This full-text paper was peer-reviewed and accepted to be presented at the IEEE ICCSP 2015 conference.

An Energy Efficient Montgomery Modular Multiplier for Security Systems using Reversible Gates

M. Mohaideen Abdul Kadar, A.V.Ananthalakshmi

***Abstract*—Recently, Security requirements forelectronic transactions have become an important concern. RSA is the widely adopted public key algorithms. The RSA public key cryptography uses modular exponentiation operation both for encryption and decryption. A famous approach is Montgomery modular multiplication decreases the multiplication period dramatically. Today's system loses information after every logic operation. The amount of energy dissipated for every lost bit is KTln2. Reversible logic has gained much interest in recent years due to its ability in preserving the information without any energy loss. Therefore Montgomery modular multiplier designed using reversible logic gates gives better energy efficiency in terms of number of gates used, number of garbage outputs produced and quantum costs.**

Index Terms — Reversible gates, CSA, Shift register, MUX.

I. INTRODUCTION

MANY people do their business in internet and most of the data communication is critic and sensitive which increased the demand for highly reliable and secure products [1]. RSA one of the public cryptography system that relies on the modular exponentiation method is proved to be an efficient system in all aspects.

Modular arithmetic uses only positive integer. One of the benefits is that, it can support higher power integer computation with less complexity [2]. For example, assume m = {$mn-1$ $mn-2$... $m0$} is normalized, which yields $1/2 \le mn-1 < 1$ or it can be interpreted as $1/2 \le m < dn$ which is normally the case with RSA modulous. It can also be normalized by replacing m with $2km$. A modular reduction step fixes the result.

M.Mohaideen Abdul Kadar, Student is with Dept. of Electronics & Communication Engineering, Pondicherry Engineering College Pillaichavady, Puducherry, (e-mail: mohaideenbtech@gmail.com).

A.V.Ananthalakshmi, Assistant Professor is with Dept. of Electronics & Communication Engineering, Pondicherry Engineering College, Pillaichavady, Puducherry, (e-mail: anantha_av@pec.edu)

Having Rk = a mod $2km$ calculated, R ←R – q. m, where q is computed from the leading digits of Rk and $2km$. These denormalization steps are only performed at the beginning and end of the calculations, so the amortized cost is negligible.

Montgomery modular multiplication is the simplest and fastest algorithm that uses right to left divisions as there are no problems with carries when the operations are carried out from right to left [3]. The traditional Montgomery multiplication performs multiplication in row order so that, it can take the advantage of speedup for squarring [4]. But the main disadvantage is that the numbers should be converted into a special form before calculation.

Power dissipation is the physical attack in security systems. So reversible logic is used to avoid this attack. In reversible logic circuit no information will be lost. Finally zero energy dissipation would be possible when using only reversible gates. In this paper the Montgomery multiplier designed using reversible logic gates which gives the better power efficient results. This research work is organized as follows. The following section presents the related work of this research. We describe the overview of reversible circuits. Then, we discuss a proposed Montgomery modular multiplier implementation and simulation. The final section concludes the research work by addressing the challenges and future scope of the work.

II. RELATED WORK

Shiann-Rong Kuang, Jiun-Ping Wang, et.al [1], introduced the Montgomery multiplier for RSA cryptosystem which required less area and less energy, also they have discussed about the modified BRFA to reduce the energy consumption in BRFA. G.A.V.Ramachandra, P.V.Lakshmi, et.al [2], introduced the novel exponentiation computation for public key cryptosystems. Here the limitation is the power consumption, but in [3] the hardware based cryptography such as RSA and ECC had been discussed and also they provides the Montgomery multiplication algorithm for RSA and ECC. The limitation is that the processor speed. Satyanarayana Vollala, Varadhan, et.al [4], provides the modular exponentiation for cryptographic applications

978-1-4799-8081-9/15/$31.00 © 2015 IEEE

like RSA to improve the speed of processor and security of the system, also they compare the Chinese remainder theorem with Montgomery algorithm.

III. REVERSIBLE CIRCUITS

In hardware point of view the power consumption is one the main criteria to be considered which is mostly due to leak from usage of ALU. Because ALU uses CPA, CSA, shift register and multiplexer [5].use irreversible circuits which requires high amount of power which calls for optimized designs. Reversible circuits is different from irreversible one as there is data loss. By using these gates, the circuit cost and the power consumption can be reduced [6].This section includes the components of reversible circuits for constructing multiplier and also the resulted number of gates used, the number of garbage outputs produced and the required quantum costs. The remaining sections describes the efficient Montgomery multiplier design and results which is compared with existing architecture.

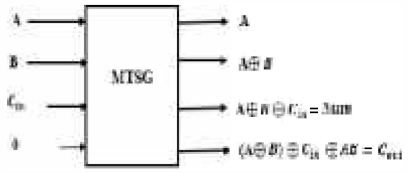

Fig. 1. Reversible 8 bit CSA

For full adder circuit designing, TSG gates are suitable, but its quantum cost is very high, therefore Modified TSG gate can be used.as it gives less quantum cost. It is shown in Fig. 1

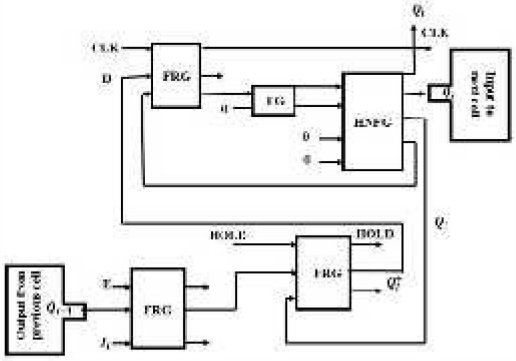

Fig. 2. Reversible PIPO Register

Reversible PIPO register shown in Fig.2 uses three fredkin gates and has four Qi outputs. One of the Qi outputs is used for the generation of, second one is used to generate, third one is considered as parallel output and the other is fed to its own D flip-flop's fredkin gate. CLK output of each basic cell is connected to the CLK input of the next basic cell.

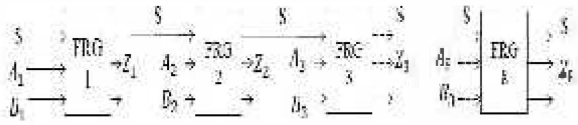

Fig. 3. Reversible 8 bit Multiplexer

Fig. 3. Shows that the 8 bit reversible multiplexer [2] Here S is the selection input, A and B are the inputs to the multiplexer. Z is the output from the multiplexer.

If S=0 means, Z=A;
If S=1 means, Z=B

Therefore, it require 8 bit inputs to the Fredkin gate and produces 8 bit garbage outputs

IV. PROPOSED REVERSIBLE MONTGOMERY MULTIPLIER ARCHITECTURE

In regular modular multiplication, all bits of the multiplicand are processed and modulus is subtracted repeatedly from the result unless the result 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 [1].

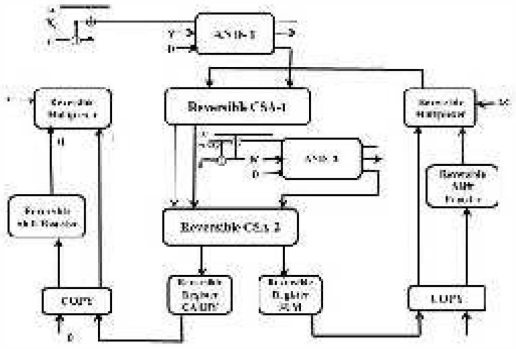

Fig. 4. Proposed Reversible MontgomeryMultiplier Architecture

The proposed reversible Montgomery multiplier architecture shown in Fig.4.

An 8-bit reversible Montgomery multiplier is desgined using the following modules:

i) a 8-bit reversible CSA
ii) a 8-bit reversible AND function
iii) a 8-bit reversible multiplexer
iv) a 8-bit reversible PIPO shift regsiter
v) a 8-bit reversible register and
vi) a 8-bit reversible COPY function

AND-1 block done AND operation where the inputs are *Xi* and Y. This operation was done by using Peres gates. AND-2 block done AND operation where the inputs are M and *SUM0*.

COPY blocks are used for copying the signals to avoid the fan-out problems. This block can be designed by using Feynman gates.

In order to reduce the garbage outputs, quantum costs and the number of gates used, reversible gates are used in CSA, shift register and in Multiplexer.

V. SIMULATION RESULTS AND DISCUSSION

The simulation results for reversible 8 bit multiplexer is shown in Fig.5. The simulation results are obtained in the tool Modelsim.

The input is given and the corresponding output is obtained. Then the reset is set to 0 and the input is given and the corresponding output is obtained. The input is given for y as 10101110, selection signal as 1, reset as 1 and the clock. The corresponding outputs obtained for z is 01010001, similarly for selection signal 0 the output is obtained as 00001010 Then the reset is changed to 0 and all other inputs are same then the corresponding outputs is 10101110. The selection signal is s. For the selection signal s=0, the ouput is 01000001 and l is 11001011

.

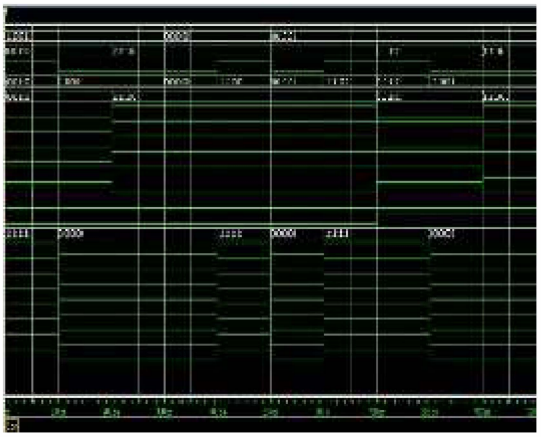

Fig. 5. Simulation Result of MUX using FRG gates

The comparison results of different reversible MUX is shown in Table 1

TABLE I

COMPARISON RESULTS OF DIFFERENT REVERSIBE MUX

S.NO	VARIABLE	TSG GATE	MTSG GATE
1	Total Number of reversible Gates used	2	1
2	Total number of garbage outputs	4	2
3	Quantum Cost	2*13=26	1*6=6

From the Table I, it is clear that FRG gate uses less number of reversible gates and produces less number of garbage outputs than by using TKS gate, also the power consumption is less in terms of quantum cost while using FRG gates.

The simulation results of 8 bit reversible CSA is shown in Fig. 6.Here, the input is given and the corresponding sum and carry is obtained.

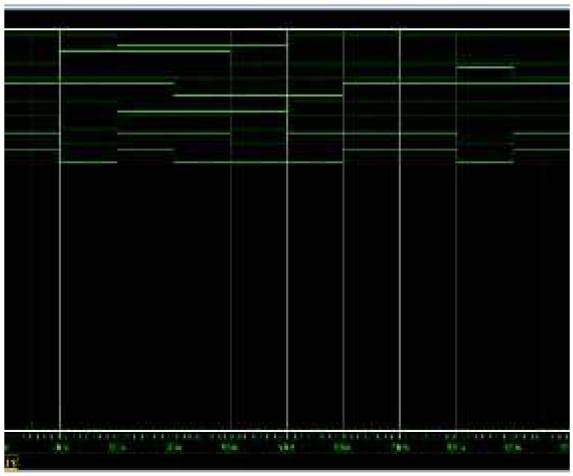

Fig. 6. Simulation Result of CSA using MTSG gates

The input is given for y as 10101110, sign as 1, reset as 1 and the clock. The corresponding outputs obtained for the sum is 01010001 and the carry is 00000000. Then the reset is changed to 0 and all other inputs are same then the corresponding outputs are the sum is 10101110 and the carry is 01010001. The internal signals are s, c and l. For the input 10101110, the output of the internal signals is s is 10011010, c is 01000001 and l is 11001011.

The comparison results of different reversible CSA is shown in Table II.

TABLE II

COMPARISON RESULTS OF DIFFERENT REVERSIBE CSA

S.NO	VARIABLE	TKS GATE	FRG GATE
1	Total Number of reversible Gates used	9	8
2	Total number of garbage outputs	18	8
3	Quantum Cost	9*13=117	8*5=40

From the Table II, it is clear that MTSG takes less power than TSG gates.

The simulation results of 8 bit reversible PIPO shift register is shown in Fig. 7.

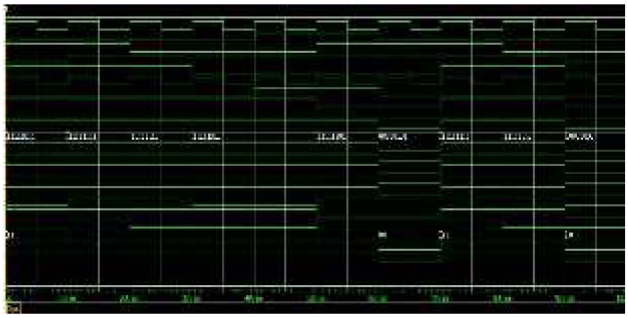

Fig. 7. Simulation Result of PIPO Shift Register

The simulation result of reversible Montgomery Multiplier is shown in Fig. 8.

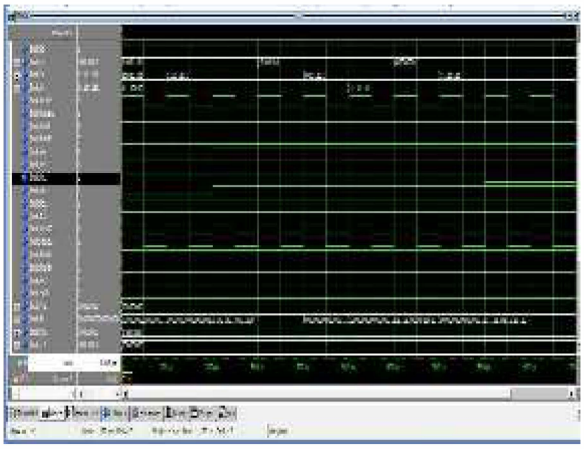

Fig. 8. Simulation Result of Reversible Montgomery Multiplier

The proposed multiplier have,

- 8 bit CSAs requiring 8 MTSG gates, 16 garbage outputs, 48 quantum cost.
- Two 8 bit Peres gates to compute AND-1 and AND-2 blocks, producing 16 garbage outputs, 64 quantum cost.
- Two 8 bit reversible multiplexers, requiring 16 Fredkin gates, 16 garbage outputs, 80 quantum cost
- Two 8 bit reversible PIPO shift registers, requiring 80 gates, 48 garbage outputs, 288 quantum cost
- Two 8-bit registers, requiring 32 gates, 18 garbage outputs, 96 quantum cost
- Two Fredkin gates for selections, producing 4 garbage outputs with 10 quantum cost
- 16 Feynman gates to construct two COPY blocks, requiring quantum cost of 16.

VI. CONCLUSION

An efficient Montgomery Multiplier was designed using reversible gates which reduces the consumption of power in hardware cryptographic systems. The proposed system requires less area and it is more cost effective than the exixting systems. It has been found that the proposed architecture uses 170 gates, 124 garbage outputs produced and requiring 602 quantum cost, where as in existing system 224 gates used, 192 garbage outputs produced and required 730 quantum cost. Because of using gated clock design technique, the power consumption of Montgomery multiplier were reduced interms of quantum cost. In future this multiplier is incorporated on hardware cryptography systems especially in RSA.

REFERENCES

[1] Shiann-Rong Kuang, Jiun-Ping Wang, Kai-Cheng Chang, and Huan-Wei Hsu, "Energy-Efficient High-Throughput Montgomery Modular Multipliers for RSA Cryptosystems," *IEEE Trans on VLSISystems*, Vol. 21, No. 11, pp. 1999-2009,2013.

[2] Laszlo Hars, "Long Modular Multiplication for Cryptographic Applications", *Springer journal of Computer Science*, Volume3156, 2004, pp 45-61

[3] G. A. V. Rama Chandra Rao, P. V. Lakshmi, and N. Ravi Shankar, "A New Modular Multiplication Method in Public Key Cryptosystem," *International Journal ofNetwork Security,* Vol. 15, No. 1, pp. 23-27,Jan. 2013.

[4] Satyanarayana Vollala, V. V. Varadhan, K. Geetha, and N.Ramasubramanian, "Efficient Modular Multiplication Algorithms for Public Key Cryptography," *IEEEInternational Advance Computing Conference (IACC*), pp. 74-78, 2014.

[5] Mahammad S.N, Veelinathan K, "Constructing Online Testable Circuits Using Reversible Logic,"*IEEE Trans. onInstrumentation and Measurements,* Vol.59, Issue: 1, pp. 101 – 109, Jan 2013.

[6] Himanshu Thapliyaland Mark Zwolinski "Reversible Logic to Cryptographic Hardware: A New Paradigm," *IEEE Midwestsymposium on Circuits and Systems*, Vol. 1,pp. 342-346, 2006.

[7] Laszlo Hars, "Long Modular Multiplication for Cryptographic Applications*", Springer journal of Computer Scienc*e, vol 3156, pp 45-61, 2004.

[8] Pallav Gupta, Abhinav Agrawal, et.al, "An Algorithm for Synthesis of Reversible Logic Circuits", *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 25, No. 11, Nov. 2006.

[9] Raghava Garipelly, P.Madhu Kiran, and A.Santhosh Kumar, "A Review on Reversible Logic Gates and their Implementation,"*International Journal of Emerging Technology and Advanced Engineering*, vol. 3, pp. 417-423, March 2013.

[10] Knezevic M., Vercauteen F and Verbauwhede I., "Faster Interleaved Modular Multiplication Based on Barrett and Montgomery Reduction Methods*", IEEE Transactions on Computers*, vol. 59, No. 12, Feb. 2010.

[11] Rashmi S.B, Umarani T.G., et.al "Optimized Reversible Montgomery Multiplier", *IJCSIC*, vol.2,pp.701-706, 2011.

[12] Richa Garg, Renu Vig "An effiecient Montgomery multiplication algorithm & RSA cryptographic processor", *International conference on Computational Intelligence & Multimedia application*, vol.4, pp. 123-128, 2007.