ISSN:0975-9646

Optimized Reversible Montgomery Multiplier

Rashmi S.B., Umarani T.G. and Shreedhar H. K
Department of Electronics and Communication,
Sri Bhagawan Mahaveer Jain College of Engineering (SBMJCE, JU),
Ramanagara District-562112, Karnataka, India

Abstract— **Reversible computation is of the growing interests to power minimization which has applications in low power CMOS design, quantum computing, optical information processing, DNA computing, bioinformatics and nanotechnology. The major component of any computing device is ALU. In order to design the reversible ALU of a crypto-processor, a high speed multiplier such as Montgomery multiplier is used. This multiplier requires efficient sequential circuits such as reversible registers, shift registers and reversible carry save adder (CSA). In this paper four to two CSA is designed using proposed reversible FAG gate and reversible sequential circuits are designed using reversible DFG gate. This will provide a starting point for developing cryptosystems secured against DPA attacks. This paper presents a better design when compared with the existing ones in terms of number of gates and number of garbage outputs.**

Keywords- ALU; Carry save adder; Montgomery multiplier; Reversible D flip flop; Shift register.

I. INTRODUCTION

Power analysis is a physical attack to cryptosystems. It exploits the fact that the power dissipation of an electronic circuit depends on the actions performed in it. Kocher et al. [16] describe Simple Power Analysis (SPA) and Differential Power Analysis (DPA) attacks which use the power-dissipation characteristics as a provider of side-channel information. Using DPA, an attacker can extract information on secret keys by statistically analyzing power consumption measurements from multiple cryptographic operations performed by a crypto processor.

DPA is more difficult to prevent, since even small biases in the power consumption can lead to exploitable weaknesses [12, 14]. In this study, the authors propose the use of reversible logic to protect the crypto-systems from power analysis attacks. According to Landauer[13,18], in logic computation every bit of information loss generates kT ln2 joules of heat energy where k is Boltzmann's constant of 1.38×10^{23} J/K and T is the absolute temperature in degree kelvin. At room temperature, the dissipated heat is around 2.9×10^{21}J. Energy loss due to Landauer limit is also important as it is likely that the increase of heat generation causing information loss will be noticeable in future. In reversible logic, no information is lost. Bennett [1] showed that zero energy dissipation would be possible if the network consists of reversible gates only. Thus the proposed reversible hardware will prevent any type of power analysis attack, since no energy will be dissipated from reversible circuits.

Modular multiplication is the most common operation in the cryptosystems, such as RSA, Elliptic Curve Cryptography (ECC), Digital Signature Algorithm (DSA) and Diffie-Hellman key exchange. It is also the critical part of the computing efficiency in the cryptosystem which involves modular multiplications with large integers for enhancing its security [21]. The most popularly used method for the implementations of fast modular multiplication is Montgomery's algorithm [2, 17]. To avoid long carry propagation during the addition stages of the computation, several techniques such as systolic array and Carry Save Adder (CSA) architecture were found in the literature [21]. This paper proposes four-to-two carry save adders (CSA) using the proposed reversible FAG gate. Furthermore, a reversible Montgomery multiplier [20] using the proposed reversible adders is shown. The major requirement for a Montgomery multiplier is the design of reversible sequential components, thus the authors have also proposed the reversible sequential components like latch, flip flop, register and shift register. The proposed reversible circuits form the primitive components of the ALU of a reversible crypto-processor.

II. REVERSIBLE LOGIC GATES

A logic gate *L* is reversible if, for any output *y*, there is a unique input x and same inputs(x) are obtained back when output(y) is applied to the gate L, as illustrated in eq. (1) and (2)

$$L(x) = y \tag{1}$$

$$L(y) = x \tag{2}$$

A. Optimization issues

For the synthesis of any reversible logic circuits, the under mentioned points are the major concerns.

- The number of outputs of a reversible logic gate should be equal to the number of inputs.
- The output of the gate that is not used as a primary output or as input to other gate is called garbage outputs. A heavy price is paid for every garbage outputs.
- The number of constant input to the gate should be as minimum as possible.
- In reversible logic, fan-out of more than one is not allowed; every output can be used only once [19].

B. Existing Reversible gates as full adder

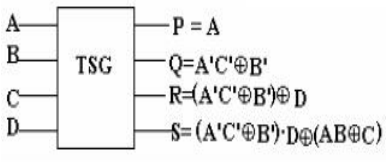

Figure 1. 4x4 TSG gate

A 4x4 one through reversible gate called a TS gate or "TSG" was proposed [4, 6, 7, 8 and 9]. The term one through means that one of the inputs is directly passed as output. The reversible TSG gate is shown in Fig. 1. It can be verified that the input pattern to generate a particular output pattern can be uniquely determined.

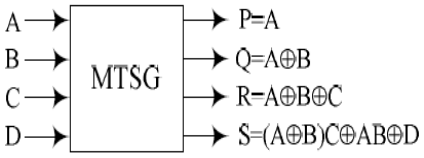

Figure 2. MTSG gate

The block diagram and corresponding functionalities of MTSG is as depicted in Fig 2. As TSG gate is very complex to design a full adder , MTSG gate was proposed [15].

C. Proposed full adder gate

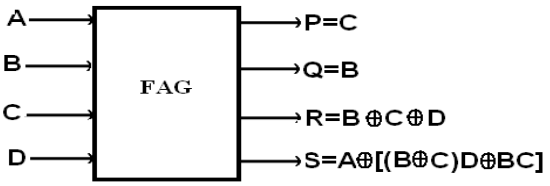

Figure 3. Proposed full adder gate

TABLE I. TRUTH TABLE OF THE PROPOSED GATE

A	B	C	D		P	Q	R	S
0	0	0	0		0	0	0	0
0	0	0	1		0	0	1	0
0	0	1	0		1	0	1	0
0	0	1	1		1	0	0	1
0	1	0	0		0	1	1	0
0	1	0	1		0	1	0	1
0	1	1	0		1	1	0	1
0	1	1	1		1	1	1	1
1	0	0	0		0	0	0	1
1	0	0	1		0	0	1	1
1	0	1	0		1	0	1	1
1	0	1	1		1	0	0	0
1	1	0	0		0	1	1	1
1	1	0	1		0	1	0	0
1	1	1	0		1	1	0	0
1	1	1	1		1	1	1	0

A 4x4 two through reversible gate called FAG gate is proposed. The term two through means that two of the inputs is directly passed as output. Fig. 3 shows the block diagram and corresponding functionality of the proposed FAG gate. The input pattern corresponding to a particular output pattern can be uniquely determined as depicted in Table I.FAG acts as 1 bit full adder when control input A is equal to zero.

Hardware Complexity: One of the main factors of a gate is its hardware complexity. It can be proved that proposed reversible FAG gate better than the existing counterparts in terms of hardware complexity.

Let

α = Two input EX-OR Gate Calculation

β = Two input AND Gate Calculation

δ = NOT Gate Calculation

T = Total Gate Calculation

TABLE II. COMPARATIVE EXPERIMENTAL RESULTS OF DIFFERENT REVERSIBLE FULL ADDER GATE

Reversible Full Adder Gate	Two Input EX-OR Gate Calculation (α)	Two Input AND Gate Calculation (β)	NOT Gate Calculation (δ)	Total Gate Calculation (T)
Proposed gate	5	2	0	5α+2 β
MTSG[15]	6	2	0	6 α +2β
TSG[4]	6	3	3	6α+3β+3 δ

Thus proposed FAG gate has minimum Total Gate calculation

III. REVERSIBLE LOGIC IN HARDWARE CRYPTOGRAPHY

The main source of power consumption in hardware cryptography is the ALU of a crypto-processor. It consists of Carry Save Adder (CSA) [10], multipliers, registers, shift registers, accumulators and multiplexers. Therefore, the ALU of a crypto-processor can be designed using reversible logic so the power dissipation is ideally zero. Each component of the crypto-processor is described here.

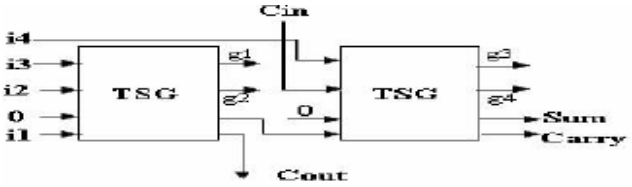

Figure 4. Existing reversible four to two CSA[5]

Fig. 4 and 5 show reversible designs for four-to-two CSA using TSG and MTSG respectively. The reversible CSA circuits are needed for zero power dissipating Montgomery [5] modulo multiplier.

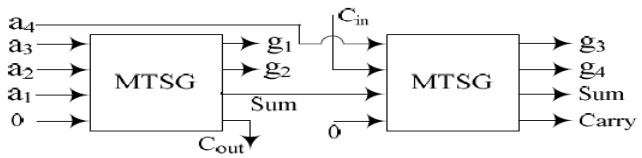

Figure 5. Existing reversible four to two CSA[15]

Fig. 6 shows the reversible four to two CSA using proposed FAG gate. In this design, hardware complexity has been reduced by maintaining garbage and gate count.

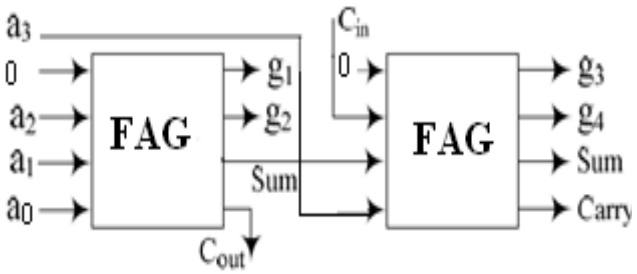

Figure 6. Proposed reversible four to two CSA

In addition to CSA adders, reversible sequential components like registers and shift registers are also required for the implementation of reversible Montgomery multiplier. Design of reversible sequential circuits is also proposed in this paper.

IV. PROPOSED REVERSIBLE SEQUENTIAL CIRCUITS

A. D latch

Fig.7 shows a conventional D latch. The characteristic equation of the D latch can be written as

$$Q^{+}=D.CP+CP'.Q$$

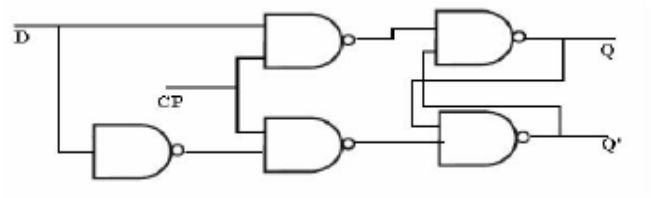

Figure 7. Conventional D latch

The characteristic equation of the D latch can be mapped onto the Fredkin gate (F). Fig. 8 shows the realization of the existing reversible D latch [11]. To avoid a fan-out problem, a Feynman gate (FG) [3] is used to copy the output.

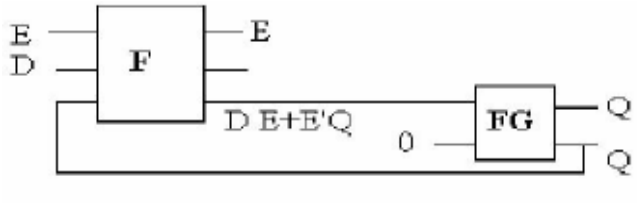

Figure 8. Existing reversible D latch

Fig. 9 shows the block diagram and corresponding functionality of the proposed DF Gate. The input pattern corresponding to a particular output pattern can be uniquely determined as depicted in Table III. It can be seen that the proposed reversible D latch is highly optimized in terms of the number of reversible gates and garbage outputs.

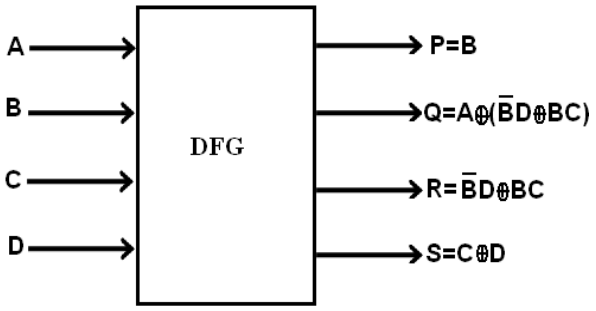

Figure 9. Proposed DFG

TABLE III. TRUTH TABLE OF DFG

A	B	C	D		P	Q	R	S
0	0	0	0		0	0	0	0
0	0	0	1		0	1	1	1
0	0	1	0		0	0	0	1
0	0	1	1		0	1	1	0
0	1	0	0		1	0	0	0
0	1	0	1		1	0	0	1
0	1	1	0		1	1	1	1
0	1	1	1		1	1	1	0
1	0	0	0		0	1	0	0
1	0	0	1		0	0	1	1
1	0	1	0		0	1	0	1
1	0	1	1		0	0	1	0
1	1	0	0		1	1	0	0
1	1	0	1		1	1	0	1
1	1	1	0		1	0	1	1
1	1	1	1		1	0	1	0

Fig. 10 shows DFG as 1 bit D latch. When control input A is equal to zero, clock input is directly passed to the output P. Outputs Q and R are same and equal to Q_{n+1}, where Q acts as present stage output and R is fed back to the input.

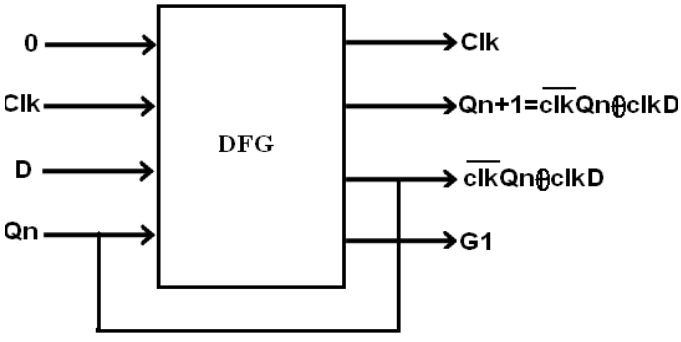

Figure 10. DFG as 1 bit D latch when A is 0

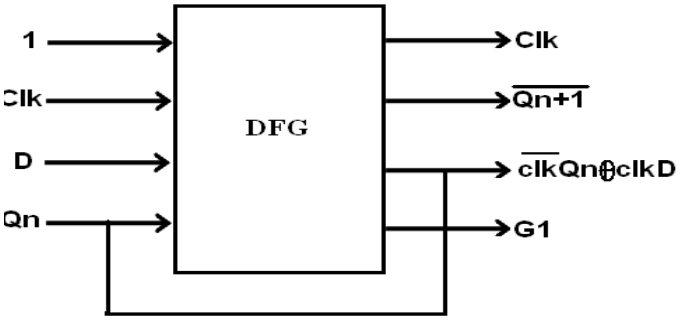

Figure 11. DFG as 1 bit D latch when A is 1

Fig. 11 shows DFG as 1 bit D latch with A is equal to one, Here clock input is directly passed to the output P. Output Q is equal to Q_{n+1}' and R is Q_{n+1} which is fed back to the input. Table IV shows the states of output Q and R for different value of control input.

TABLE IV. Q AND R OUTPUTS FOR DIFFERENT CONTROL INPUTS IN DFG

Control input A	Output Q	Output R
0	Qn+1	Qn+1
1	Qn+1'	Qn+1

The reversible D latch is used to implement more complex reversible sequential circuits. Fig. 12 shows a reversible storage register [5] constructed from four reversible D latches and a common clock input. Fig. 13 shows the existing reversible n-bit register [15] constructed using D flip flop. To construct n-bit reversible register, 2n gate count, n constant inputs are required and n+1 garbage outputs are produced.

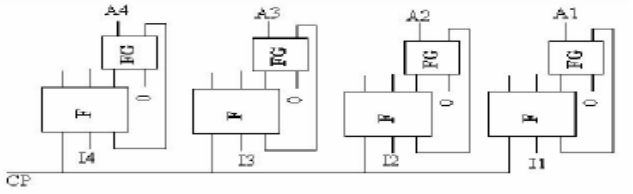

Figure 12. Existing 4 bit reversible register

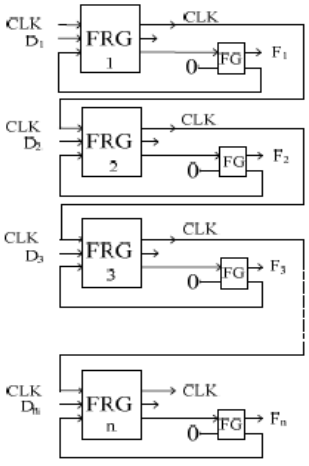

Figure 13. Existing nbit reversible register

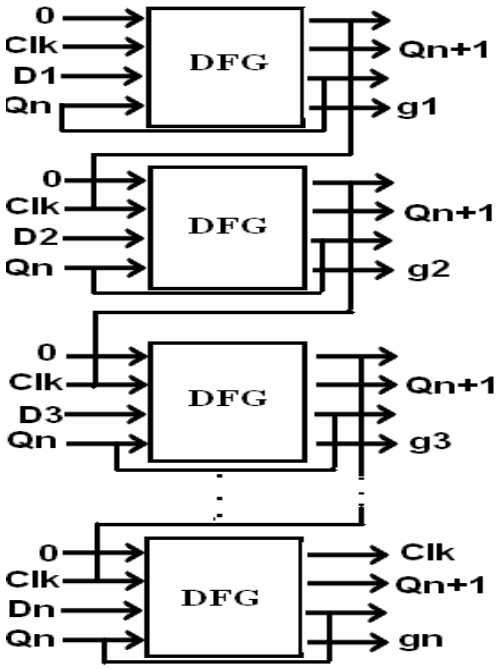

Figure 14. Proposed n bit reversible register

Fig. 14 shows the proposed n-bit reversible register, which requires gate count of n, n constant inputs and n+1 garbage bits. The comparative study of existing and proposed n-bit reversible register in terms of gate count and garbage outputs are depicted in table V

TABLE V. COMPARISION TABLE FOR N BIT REVERSIBLE REGISTER

	No. of gates	Garbage output
Existing circuit[5]	2n	2n
Existing circuit[15]	2n	n+1
Proposed circuit	n	n+1

A master-slave flip-flop is normally constructed from two flip-flops; one is the Master flip-flop and the other is Slave. In addition to these two flip-flops, the circuit also includes an inverter. Inverter is connected to clock pulse in such a way that the inverted clk is given to the slave flip-flop. For example, if the clk=0 for a master flip-flop, then the output of the inverter is 1, and this value is assigned to the slave flip-flop. In other words if clk=0 for a master flip-flop, then clk=1 for a slave flip-flop.

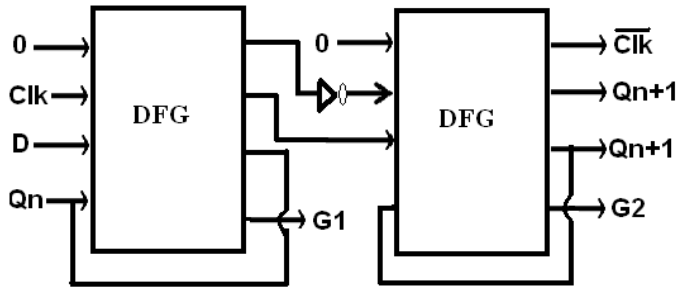

Figure 15. Reversible master-slave D flip-flop

A master-slave flip flop can be constructed using any type of flip-flop which forms a combination with a clocked D flip-flop, and with an inverter as slave circuit. Fig. 15 shows the master-slave D flip flop designed from the proposed D Latch. Fig. 16 shows the block diagram of reversible MS D flip-flop.

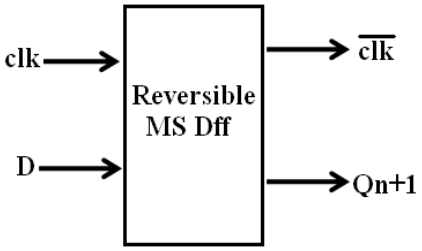

Figure 16. Block diagram of reversible MS D flip-flop

The shift register is one of the most extensively used functional devices in digital systems. A shift register consists of a group of flip-flops connected together so that information bits can be shifted one position to either right or left depending on the design of the device. SISO shift register is presented in this section.

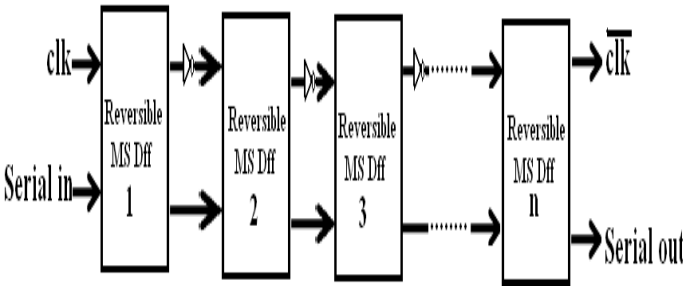

Figure 17. Proposed reversible n-bit SISO shift register

SISO shift register is the simplest shift register that contains only flip-flops. In right shift register, output of a given flip-flop is connected to the data input of the next flip-flop at its right. Each clock pulse shifts the contents of the register one bit position to the right. The serial input is provided to the leftmost flip-flop and the serial output is the output of the rightmost one. Fig. 17 shows the proposed n-bit reversible SISO shift register built from n reversible clocked D flip-flops.

V. Reversible Montgomery Multiplier

Montgomery multiplication is simple and fast utilizing right to left divisions. There are no problems with carries or with estimating the quotient digits. Therefore no correction steps are necessary. The Montgomery multiplication calculates product in "row order", but it still take advantage of speed up for squaring.

Fig. 18 shows the reversible implementation of the Montgomery multiplier using the reversible components shown in this paper. Here the first reversible CSA performs S, C: = S + C + X_i*Y; the S, C produced are stored in proposed reversible registers S and C. The LSB S_o of the reversible register S is multiplied with M to generate S_o * M. After its generation, the second CSA performs S, C: = S + C + S_o*M. The S, C thus generated are passed to the reversible shift registers to produce S div 2 and C div 2. The other components required in the multiplier such as for (P: = S + C and if P > M then P: = P - M) can also be designed using reversible logic.

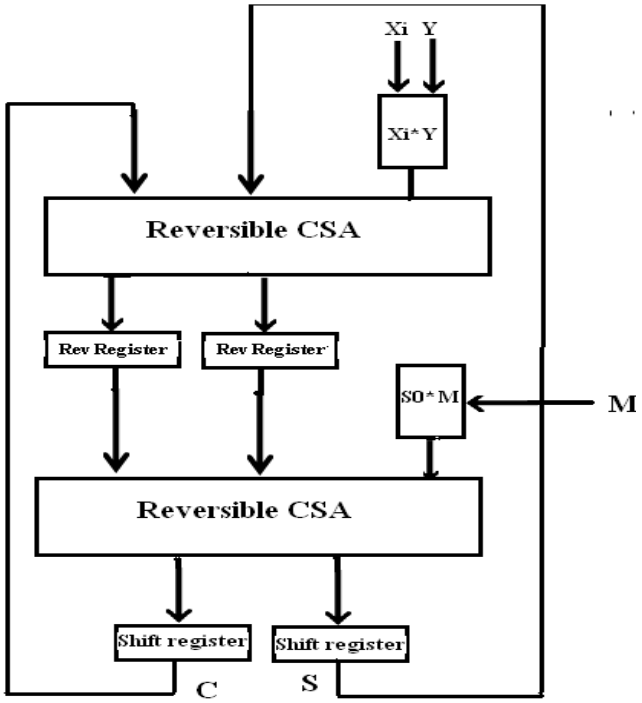

Figure 18. Architecture of Montgomery multiplier

VI. Conclusion

In crypto processors modular multiplication is one of the very important tasks. The paper proposes reversible CSA and reversible sequential circuits which require minimum hardware. The design of reversible Montgomery multiplier using the proposed sequential circuits and reversible CSA requires less hardware and it is faster. The proposed reversible design is better than the existing ones in terms of number of gates needed and number of garbage outputs produced.

Acknowledgment

The authors would like to thank the management of Sri Bhagawan Mahaveer Jain College of Engineering, Jain University, Bangalore for their Constant support, valuable guidance and encouragement in undertaking the research work.

References

[1] C.H. Bennett, "Logical Reversibility of Computation", IBM J. Research and Development, pp. 525-532, November 1973.

[2] C. Mclvor, M. McLoone and J.V. McCanny, "Modified Montgomery modular multiplication and RSA exponentiation techniques", IEE Proc.-Comput. Digit. Tech., Vol. 151, No. 6, November 2004.

[3] E. Fredkin, T Toffoli, "Conservative Logic", International Journal of Theor. Physics, 21(1982),pp.219-253.

[4] H. Thapliyal and M.B Srinivas, "Novel Reversible "TSG" Gate and Its Application for Designing Reversible Carry Look Ahead Adder and Other Adder Architectures", Tenth Asia-Pacific Computer Systems Architecture Conference (ACSAC05), Singapore, October 24 - 26, 2005, pp. 805-817.

[5] H.Thapliyal, and M. Zwolinski, 2006. "Reversible logic to cryptographic hardware: a new paradigm". Proceedings of the 49th IEEE International Midwest Symposium on Circuits and Systems (MWSCAS '06), Aug. 6-9, Puerto Rico, 1: 342- 346, doi: 10.1109/MWSCAS.2006.382067."

[6] H. Thapliyal and M.B Srinivas, "A New Reversible TSG Gate and Its Application For Designing Efficient Adder Circuits", 7th International Symposium on Representations and Methodology of Future Computing Technologies(RM 2005), Tokyo, Japan,September 5-6, 2005.

[7] H. Thapliyal and M.B Srinivas, "Novel Reversible "TSG" Gate and Its Applications for Designing Components of Primitive Reversible/Quantum ALU", Fifth IEEE International Conference on Information, Communications and Signal Processing (ICICS 2005),Bangkok, Thailand, 6-9 December 2005.

[8] H. Thapliyal, S. Kotiyal and M.B Srinivas, "Novel BCD Adders and their Reversible Logic Implementation for IEEE 754r Format", 19th International Conference on VLSI Design and 5th International Conference on Embedded Systems (VLSI Design 2006), Hyderabad, India, Jan 4-7, 2006,pp. 387-392.

[9] H. Thapliyal and M.B Srinivas, "An extension of Fredkin gate circuits using DNA: reversible logic synthesis of sequential circuits using Fredkin gate", SPIE International Symposium on Optomechatronic Technologies, Sapporo, Japan, December 5-7, 2005, pp. 196-202.

[10] H. Thapliyal and M.B Srinivas et.al, "Modified Montgomery modular multiplication Using 4:2 Compressor And CSA Adder", Third IEEE International Workshop on Electronic Design, Test and Applications (DELTA'06), Kuala Lumpur, Jan 17-19, 2006,pp. 414-417

[11] H. Thapliyal, M.B Srinivas and M. Zwolinski, "A Beginning in the Reversible Logic Synthesis of Sequential Circuits", 8th MAPLD Conference(NASA office of Logic Design), Washington D.C, Sep 2005.

[12] K. Tiri and I. Verbauwhede, "A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation", 2004, pp. 246-251.

[13] Keyes, R. and R. Landauer, 1970. Minimal energy dissipation in logic.IBMJ.Res.Develop.14152157, http://www.research.ibm.com/journal/rd/142/I bmrd1402H.pdf

[14] M. P Frank, "Introduction to reversible computing: motivation,progress,and challenges", Proceedings of the 2nd Conference on Computing Fron-tiers, 2005, pages 385-390P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis", Lecture Notes in Comp. Sci., 1666:388-397, Jan. 1999.

[15] Noor Muhammed Nayeem, Lafifa Jamal and Hafiz Md. Hasan Babu" Efficient Reversible Montgomery Multiplier and Its Application to Hardware Cryptography" Journal of Computer Science 5 (1): 49-56, 2009

[16] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis", Lecture Notes in Comp. Sci., 1666:388-397, Jan. 1999.

[17] P.L. Montgomery, "Modular Multiplication without Trial Division",Math. Comput., 1985, 44, pp. 519-521.

[18] R. Landauer, "Irreversibility and Heat Generation in the Computational Process", IBM Journal of Research and Development, 5, pp. 183-191, 1961.

[19] Robert Wille, Rolf Drechsler "Towards a Design Flow for Reversible Logic", (9-13).

[20] S. B. Ors et.al , "Hardware implementation of a Montgomery modular multiplier in a systolic array", The 10th Reconfigurable Architectures Workshop (RAW),Nice, France, April 22 2003

[21] Zhang, Y.Y., Z. Li, L. Yang and S.W. Zhang,2007. An efficient CSA architecture for montgomery modular multiplication. Microprocess. Microsyst., 31(7): 456-459, doi:10.1016/j.micpro.2006.12.003.