ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Design of Reversible LFSR for Its Application in Cryptography

G.Surekha
M.Tech,
Dr.K.V.Subba Reddy Institute of Technology.

J.Naveen Kumar, M.Tech
Assistant Professor,
Dr.K.V.Subba Reddy Institute of Technology.

Abstract:
Reversible logic has emerged as an alternate design technique to the conventional logic, resulting in lower power consumption and lesser circuit area. Comparators are a key element in most digital systems.One-to-one mapping from input to output is the necessary condition for a reversible computational model transiting from one state of abstract machine to another. Probably, the biggest motivation to study reversible technologies is that, it is considered to be the best effective way to enhance the energy efficiency than the conventional models. The research on reversibility has shown greater impact to have enormous applications in emerging technologies such as Quantum Computing, QCA, Nanotechnology and Low Power VLSI. In this paper, we have realized novel reversible architecture of Linear Feedback Shift Register (LFSR) and Parallel Signature Analyzer (PSA) and have explored these in terms of delay, quantum cost and garbage. While approaching for LFSR, we have shown new reversible realization of Serial Input Serial Output (SISO) and Serial Input Parallel Output (SIPO) registers up to N-bit and analyzed their delay, quantum cost & garbage in terms of some lemmas, which will outperform the existing designs available in literature.

Keywords:
Reversible Logic; SISO; SIPO; Reversible LFSR; Reversible PSA.

I.INTRODUCTION

The power dissipation of devices is increasing with the technological advancement day-by-day, thereby making it the major limitation of technology. Reversible logic gates due to its ability to reduce power dissipation attracted researcher's attention. Irreversible gates produce energy loss due to the information bits lost during computation process. Information loss occurs due to less no. of generated output signals than what is applied. According to R. Landauer's principle[1], given in 1961, irreversible logic gates dissipates KTln2 joules of energy for the loss of 1-bit information, where K is the Boltzmann constant and T is the absolute temperature at which operation is performed which means that the power dissipation is directly proportional to the number of information bit loss. Charles Bennet, in 1973 [2], proposed that, to avoid heat dissipation, logic circuit must be built from reversible circuit since there no information loss occurs. At first, in the design of reversible logic circuits, design was limited to combinational logic circuits and it was just because of the convention that the feedback is not allowed in the reversible computing [19]. But, in 1980, Toffoli [4] has shown that the feedback is allowed in reversible computing.

According to Toffoli [11], a sequential network is reversible if its combinational part is reversible. The recent works focus on optimizing the reversible sequential designs in terms of number of reversible gates and garbage outputs. The shift registers are the most exhaustively used functional devices in digital system design for multiple bits storing & shifting of the same if required. In this paper, we are presenting reversible realization of two shift registers naming Serial-in Serial-out and Serial-in Parallel-out for their application in designing sequence pulse generator. We will also present novel reversible architecture of Linear Feedback Shift Register (LFSR) and Parallel Signal Analyzer (PSA). In computing, the input bit of LFSR is a linear function of its last state. The starting value of the LFSR is termed seed, and due to the deterministic operation of the register, the bit stream

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

produced is completely determined by its current (or previous) state.

II. RELATED WORK:

The concept of a reversible memory cell was first shown by Fredkin and Toffoli [5], in 1982, where, design of a JK latch was introduced. Later, in 1996, Picton [7] developed a design of clock less SR-latch using two crosscoupled NOR gate, where NOR gates were designed from Fredkin gate. All the reversible latches such as D-Latch, Tlatch etc. along with their flip-flop and master-slave configuration were introduced for the first time in 2005 by Thapliyal et.al.[9]. In 2006, Rice [10] introduced a SR-latch without fan-out problem available in the design by Picton and subsequently designed other latches from SR. In 2007, Thapliyal and Vinod [11] proposed a better design of reversible flip-flops than by Rice in terms of number of reversible gates being used and garbage outputs.

A more detailed analysis of SR-latch was presented by Rice [12] in 2008. A better design of all reversible latches (except SRlatch) along with their flip-flops than that of Thapliyal 2015 2nd International Conference on Signal Processing and Integrated Networks (SPIN) 978-1-4799-5991-4/15/$31.00 ©2015 IEEE 601 (2005) and Rice (2006) were presented by Chuang and Wang [13]. Morita (2008) [14] gave a brief note on how a universal reversible computer could be made from reversible logic elements and reversible sequential circuits, but no practical hardware design was presented.

This gave a direction of making RAM as it is the fundamental storage for computer system. In 2009, Hafiz [15] presented a novel design of reversible FPGA. In 2011, Morrison [16] designed a static and dynamic RAM arrays with reversible logic. In this work, we have developed novel architecture of Shift Registers to have a reversible operation on LFSR with reduced quantum cost and minimum delay.

III. BRIEF OVERVIEW OF REVERSIBLE GATES

The laws of physics are primarily reversible. If any physical process (f) relates input (x,y) and outputs (z) such that, Z = f (x, y), the laws of reversibility ensures that for any given output, z the inputs, x & y are deductible. But the classical computers violate this law of reversibility. For example, in an AND function, for output z = 0, the inputs cannot be exactly deducible as there 3 sets of inputs that make z = 0. We assume the followings to describe a generalized reversible gate:

i) Set of domain variable = {x1, x2, …..,xn}

ii) Set of controls = C & the no. of elements in C defines the width of gate

iii) A Target = T

There are some reversible basic gates which we are going to use in design of Registers and are as follows:

A. NOT Gate

NOT gate is a simple 1 input and 1 output (1*1) reversible logic gate which performs inversion of input. It has unit quantum cost and unit delay (i.e.Abar).

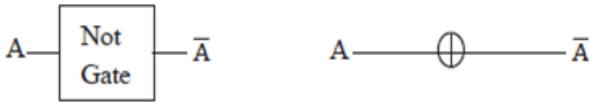


Fig.1. NOT gate and its quantum representation

B. Controlled-V and Controlled-V+ Gate

Controlled V and V+ are the basic gates. In the controlled-V gate when the control signal A = 0, then the input B on target line will pass through the controlled part unchanged, that is Q = B. When A = 1, then the unitary operation V is applied to the input B, and output will be

Q =V(B).

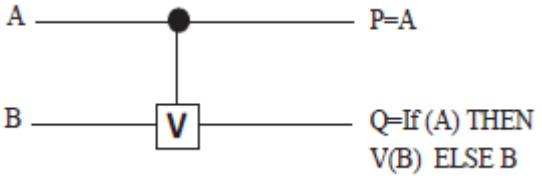


Fig.2. Quantum representation of Controlled-V

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

In the controlled-V+ 5.gate when the control signal A = 0, then the input B will pass through the controlled part unchanged, that is Q = B. When A = 1, then the unitary operation V+= V- 1 is applied to the input B, that is, Q = V+(B).

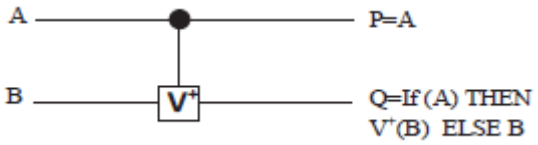


Fig.3. Quantum Representation of Controlled-V+

The V and V+ gates have the following properties:
V×V = NOT
V×V+ = V+×V = I
V+×V+ = NOT

C. Controlled-NOT Gate/ Feynman Gate

It is a 2*2 reversible logic gate. CNOT Gate, also known as FEYNMAN Gate and is used to overcome the fan-out problem since it can be used for copying the information. CNOT gate has unit quantum cost and unit delay.

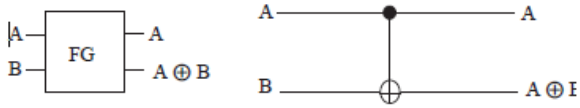


Fig.4. Feynman Gate & its Quantum representation

D. Toffoli Gate

Toffoli gate is a 3*3 reversible gate with quantum cost of 5 and delay of 5□. It is called also universal reversible gate.

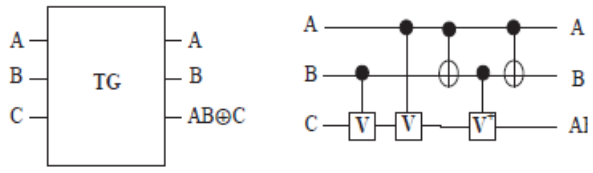


Fig.5. Toffoli gate and its Quantum representation

E. Fredkin Gate

Fredkin Gate is also a 3*3 gate. It has 5 quantum cost and delay is 5□.

When A = 0, the other two inputs B and C is simply copied to the output. But when A = 1, B and C is swapped in the output. Hence, it is also termed as a controlled swap gate. Basic logic function can be implemented using this gate and called universal reversible gate.

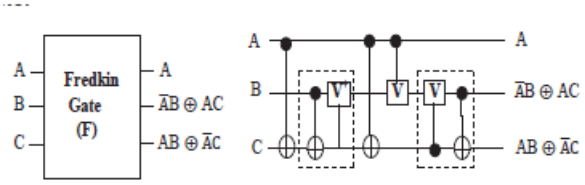


Fig.6. Fredkin Gate and its Quantum representation

F. Peres Gate

Peres gate is a 4-input and 4-output (4*4) reversible gate. It has a minimum quantum cost among the 4*4 reversible gate and is equal to 4 and delay is 4□. The following figure shows the Peres gate and its quantum representation.

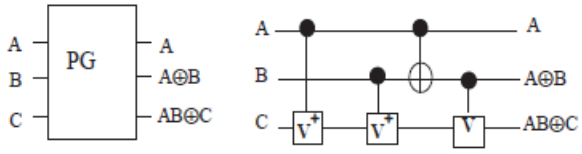


Fig7. Peres gate and its quantum representation

G. Proposed Modified Fredkin (MF) Gate

It is the proposed modified version of 3*3 Fredkin gate with a quantum cost of 4 and a delay of 4□. When A = 0, it does the same as Fredkin Gate, but when A = 1, B and complement of C is swapped in the output. Quantum representation of this gate is

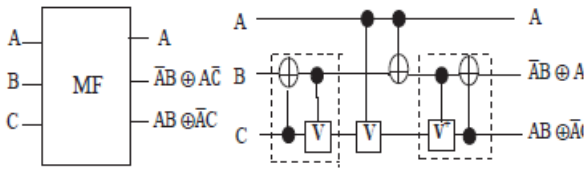


Fig8. MF gate and its Quantum representation

IV. REVERSIBLE SHIFT REGISTER

Flip-flops are the basic memory element used for storage of single bit data. To store more number of bits, combination of FF is used and called shift registers. Loading of data may be serial or parallel.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

In serial loading, data shifted from one FF to another in serial form, i.e. 1-bit at a time, upon triggering clock. In parallel loading, all data-bits appear in parallel form at a time upon triggering clock. In this section, we have proposed Serial-in Serial-out and Serial-in Parallelout shift registers. To design reversible shift register for Pulse generation we are using master-slave D-FF block diagram.

A. Reversible D-FF

Characteristic equation of reversible D-Latch can be written as Q+=D where output is equal to its input value. The characteristic equation of clock enabled reversible D-Latch (D-FF) can be written as

$$Q^{+}=D.E+\bar{E}.Q \qquad (1)$$

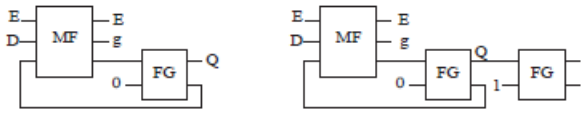


Fig 9. Clock enabled D-latch and D-FF with output Q and □

Figure 9 [22] shows the clock enable D-latch (QC = 5) where output Q+=D for E=1 and output Q+=Q for E=0 output remain in its previous state. For the input D=1 and Q=0, the output of MF gate when E=1 is Q+=1 which is applied to FG gate to provide feedback. The proposed Master-Slave configuration of D-FF is shown in figure 10.

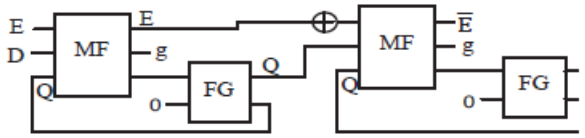


FIG10. MASTER SLAVE D-FF USING MF GATE

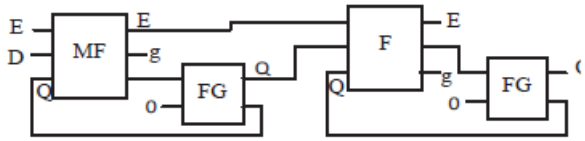


Fig.11. Master-slave D-FF using MF and F gate

Figure 10 shows the design of master slave D-FF using MF gate & Feynman gate. Since this design produce a clock inversion (i.e.) at the output of slave FF, to use clock pulse to the next FF in a shift register, we need to use NOT gate to convert □□ into E. Hence, to overcome this problem we proposed a new design shown in figure 11 replacing MF gate by Fredkin gate in Slave FF since Fredkin gate does not require clock inversion and produces clock pulse as what is applied to its input. This proposed design (i.e. figure 11), is used for Master-slave D-FF to realize registers.

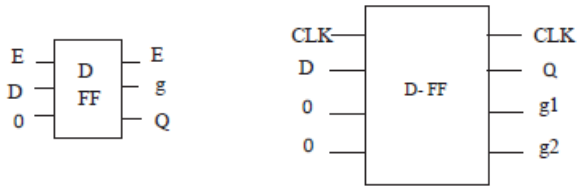


Fig12. Block diagram of D-FF and Master Slave D-FF

B. Proposed Reversible Serial-in Serial-out (SISO) Shift Register

Serial-in Serial-out shift register accepts data in serial form and produces output serially. For N-bit shift register it takes n-1 clock pulse to store data serially and n-clock pulse to generate output. The following figure 13 & 14 shows the reversible N-bit serial-in serial-out shift register for edge triggering & pulse triggering applications.

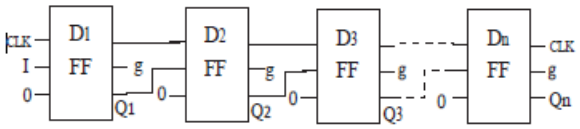


Fig13. Edge-triggered N-bit SISO registers using D-FF

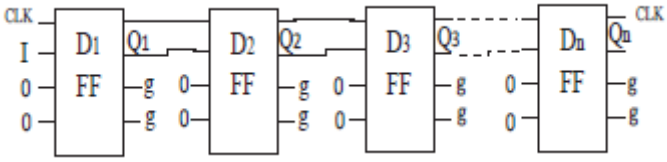


Fig14. Pulse-triggered N-bit SISO registers using master-slave D-FF

When serial data is applied, each new bit is entered into first FF upon application of each clock pulse. The bit that was previously stored by first FF transferred to second FF on application of second clock pulse and n-

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

1 FF bit transferred to n–bit FF on application of n-1 clock pulse. The bit that was stored by last FF, i.e. n-FF, is outputted on the application of n clock pulse. The proposed design of SISO is optimized in terms of Quantum cost, delay and garbage output.

TABLEI. A COMPARISON OF 4-BIT SISO SHIFT REGISTER

SISO	PARAMETERS		
	Quantum Cost Qc	*Delay D*	*Garbage G*
A.V.Ananthalakshmi 2013[23]	52	52	8
Proposed design for edge triggering	20	20	4
%improvement w.r.t [23]	62	62	50
Proposed design for pulse triggering	44	44	8
% improvement w.r.t. [23]	16	16	-

Lemma I: The minimum Quantum cost (Qc) and delay (D) of n-bit reversible Edge triggered SISO shift register is 5n.

Proof: For n-bit reversible SISO, it requires n-FF to store nbit data. From figure 13 we can observe that, n reversible DFF is used to store n-bit data. Since each reversible

D-FF has Qc of 5 and D of 5□, hence,

Qc/D = 5n

Lemma II: An n-bit reversible Edge triggered SISO shift register produces minimum garbage output (G) equal to n.

Proof: From figure 13 we can see that each reversible D flip-flop produces one garbage output. For n-bit reversible SISO shift register it require n-FF, hence, we can conclude that for n-bit SISO shift register total number of garbage output produced

G = n

C. Proposed Reversible Serial-in Parallel-out (SIPO) Shift Register

SIPO takes input data serially and the data stored in the register produces output in parallel form. Data input appears on register bit-by-bit basis whereas when data is stored in register then all output appears in their respective FF at a time.

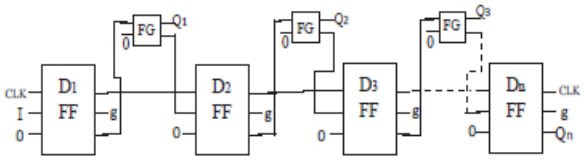


Fig.15. Edge-triggered N-bit SIPO registers using D-FF

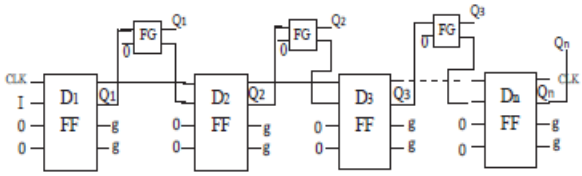


Fig.16. Pulse-triggered N-bit SISO registers using master-slave D-FF

It takes n-1 clock pulse to store data in register and 1 clock pulse to produce output. In the above figure15 data input is same as in SISO shift register and output appears as data, stored in shift register on a single clock pulse. This proposed design is also optimized in terms of quantum cost, delay and garbage outputs.

TABLE II. A COMPARISON OF 4-BIT REVERSIBLE SIPO SHIFT REGISTER

SIPO	PARAMETERS		
	Quantum Cost Qc	*Delay D*	*Garbage G*
A.V.Ananthalakshmi 2013[23]	52	52	8
Proposed design for edge triggering	23	23	4
%improvement w.r.t [23]	56	56	50
Proposed design for pulse triggering	47	47	8
% improvement w.r.t. [23]	10	10	-

Lemma III: The minimum quantum cost (Qc) and delay (D) of n-bit reversible Edge triggered SIPO shift register is equal to 6n-1.

Proof: From figure 15 we can observe that reversible SIPO shift register have D-FF (Qc=5 and D=5□) and Feynman gate (Qc=1 and D=□) for copying the output of each reversible D-FF except last FF. For n-bit reversible SIPO shift register it require n reversible D-FF and n-1 Feynman gate, hence, the total Qc and D for n-bit reversible SIPO shift register is

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Qc/D = 5n + n-1 = 6n-1

Lemma IV: An-bit reversible Edge triggered SIPO shift register produces minimum garbage output (G) equal to n.

Proof: From figure 15 we can observe that each flip-flop produces one garbage output. For 2-bit and 4-bit reversible shift register it will produce 1x2=2 and 1x4=4 garbage output respectively. Hence, we can conclude that for n-bit reversible SIPO shift register, the total garbage output is

G = n

V.PULSE GENERATION USING SHIFT REGISTER

In this section we are going to present an application of shift register in designing Pulse Generator. The basic structure of sequence pulse generator is shown in the following figure 17.

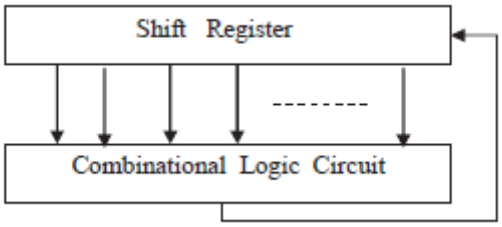


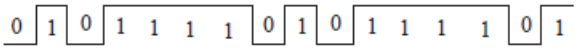
Fig17. Basic structure of sequence pulse generator

First input of reversible shift register is function of the output of all registers

I1= f (Q1, Q2, Q3…Qn)

In order to build reversible sequence generator capable of generating a sequence of length S, it is necessary to use at least n-FFs where S<= 2n-1.

Example: Consider, the following sequence pulse train



In the given pulse train 1011110, the Sequence of pulse train S=7; hence number of reversible FF required is 4. By this, unique states can be obtained using 4 FFs. From K-map of truth table of this pulse, we obtained the output of the combinational circuit in terms of the output of the FFs and is

$$f = \overline{Q4\ Q3\ Q1}.$$

Realization of this sequence generator using reversible logic gate is shown in the following figure

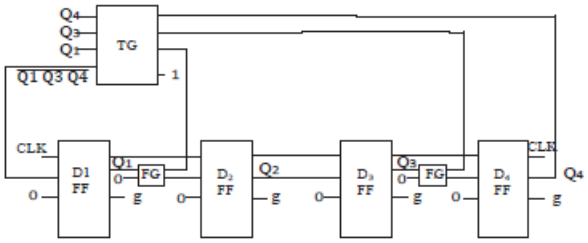


Fig18. Sequence pulse generator using SISO shift register and Toffoli gate

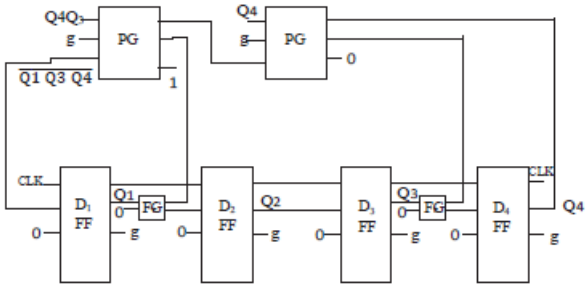


Fig19. Minimized form of Sequence pulse generator

The figure18 can be further minimized in terms of quantum cost using two Peres gate instead of using 4x4 Toffoli gate as Peres gate has a quantum cost of 4 whereas 4x4 Toffoli gate has a quantum cost of 13. The further minimized form of sequence generator is shown in figure 19.

VI.PROPOSED REVERSIBLE LFSR

Linear Feedback Shift Register (LFSR) is used to generate periodic sequence, but it does not produce all zero sequence until it starts from all zero. A LFSR can be constructed by doing exclusive-OR on the outputs of two or more of the FFs together and applying this output to one of the FFs. The figure20 shows the design of 3 bit reversible LFSR

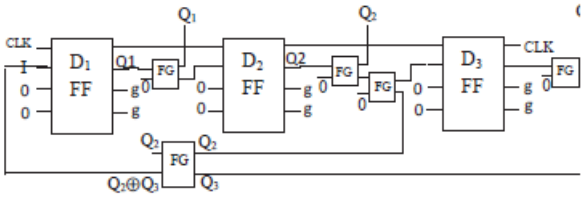


Fig20.Realization of pulse triggered reversible LFSR

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Feynman gate is used to operate exclusive-OR operation on feedback path whereas it is also used between any two FFs to copy the output. Q1, Q2 and Q3, at initial point of time should not start with all 0 otherwise, LFSR produces all 0 pattern output for every clock pulse applied. If the flip-flops are loaded with a seed value (anything except all 0s) and if the LFSR is triggered, it will generate a pseudorandom pattern of 1s and 0s. The pattern count of LFSR equals to 2n– 1, where n is the number of flip-flops. The patterns have an approximately equal number of 1's and 0's.

TABLE III.A 3-BIT REVERSIBLE LFSR PARAMETERS

LFSR	PARAMETERS		
	Quantum Cost Qc	*Delay D*	*Garbage G*
Proposed Design	38	38	7

VII. PROPOSED REVERSIBLE PSA

A LFSR of any length will produce huge number of patterns. To avoid having to check the outputs of severalhundred thousand or more vectors, a parallel signal analyzer (PSA) is used to minimize the number of data at the outputs of the Application Specific Integrated Circuit (ASIC). PSA is same as the LFSR with exclusive-OR gates between the flip-flops of shift register.

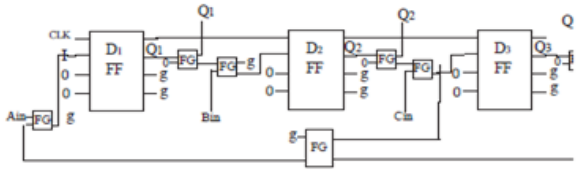


Fig21. Realization of 3 bit Reversible PSA

Figure 21 shows the diagram of Reversible PSA. PSA can be used as LFSR if the inputs Ain, Bin and Cin all held at 0, PSA will produce exactly the same bit pattern as LFSR. Inputs Ain, Bin, etc. are multiplexed with the outputs of ASIC. Each bit stream is applied through the LFSR to the ASIC inputs & the output of ASIC is read into the PSA.

As each new bit stream is applied, the PSA will perform an exclusive-OR of the last pattern's outputs with the current pattern's output to generate a new value in the PSA. This is quite similar to a calculator performing addition of a series of numbers. Instead of using addition, the PSA performs an exclusive-OR of the series of 1s and 0s together to get the new result. The value of quantum cost, delay and garbage is shown in table5. IV.

TABLEIV.A 3-BIT REVERSIBLE PSA PARAMETERS

LFSR	PARAMETERS		
	Quantum Cost Qc	*Delay D*	*Garbage G*
Proposed Design	40	40	9

VIII. SIMULATION RESULTS

All the synthesis and simulation results are performed using Verilog HDL. The synthesis and simulation are performed on Xilinx ISE 14.4. The simulation results are shown below figures.

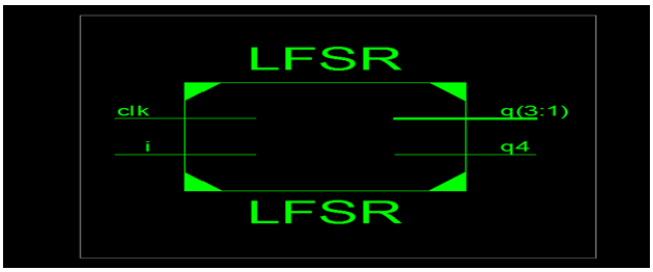


Fig 22.RTL schematic ofpulse triggered reversible LFSR

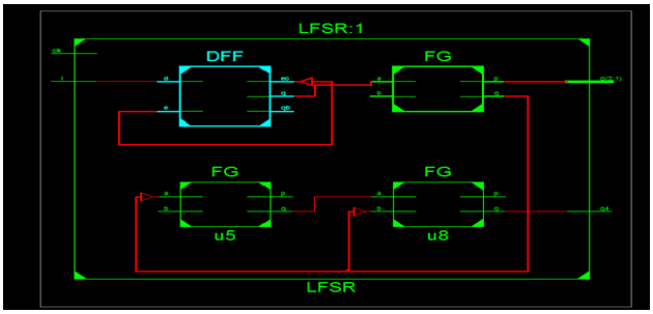


Fig 23.RTL sub schematic ofpulse triggered reversible LFSR

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

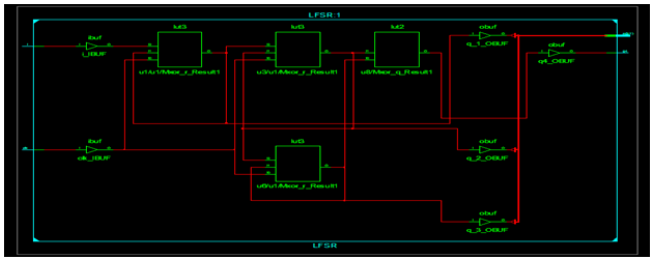


Fig 24.Technology schematic ofpulse triggered reversible LFSR

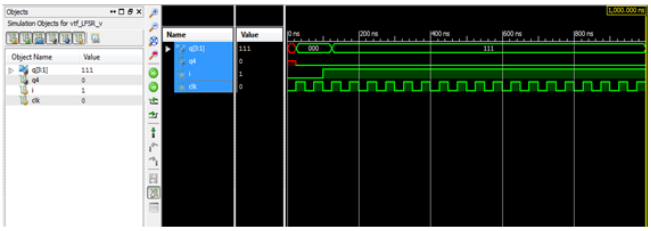


Fig 25.Simulation ofpulse triggered reversible LFSR

CONCLUSION AND FUTURE SCOPE

In this paper, we have demonstrated novel architecture of pulse triggered and edge triggered SISO & SIPO registers and analyzed their quantum cost, delay and garbage in terms of some lemmas. Using the registers we have shown an example of sequence pulse generation with minimized delay & cost. Lastly, we have realized reversible architecture of LFSR and PSA which can be used for random bit generation. Due to the ease in construction, the novel architecture of LFSR & PSA can be used in military cryptography. However, as the reversible LFSR is a linear system, it leads to most easy cryptanalysis. We are trying to simulate the demonstrated circuits in Xilinx using Verilog and will focus to design a reversible BIST for digital systems.

REFERENCES:

[1] R. Landauer, "Irreversibility and heat generation in the computational process", IBM Journal of Research.Dev. 5, 183-191, 1961.

[2]C. H. Bennett, R. Landauer, "The fundamentals physical limits of computation".

[3]C. H. Bennett, "Logical reversibility of computation", IBM Journal of Research. Devel.17,525-532, 1973.

[4]TommasoToffoli, "Reversible Computing," Automata, Languages and programming, 7th Colloquium of Lecture Notes in Computer Science, vol. 85, pp. 632-644,1980.

[5] E. Fredkin, T. Toffoli, "Conservative logic ", Int. J. Theor.Physics 21, 219-253, 1982.

[6]A. Peres, "Reversible logic and quantum computers", Phys. Rev. A, Gen. Phys. 32, 6, 3266-3276, 1985.

[7]P. Picton, "Multi-valued sequential logic design using Fredkin gates" MVL J. 1, 241-251, 1996.

[8]J. Smolin, D. divincenzo, "Five 2-bit quantum gates are sufficient to implement quantum Fredkin gate", Phys. Rev. A53, 2855-2856,1996.

[9]H. Thapliyal, M. B. Srinivas, M Zwolinski, A beginning in the reversible logic synthesis of sequential circuits.In proceedings of the Int. Conf. on the military & Aerospace Programmable Logic devices, 2005.

[10]J. Rice, "A new look at reversible memory elements", In proceedings of the International Symposium on circuit and systems. 243-246, 2006.

[11]H. Thapliyal, A. P. Vinod, "Design of reversible sequential elements with feasibility of transistor implementation" In proceedings of the IEEE International Symposium on circuits and system, 625-628, 2007.

[12]J. Rice, "An introduction to reversible latches"' Computation. J. 51, 6, 700709,2008.

[13]M.L. Chuang, C.Y. Wang, "Synthesis of reversible sequential elememts" J. Emerg. Technol. Comput. Syst. 3, 4, 1-19, 2008.

[14]K. Morita, "Reversible computing and cellular automata- a survey", Elsevier Theor.Compt. Sci. 395, 1, 101-131, 2008.

[15]Hafiz Md., Md. M. A. Polash, a. S. Md. Sayem, "A novel design of a reversible field programmable gate array",silvar Jubilee conference on Comm. Tech. & VLSI Design (Comm V09), VIT University, Vellore, India. Oct 8-10, 1009, pp 502-503.

[16]Mathew Morrison, Matthew Lewandowski, Richard meana and NagarajanRanganathan, "Design of static and Dynamic RAM Arrays using a novel reversible logic gate and decoder", 11th IEEE Int. Conference on Nanotechnology, Oregon, USA, August 15-18, 2011.

[17]Sk. Noor Mohammad and KamakotiVeezhinathan, "Constructing Online Testable Circuits using Reversible Logic", IEEE transactions on Instrumentation and measurement, vol. 59, no.1, January 2010.

[18]Abu Sadat Md. Sayem, Masashi Ueda, "Optimization of reversible sequential circuits", Journal of Computing, Vol. 2, issue 6, June 2010.

[19]H. Thapliyal and N. Ranganathan Design of Reversible Sequential Circuits Optimizing Quantum Cost, Delay, and Garbage Outputs, ACM Journal on Emerging Technologies in Computer Systems, Vol. 6, No. 4, Article14, Pub. Dec. 2010.

[20]Mohammadi, M. and Mishghi, M. On figures of merit in reversible and quantum logic designs, Quantum Inform. Process.8, 4, 297-318, 2009.

[21]Michael a. Nielsen, Isaac L. Chuang, " Quantum Computation Information", Cambridge University Press, New York, USA 2010.

[22]AlakMajumder, PrasoonLata Singh, Nikhil Mishra, AbirJyotiMondal, BarnaliChowdhury ,"A Novel Delay & Quantum Cost Efficient Reversible Realization of 2i x j Random Access Memory", International Conference on VLSI Systems, Architecture, Technology and Applications (VLSI - SATA 2015), Sponsored by IEEE, Banglore (Accepted).

[23]A.V. Ananthalakshmi, G.F.Sudha, "Design of 4-Bit Reversible Shift Registers", E ISSN: 2224-266X, Issue 12, Volume 12, December 2013.