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

An Efficient Comprehension of Reversible LFSR for Its Application in Cryptography

Pabballa Mahesh
M.Tech(Digital Systems & Computer Electronics),
Department of ECE
Scient Institute of Technology, Ibrahimpatnam,
Ranga Reddy (Dt), Telangana, India.

Dr. Arvind Kundu, (Ph.D)
HoD
Department of ECE
Scient Institute of Technology, Ibrahimpatnam,
Ranga Reddy (Dt), Telangana, India.

Abstract:

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.*

INTRODUCTION

Objectives Of The Project :

The main objective is to design an reversible implementation of a digital linear feedback shift register (LFSR) using reversible logic gates.

Other objectives are given below.

- To design both non-reversible and reversible versions of linear feedback shift register(LFSR) along with analytical evaluation of the design complexities both in terms of garbage outputs and constant inputs requirements.
- To optimize the shift registers optimizing techniques are also implemented .
- To design reversible linear feedback shift register(LFSR) with proposed reversible logic gates.

Motivation:

The present invention and motivation is relates to a linear-feedback shift register (LFSR) design using reversible logic gates.

One of the major goals in modern circuit design is reduction of power consumption. As demonstrated by R.Landauer in the early 1960s, irreversible hardware computation, regardless of its realization technique, results in energy dissipation due to the information loss [1]. Reversible logic circuits have theoretically zero internal power dissipation because they do not lose information. Hence,. In 1973, Bennett showed that in order to avoid KTln2 joules of energy dissipation in a circuit, it must be built using reversible logic gates [2]. A circuit is said to be reversible if the input vector can be uniquely recovered from the output vector and there is a one-to-one correspondence between its input and output assignments, i.e. not only the outputs can be uniquely determined from the inputs, but also the inputs can be recovered from the outputs [4-6].

In computing, a linear-feedback shift register (LFSR) is a shift register whose input bit is alinear function of its previous state.

The most commonly used linear function of single bits is exclusive-or (XOR). Thus, an LFSR is most often a shift register whose input bit is driven by the XOR of some bits of the overall shift register value.

The initial value of the LFSR is called the seed, and because the operation of the register is deterministic, the stream of values produced by the register is completely determined by its current (or previous) state. Likewise, because the register has a finite number of possible states, it must eventually enter a repeating cycle. However, an LFSR with a well-chosen feedback function can produce a sequence of bits which appears random and which has avery long cycle. Applications of LFSRs include generating pseudo-random numbers, pseudo-noise sequences, fast digital counters, and whitening sequences. Both hardware and software implementations of LFSRs are common.

The mathematics of a cyclic redundancy check, used to provide a quick check against transmission errors, are closely related to those of an LFSR.

LITERATURE SURVEY

Today's computers erase a bit of information (in the sense used here) every time they perform a logic operation. These logic operations are therefore called "irreversible." This erasure is done very inefficiently, and much more than kT is dissipated for each bit erased.

If we are to continue the revolution in computer hardware performance we must continue to reduce the energy dissipated by each logic operation. Today, because we are dissipating much more than kT, we can do this by improving conventional methods, i.e., by improving the efficiency with which we erase information.

An alternative is to use logic operations that do not erase information. These are called reversible logic operations, and in principle they can dissipate arbitrarily little heat. As the energy dissipated per irreversible logic operation approaches the fundamental limit of ln 2 x kT, the use of reversible operations is likely to become more attractive. If current trends continue this should occur sometime in the 2010 to 2020 timeframe. If we are to reduce energy dissipation per logic operation below ln 2 x kT we will be forced to use reversible logic. Nano technologyshould let us build mole quantities of logic elements. Unless energy dissipation per logic operation can be reduced below kT, the raw cost of electricity might well prove prohibitive and the system might quickly overheat.

Even today the use of reversible logic operations can be a useful heuristic in the design of systems that use very little power. To achieve a completely reversible system (which erases no bits at all) is very difficult. As we allow more and more bits to be erased during normal system operation, it becomes easier and easier to design the system. Today's systems erase a bit for every logic operation they perform and are very dissipative. Systems that perform some operations in a reversible fashion can dissipate less energy and might prove competitive (particularly in niche applications) today.

Reversible logic is becoming a popular emerging paradigm because of its applications in various emerging technologies, like quantum computing, DNA computing, optical computing, etc. It is also considered an alternate low power design methodology. A reversible circuit consists of a cascade of reversible gates without any fanout or feedback connections, and the number of inputs and outputs must be equal. There exists various ways by which reversible circuits can be implemented like NMR technology, optical technology, etc.

Reversible computing is a model of computing where the computational process to some extent is reversible, i.e., time-invertible. In a computational model that uses transitionsfrom one state of the abstract machine to another, a necessary condition for reversibility is that the relation of the mapping from states to their successors must be one-to-one. Reversible computing is generally considered an unconventional form of computing.

Existing method:

LFSRs have long been used as pseudo-random number generators for use in stream ciphers (especially in military cryptography), due to the ease of construction from simpleelectromechanical or electronic circuits, long periods, and very uniformly distributed output streams. However, an LFSR is a linear system, leading to fairly easy cryptanalysis. For example, given a stretch of known plaintext and corresponding ciphertext, an attacker can intercept and recover a stretch of LFSR output stream used in the system described, and from that stretch of the output stream can construct an LFSR of minimal size that simulates the intended receiver by using the Berlekamp-Massey algorithm. This LFSR can then be fed the intercepted stretch of output stream to recover the remaining plaintext.

The linear feedback shift registers (LFSR)are designed by using conventional gates and existing reversible logic gates etc. using the Boolean expressions.

Proposed method:

The development in the field of nanometer technology leads to minimize the power consumption of logic circuits. Reversible logic design has been one of the promising technologies gaining greater interest due to less dissipation of heat and low power consumption. In the digital design, the linear feedback shift register(LFSR)is a widely used process.

So, the reversible logic gates and reversible circuits for realizing linear feedback shift register(LFSR)s using reversible logic gates is proposed. The proposed design leads to the reduction of power consumption compared with conventional logic circuits.

INTRODUCTION TO REVERSIBLE LOGIC GATES

Reversible computing:

Reversible computing is a model of computing where the computational process to some extent is reversible, i.e., time-invertible. A necessary condition for reversibility of a computational model is that the relation of the mapping states of transition functions to their successors should at all times be one-to-one. Reversible computing is generally considered an unconventional form of computing.

There are two major, closely related, types of reversibility that are of particular interest for this purpose: physical reversibility and logical reversibility. A process is said to be physically reversible if it results in no increase in physical entropy; it is isentropic.

These circuits are also referred to as charge recovery logic or adiabatic computing. Although in practice no non stationary physical process can be exactly physically reversible or isentropic, there is no known limit to the closeness with which we can approach perfect reversibility, in systems that are sufficiently well-isolated from interactions with unknown external environments, when the laws of physics describing the system's evolution are precisely known.

Probably the largest motivation for the study of technologies aimed at actually implementing reversible computing is that they offer what is predicted to be the only potential way to improve the energy efficiency of computers beyond the fundamental von Neumann-Landauer limit of kTln(2) energy dissipated per irreversible bit operation.

As was first argued by Rolf Landauer of IBM, in order for a computational process to be physically reversible, it must also be logically reversible. Landauer's principle is the loosely formulated notion that the erasure of n bits of information must always incur a cost of nkln(2) in thermodynamic entropy. A discrete, deterministic computational process is said to be logically reversible if the transition function that maps old computational states to new ones is a one-to-one function; i.e. the output logical states uniquely defines the input logical states of the computational operation.

Reversible circuits

To implement reversible computation, estimate its cost, and to judge its limits, it is formalized it in terms of gate-level circuits. For example, the inverter (logic gate) (NOT) gate is reversible because it can be undone. The exclusive or (XOR) gate is irreversible because its inputs cannot be unambiguously reconstructed from an output value. However, a reversible version of the XOR gate—the controlled NOT gate (CNOT)—can be defined by preserving one of the inputs. The three-input variant of the CNOT gate is called the Toffoli gate. It preserves two of its inputs a,b and replaces the third c by c\oplus (a\cdot b). With c=0, this gives the AND function, and with a\cdot b=1 this gives the NOT function. Thus, the Toffoli gate is universal and can implement any reversible Boolean function (given enough zero-initialized ancillary bits). More generally, reversible gates have the same number of inputs and outputs. A reversible circuit connects reversible gates without fanouts and loops. Therefore, such circuits contain equal numbers of input and output wires, each going through an entire circuit.

Some of reversible gates:

Feynman / CNOT Gate:

The Reversible 2*2 gate with Quantum Cost of one having mapping input (A, B) to output (P = A, Q= A^B) .

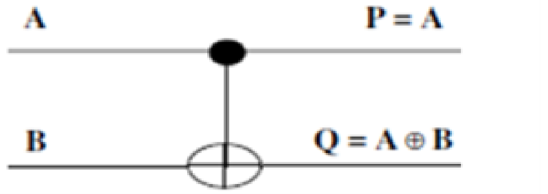


Fig 3.1 Reversible Feynman/CNOT gate (FG)

TABLE 3.1: Truth Table For CNOT Gate

INPUT		OUTPUT	
a	b		
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

LINEAR FEEDBACK SHIFT REGISTE

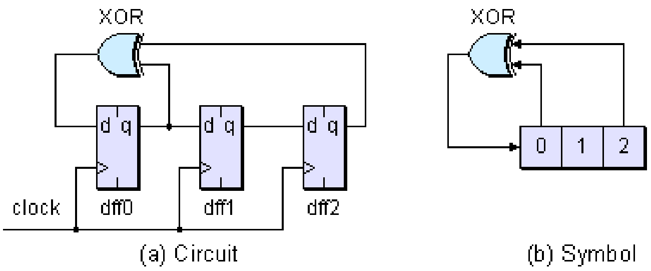
A linear feedback shift register (LFSR) is the heart of any digital system that relies on pseudorandom bit sequences (PRBS), with applications ranging from cryptography and bit-error-rate measurements, to wireless communication systems employing spread spectrum or CDMA techniques.

The equivalent to the world of electronics would be the Linear Feedback Shift Register (LFSR), in which the output from a standard shift register is cunningly manipulated and fed back into its input in such a way as to cause the function to endlessly cycle through a sequence of patterns.

Many-to-oneimplementations:

LFSRs are simple to construct and are useful for a wide variety of applications, but are often sadly neglected by designers. One of the more common forms of LFSR is formed from a simple shift register with feedback from two or more points, or taps, in the register chain (Fig 4.1).

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



(a) Circuit (b) Symbol

Fig4.1. LFSR with XOR feedback path.

LFSR Generator Implementations:

Linear feedback shift registers can be implemented in two ways. The Fibonacci implementation consists of a simple shift register in which a modulo-2 sum of the binary-weighted taps is fed back to the input. (The modulo-2 sum of two 1-bit binary numbers yields 0 if the two numbers are identical, and 1 if the differ: 0+0=0, 0+1=1, 1+1=0.)

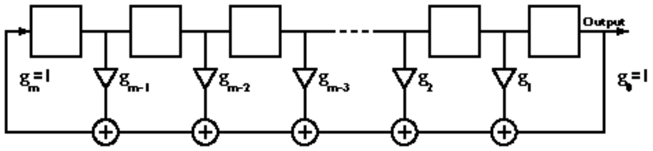


Fig4.4. Fibonacci implementation of LFSR.

REVERSIBLE LFSR

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

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 figure5. 20 shows the design of 3 bit reversible LFSR

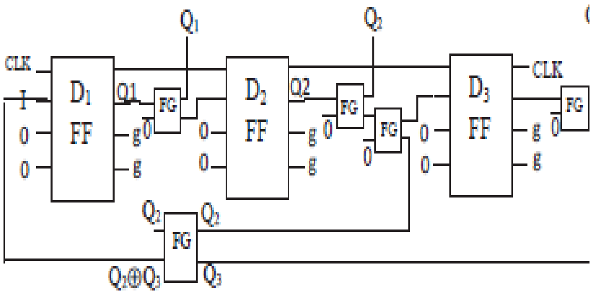


Fig5..20. Realization of pulse triggered reversible LFSR

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 5.III.A 3-BIT REVERSIBLE LFSR PARAMETERS

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

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.

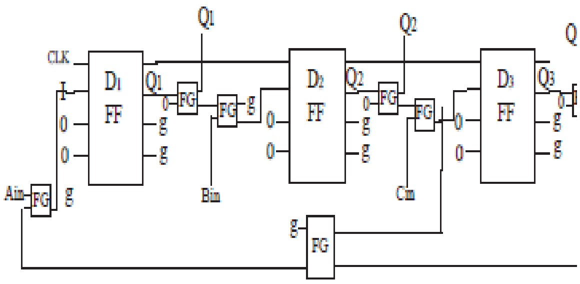


Fig5.21. Realization of 3 bit Reversible PSA

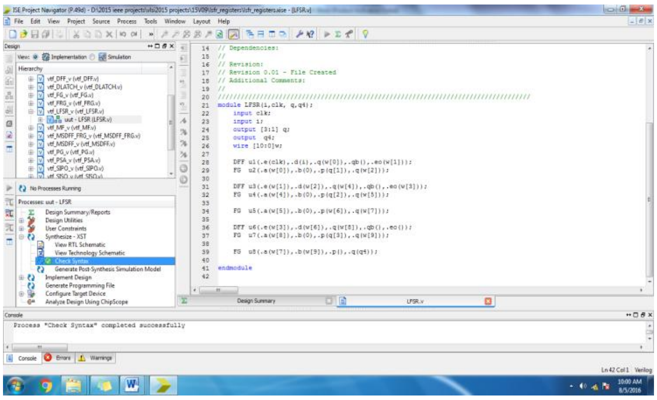
Figure 21 shows the diagram of Reversible PSA. PSA can be used as LFSR if the inputs Ain, Bin and Cin all held at 0, PSA will produce exactly the same bit pattern as LFSR. Inputs Ain, Bin, etc. are multiplexed with the outputs of ASIC. Each bit stream is applied through the LFSR to the ASIC inputs &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

TABLE5. IV. A 3-BIT REVERSIBLE PSA PARAMETERS

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

Screen Shots

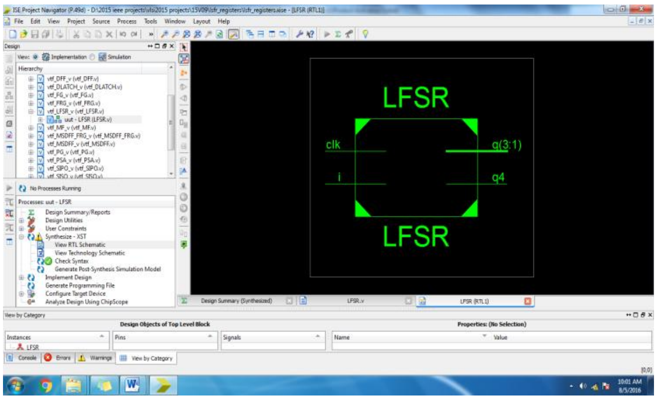
Syntax:



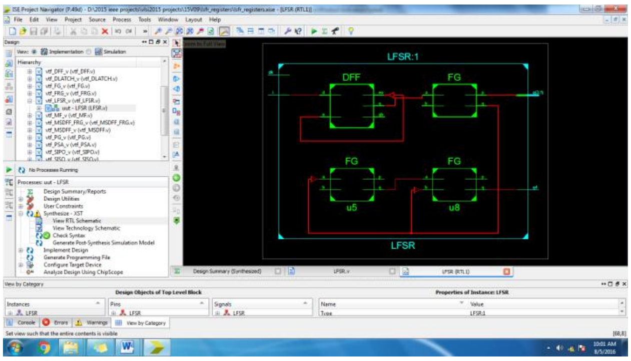
```
// Dependencies:
//
// Revision:
// Revision 0.01 - File Created
// Additional Comments:
//
////////////////////////////////////////////////////////////////////////////////
module LFSR(i,clk, q,q4);
    input clk;
    input i;
    output [3:1] q;
    output  q4;
    wire [10:0]w;

    DFF u1(.e(clk),.d(i),.q(w[0]),.qb(),.eo(w[1]));
    FG  u2(.a(w[0]),.b(0),.p(q[1]),.q(w[2]));

    DFF u3(.e(w[1]),.d(w[2]),.q(w[4]),.qb(),.eo(w[3]));
    FG  u4(.a(w[4]),.b(0),.p(q[2]),.q(w[5]));

    FG  u5(.a(w[5]),.b(0),.p(w[6]),.q(w[7]));

    DFF u6(.e(w[3]),.d(w[6]),.q(w[8]),.qb(),.eo());
    FG  u7(.a(w[8]),.b(0),.p(q[3]),.q(w[9]));

    FG  u8(.a(w[7]),.b(w[9]),.p(),.q(q4));

endmodule
```

```
Process "Check Syntax" completed successfully
```

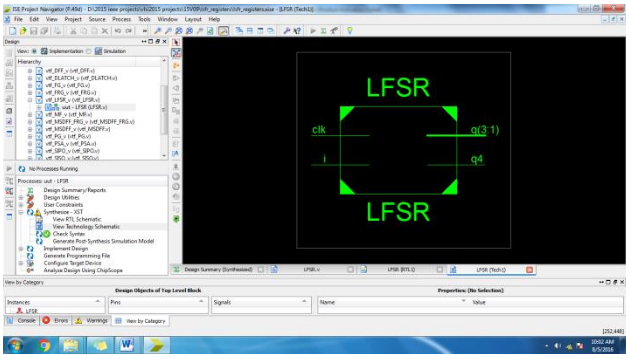
RTL Schematic:



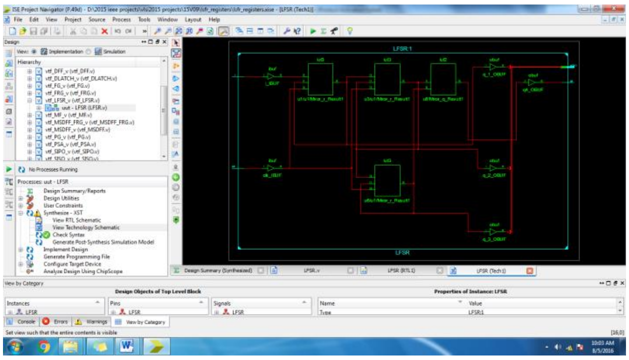
Sub RTL schematic:



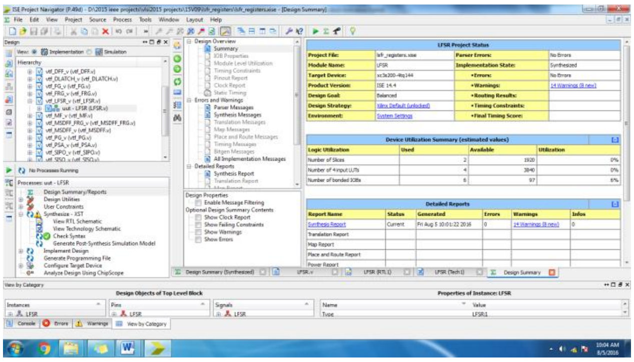
Technology Schematic:



Sub Technology schematic:



Design Design summary:

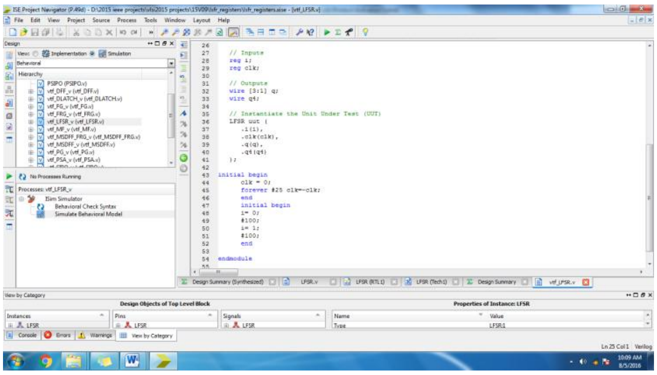


LFSR Project Status			
Project File:	lsfr_registers.xise	Parser Errors:	No Errors
Module Name:	LFSR	Implementation State:	Synthesized
Target Device:	xc3s200-4tq144	•Errors:	No Errors
Product Version:	ISE 14.4	•Warnings:	14 Warnings (8 new)
Design Goal:	Balanced	•Routing Results:	
Design Strategy:	Xilinx Default (unlocked)	•Timing Constraints:	
Environment:	System Settings	•Final Timing Score:	

Device Utilization Summary (estimated values)			
Logic Utilization	Used	Available	Utilization
Number of Slices	2	1920	0%
Number of 4 input LUTs	4	3840	0%
Number of bonded IOBs	6	97	6%

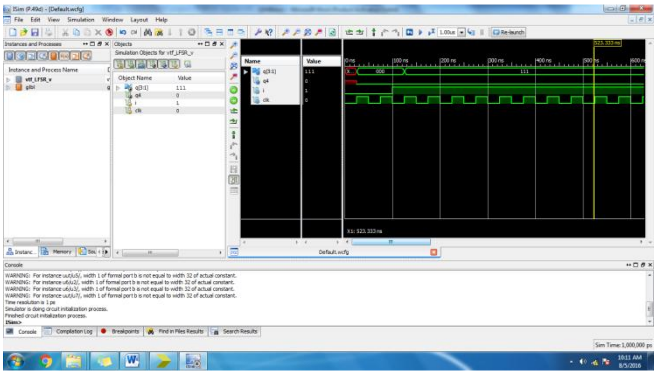
Detailed Reports					
Report Name	Status	Generated	Errors	Warnings	Infos
Synthesis Report	Current	Fri Aug 5 10:01:22 2016	0	14 Warnings (8 new)	0
Translation Report					
Map Report					
Place and Route Report					
Power Report					

Test Bench :



```
    // Inputs
    reg i;
    reg clk;

    // Outputs
    wire [3:1] q;
    wire q4;

    // Instantiate the Unit Under Test (UUT)
    LFSR uut (
        .i(i),
        .clk(clk),
        .q(q),
        .q4(q4)
    );

initial begin
        clk = 0;
        forever #25 clk=~clk;
        end
        initial begin
        i= 0;
        #100;
        i= 1;
        #100;
        end

endmodule
```

Simulated output:



```
WARNING:  For instance uut/u5/, width 1 of formal port b is not equal to width 32 of actual constant.
WARNING:  For instance u6/u2/, width 1 of formal port b is not equal to width 32 of actual constant.
WARNING:  For instance u6/u3/, width 1 of formal port b is not equal to width 32 of actual constant.
WARNING:  For instance uut/u7/, width 1 of formal port b is not equal to width 32 of actual constant.
Time resolution is 1 ps
Simulator is doing circuit initialization process.
Finished circuit initialization process.
ISim>
```

Advantages:

1. Area Efficient circuits.
2. Low power Circuits
3. High speed circuits

Applications:

Pattern generators like LFSR (Linear Feed Back Shift Registers) can produce random patterns with low hardware requirements and is preferred choice for testing. It is categorized under pseudo-random test pattern generators which can produce a random pattern for every clock cycle applied to it

CONCLUSION AND FUTURE SCOPE

Due to the feedback function, a LFSR can produce a sequence of random bits which has a very long cycle. The repeating sequence of bit patterns of an LFSR allows it to be used as a frequency divider or as a counter when a nonbinary pattern is acceptable. 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 for its FPGA prototyping 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.