr.S.Joshua kumaresan, Associate Professor, Department of ECE, R.M.K. Engineering College, skn.ece@rmkec.ac.in

S. Satheesh Kumar, Assistant Professor, Department of ECE, Sri Krishna College of Engineering and Technology, ssatheeshkumarpsg@gmail.com

II. MONTGOMERY MODULAR MULTIPLIER

Modular multiplication with large integers is a time-consuming operation and considered difficult. Therefore, many algorithms were derived in-order to make this process easier. One of these techniques is Montgomery Modular Multiplication (MMM). The existing systems that are being considered for the implementation of this project is the radix 2 Montgomery Modular Multiplication and Semi-Montgomery modular multiplication based on Carry-Save. The architecture and algorithms are as follows.

A. CARRY SAVE ADDER

Carry Save Adder is one of the classification of digital adders which finds its importance in computer architecture to compute sum of three or more n-bits in binary. CSA is a digital adders that differs slightly from other adders. It outputs two numbers of the similar dimensions as the inputs bits. One output is a sequence of partial sum bits and another is a sequence of carry bits. This unique property of CSA makes it employable where there is an adequate need for fast multiplication. In this paper for each iteration the conditions are been checked and the addition is carried out only with the help of carry save adder. The proposed system will have its impact on the carry save adder by replacing the Conventional-Complementary Metal-Oxide semi-conductor Full-Adder by Hybrid Full-Adder circuit.

III. RADIX 2 BASED MONTGOMERY MODULAR MULTIPLIER

A, B, N are considered as inputs, S(k) is considered as output**,** k is the number of input bits which determines the number of iterations and i is the iteration value. Initially for 0^{th} iteration k=0, S(k) is considered as 0. The input Ai and B gets multiplied. Once when this multiplication is over the initial carry and sum value are added with the multiplied value. Here q_i is the last bit of sum obtained from carry save adder 1. The sum and carry obtained from carry and sum is denoted as SS(Sum) and SC(Carry). The value of qi when it is said to be 1, gets multiplied with N and added with the already multiplied value of Ai and B.

this process takes place until the number of iterations is k-1 and the result S[k] is obtained. The block diagram is shown in figure 1.

Algorithm MM:
Radix-2 based Montgomery Modular Multiplier
Inputs: A,B,N (modulus)
output: S[k]
1. S[0] = 0;
2. for i = 0 to k – 1 {
3. qi = (S[i] + Ai * B) mod 2;
4. S[i+1] = (S[i]+ * B + qi * N)/2;
5. }
6. if (S[k] > N) S[k} = S[k] – N;
7. return S[k];

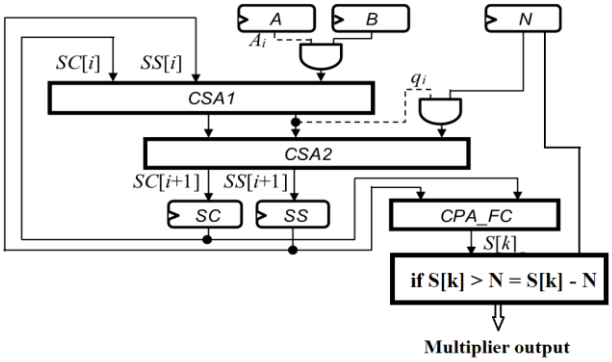

Fig. 1.Radix-2 based Montgomery Modular Multiplier.

IV. SCS BASED MONTGOMERY MODULAR MULTIPLIER

The SCS based MMM gives results in Semi Carry Save format. SS and SC are the corresponding outputs that are been obtained. The main advantage of SCS based MMM over radix 2 MMM is that the usage of subtractor is avoided. Instead of subtractor the number of iterations are increased by 2 i.e k to k+2 so that the final comparing and subtraction can be fully avoided. Due to this the area optimization, can be done and the power dissipation is also reduced with reduction in the overall delay. The algorithm of SCS based MMM is given as follows and the block diagram is given in figure 1.
Algorithm MM:
SCS based Montgomery Modular Multiplier
Inputs: A,B,N (modulus)
output: S[k+2]

1. SS [0] = 0; SC [0] = 0;
2. for i = 0 to k + 1 {
3. q_i = (SS[i] + SC[i] + A_i * B) mod 2;
4. (SS[i+1], SC[i+1]) = (SS[i] + SC[i] + A_i * B + q_i* N)/2;
5.}
6. S[k+2] = SS[k+2] + SC[k+2];
7. return S[k+2];

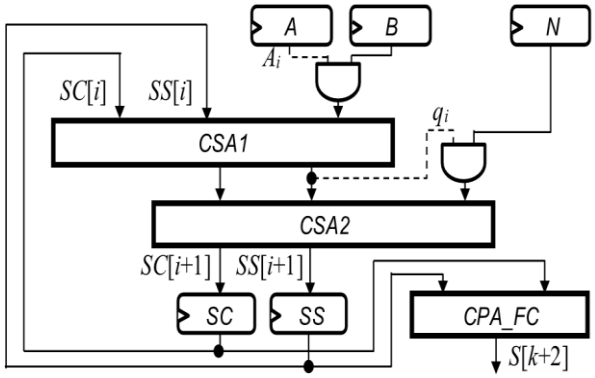

Fig. 2.SCS based Montgomery Modular Multiplier.

V. HYBRID FULL-ADDER

The hybrid logic has different modules such as Modified XNOR module and Carry generation module. SUM generation is carried out by the XNOR module and the Carry generation is done by CARRY generation module. Here in hybrid logic C-CMOS and transmission gates are coupled together to achieve low power and high speed operation when compared to other conventional Full-Adder design logic styles. The XNOR module is designed using Conventional CMOS and the carry generation module is designed using transmission gates.

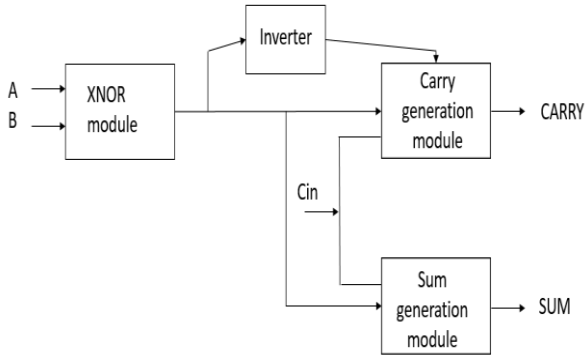

Fig. 3.Hybrid Full-Adder.

The transistor level diagram of carry/sum generation module, XNOR module in Hybrid full-adder is given as follows.

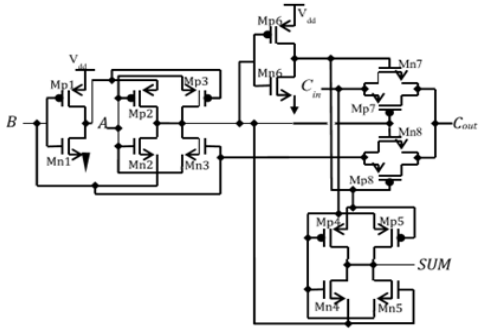

Fig. 4.Hybrid Full-Adder (transistor level)

In the place of normal Full-Adders, these Hybrid Full-Adders are being used and the major optimization is been achieved.

VI. RESULTS AND DISCUSSION

The Area and Power calculations are done in Mentor graphics Pyxis Schematic Tool and Delay Calculation is done with the help of Xilinx ISE 14.2.

The output waveform in Xilinx ISE 14.2 and schematic in Pyxis Schematic is given as follows.

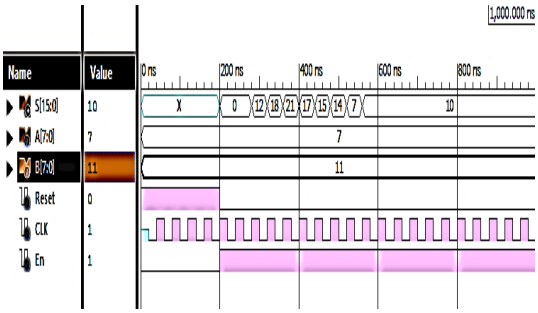

Fig. 5.Radix-2 MMM output Waveform.

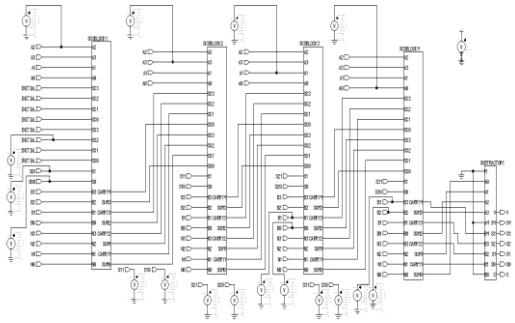

Fig. 6.Radix-2 MMM Schematic.

Factors	Radix 2 MMM		SCS based MMM	
	C-CMOS FA	Hybrid FA	C-CMOS FA	Hybrid FA
Area (4-bit)	2682	1458	1866	1040
Delay (8-bit)	2.477 n sec		1.169 n sec	
Power Dissipated (4-bit)	66.461 n watts	35.166 n watts	45.609 n watts	21.064 n watts

VII. GRAPHICAL REPRESENTATION

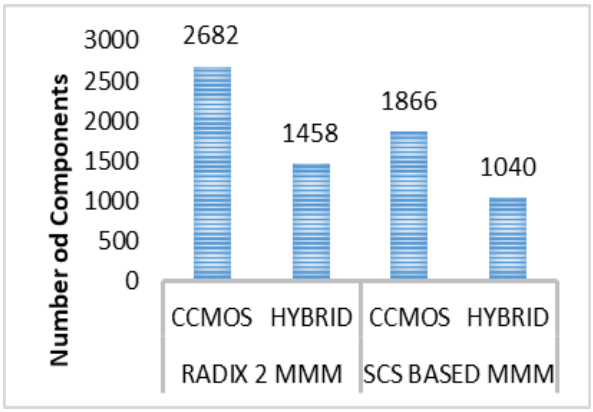

Fig. 7.Area comparison

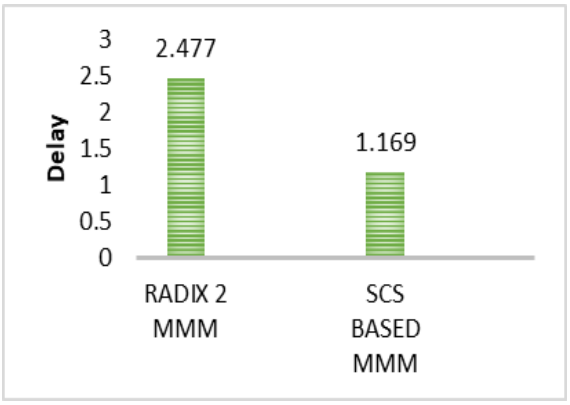

Fig. 8.Delay comparison (n sec)

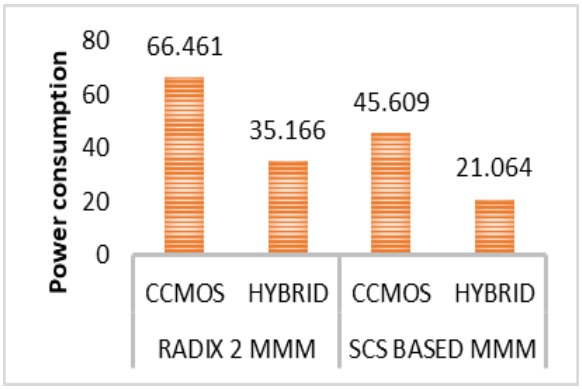

Fig. 9.Power Comparison (n watts).

VIII. CONCLUSION

Thus, a Montgomery Modular Multiplier architecture is designed with Hybrid Full-Adders. This reduces the overall delay, power dissipation and area. The efficiency of the multiplier is improved by replacing normal C-CMOS adder with Hybrid Full-Adder. This architecture is implemented in both Xilinx ISE 14.2 and Mentor Graphics Pyxis schematic tool. The comparison of area, delay and power dissipation is given for both Radix 2 MMM and SCS based MMM. The significance of using Hybrid Full-Adder in place of C-CMOS Full-Adder is the reduction of overall area of about 54% and 55% for Radix 2 MMM and SCS based MMM respectively. The improvement in delay is studied using Xilinx ISE 14.2 tool from Radix 2 MMM and SCS based MMM is of 47%. The optimization obtained in Power dissipation is 52% and 46% for Radix 2 MMM and SCS based MMM when Hybrid Full-Adder is used in place of C-CMOS Full-Adders.

ACKNOWLEDGMENT

The authors would like to thank College of the author and the co-authors for providing the required facility in the research work.

REFERENCES

1. C. D. Walter, “Montgomery exponentiation needs no final subtractions,” Electron. Lett., vol. 35, no. 21, pp. 1831–1832, Oct. 1999.
2. C. McIvor, M. McLoone, and J. V. McCanny, “Modified Montgomery modular multiplication and RSA exponentiation techniques,” IEE Proc.Comput. Digit. Techn., vol. 151, no. 6, pp. 402–408, Nov. 2004.

3. D. Bayhan, S. B. Ors, and G. Saldamli, “Analyzing and comparing the Montgomery multiplication algorithms for their power consumption,” in Proc. Int. Conf. Comput. Eng. Syst., Nov. 2010, pp. 257–261.
4. 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.
5. M. Zhang, J. Gu, and C.-H. Chang, “A novel hybrid pass logic with static CMOS output drive full-adder cell,” in Proc. Int. Symp. Circuits Syst., May 2003, pp. 317–320.
6. P. Bhattacharyya, B. Kundu, S. Ghosh, V. Kumar and A. Dandapat, “Performance Analysis of a Low-Power High-Speed Hybrid 1-bit Full-Adder Circuit,” IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 23, no. 10, pp. 2001–2008, Oct. 2015.
7. P. L. Montgomery, “Modular multiplication without trial division,” Math. Comput., vol. 44, no. 170, pp. 519–521, Apr. 1985.
8. Y. S. Kim, W. S. Kang, and J. R. Choi, “Asynchronous implementation of 1024-bit modular processor for RSA cryptosystem,” in Proc. 2nd IEEE Asia-Pacific Conf. ASIC, Aug. 2000, pp. 187–190.
9. Shiann-Rong Kuang, Member, IEEE, Kun-Yi Wu, and Ren-Yao Lu, “Low-Cost High-Performance VLSI Architecture for Montgomery Modular Multiplication,” in IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, VOL. 24, NO. 2, Feb 2016.

AUTHORS PROFILE

Mrs. M S. Shobana Priya is a Assistant Professor working at Saveetha School of Engineering, Thandalam, Chennai. She is currently pursuing her Ph.D in Machine learning at Saveetha School of Engineering, SIMATS, Thandalam since June, 2018. She did her bachelor’s degree in Engineering from Jaya Engineering College, Thiruniravur under Anna University & master’s degree in Engineering from College of Engineering, Anna University, Guindy during 2011 & 2015, respectively. She is having 1.5 years of teaching experience in UG. She also guided many projects at UG levels.

R.Priyanka pursued her B.E Degree in Electronics and Communication Engineering in 2015 and M.E degree in Applied Electronics from R.M.K Engineering College in 2017.She is pursuing her Ph.D degree and working as an Assistant Professor in ECE Department at Saveetha school of Engineering. She has a teaching experience of 2 years. Her area of research includes Machine learning and Artificial Intelligence.

Dr. T. Manikandan is a Professor working at Rajalakshmi Engineering College, Thandalam, Chennai. He has completed his Ph.D titled “A study on computer-aided diagnosis systems for lung cancer detection and its three dimensional visualization using machine learning techniques” at Anna University, Chennai during January, 2017. He did his bachelor’s degree in Engineering from Vellore Engineering College, Chennai under Madras University & master’s degree in Engineering from College of Engineering, Anna University, Guindy, Chennai during 1998 & 2007, respectively. He is having 21 years of teaching experience which includes both UG and PG. He also guided many projects at UG & PG levels. He has 50 papers in refereed international journals and conferences in his credit. He is serving as editorial board member for various international journals such as International journal of Biomedical and Healthcare Sciences, Archives of General Internal Medicine, Journal of Cancer Diagnosis, Journal of Medical and Clinical Oncology, Journal of Clinical Epigenetics and Integrative Cancer Biology and Research.

Dr.S.Joshua Kumaresan is working as Associate professor in the department of ECE of R.M.K. Engineering college. He completed his Ph.D in the area of image processing in 2018, M.E (VLSI Design) in 2007 both from Anna university Chennai. He also completed M.S (Electronics and Control) from BITS, Pilani in 1999 and B.E (ECE) in 1994 from Bharathidasan University. He has 23 years of teaching experience which includes both UG and PG. and 1 year he worked in an industry as R& D Engineer. He published more than 20 papers in international journal and conferences.He published books on Electromagnetic Fields, Digital Electronics, Digital Principles system design and Digital logic circuits. . He guided many projects at UG & PG levels. He also mentored and guided many students for various competitions like Smart India Hackathon, Arm design contest, India Innovation challenge design contest 2018 etc. He organized many college level National conferences and symposiums. He is a member of professional societies IEI, ISTE, ISRO-ISSE, and IACSIT.

Satheesh Kumar S currently working as Assistant Professor at Sri Krishna College of Engineering and Technology, Coimbatore. He accomplished his Master of Engineering in the field of Communication Systems from PSG College of Technology, Coimbatore and B.E. from Anna University, Chennai. He is also a Life time member of IETE and ISRD. Having more than 4 years of teaching experience, he is acting as a board member for some Private Engineering Institutions in Coimbatore. He is also a recipient of various honors and faculty awards in his teaching fraternity. He also published over 20 technical articles in various International and national journals and filed a patents in his research field.His research focus include Electromagnetics, Microwave Engineering, Speech Processing and Block Chain technology.