A Novel Realization of 8 Bit Reversible LFSR Encryption And Decryption

Rangappagari Sarath Babu[1], T.K.Kalaiarasan[2]
Department of ECE
[1, 2]Swetha Institute of Technology & Science, Tirupati.

Abstract-*Reversible logic has emerged as an trade layout method to the conventional common sense, ensuing in decrease electricity intake and lesser circuit area. Comparators are a key element in maximum virtual structures.One-to-one mapping from enter to output is the important circumstance for a reversible computational version transiting from one country of summary system to some other. Probably, the most important motivation to have a look at reversible technologies is that, it's far considered to be the best powerful manner to decorate the electricity efficiency than the traditional models. 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.*

I. INTRODUCTION

The energy dissipation of devices is growing with the technological development day-by-day, thereby making it the major predicament of generation. Reversible logic gates because of its potential to lessen energy dissipation attracted researcher's interest.Irreversible gates produce energy loss due to the statistics bits lost for the duration of computation procedure. Information loss takes place because of much less no. Of generated output indicators than what's implemented. According to R.Landauer's precept[1], given in 1961, irreversible logic gates dissipates KTln2 joules of energy for the lack of 1-bit records, where K is the Boltzmann regular and T is the absolute temperature at which operation is executed which means that the energy dissipation is without delay proportional to the wide variety of statistics bit loss.

Charles Bennet, in 1973 [2], existed that, to avoid heat dissipation, good judgment circuit must be built from reversible circuit due to the fact that there no facts loss occurs.

The latest works focus on optimizing the reversible sequential designs in phrases of wide variety of reversible gates and garbage outputs. The shift registers are the maximum exhaustively used useful devices in digital system design for more than one bits storing & moving of the same if required. In this task, we're offering reversible realization of shift registers naming Serial-in Serial-out and Serial-in Parallel-out for his or her utility in designing series pulse generator. We may even gift novel reversible structure of Linear Feedback Shift Register (LFSR) and Parallel Signal Analyzer (PSA). In computing, the enter little bit of LFSR is a linear feature of its final country. The starting price of the LFSR is termed seed, and because of the deterministic operation of the sign in, the bit circulate produced is completely decided by way of its modern-day (or previous) kingdom.

II. BRIEF OVERVIEW OF REVERSIBLE GATES

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).

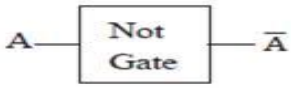

Fig1. NOT gate and its quantum representation

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).

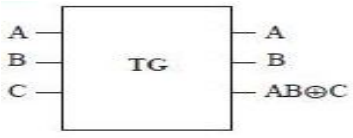

Fig.2 Quantum representation of Controlled-V

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)

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.

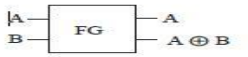

Fig3. Feynman Gate & its Quantum representation

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.

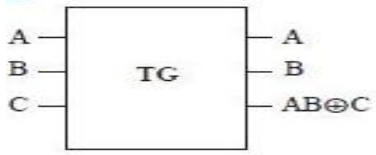

Fig.4. Toffoli gate and its Quantum representationFredkin Gate

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.

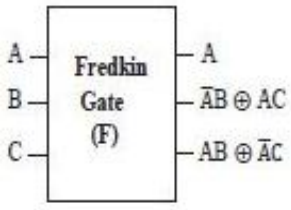

Fig.5. Fredkin Gate

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.

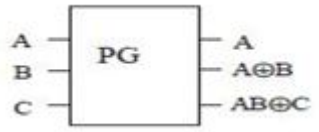

Fig6. Peres gate and its quantum representation

Modified Fredkin (MF) Gate

It is the existed 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

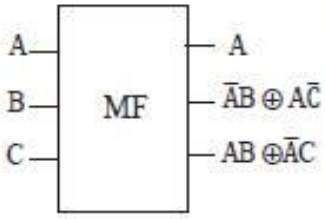

Fig7. MF gate and its Quantum representation.

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

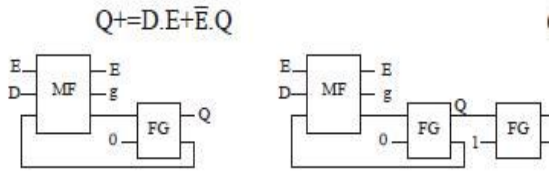

Fig 8 Clock enabled D-latch and D-FF with output Q and

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 existed Master-Slave configuration of D-FF is shown in figure 10.

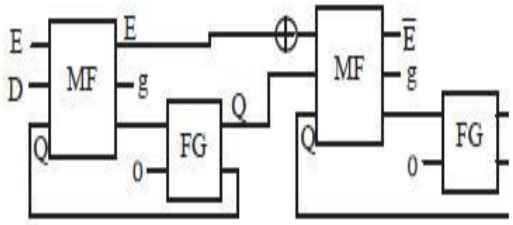

Fig 9. MASTER SLAVE D-FF USING MF GATE

III. EXISTED 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 figure3.1 shows the design of 3 bit reversible LFSR

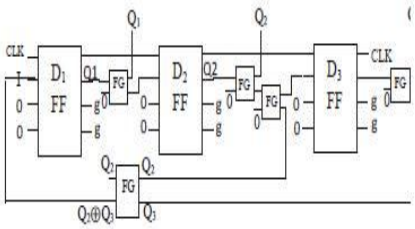

Fig14.Realization of pulse triggered reversible LFSR

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.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.

IV. PROPSED 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 figure3.3 shows the design of 4 bit reversible LFSR.

This four bit LFSR consist of four D Flip-flops, fredkin gate and Feynman gate. Each D flip flop is three inputs (clk,data,'0') and three outputs(clk,Q,open) reversible flipflop .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 , Q3 andQ4 , 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. For example LFSR loaded with a seed value is "1100"after eight iteration it will generate a pseudorandom pattern of "1111" again if it is given back to same LFSR after eight iteration it will generate a pseudorandom pattern of "1100" .

The sequences of iterations are 1100,0110,1011,0101,1010,1101,1110,1111. Feynman gate is used to used between any two FFs to copy the output is necessary for analog design but for digital point of view is not necessary. The pattern count of LFSR equals to 2n– 1, where n is the number of flip-flops.

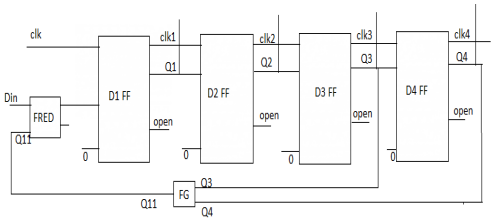

Fig11: proposed 4 bit Reversible LFSR

Proposed Architecture Using Reversible Lfsr For Image Encryption And Decryption:

The proposed architecture consists of altera memory blocks and two four bit reversible LFSR connected as show in figure 3.4. Initially the memory loaded with 64 pixels data which is to be the data_in for 8 bit LFSR. Each pixel 8 bit data can be divided into two 4 bit data and then given to two 4 bit reversible LFSR to convert encrypted data which is shown in figure 3.5.This encrypted data stored into altera memory.

This encrypted 8 bit data again is given to two 4 bit reversible LFSR it will give back the original image pixel values as shown in figure3.5.For example LFSR loaded with a seed value is "1100(12)"after eight iteration it will generate a pseudorandom pattern of "1111(15)" again if it is given back to same LFSR after eight iteration it will generate a pseudorandom pattern of "1100" .The sequences of iterations are 1100,0110,1011,0101,1010,1101,1110,1111 for encrypted vales.

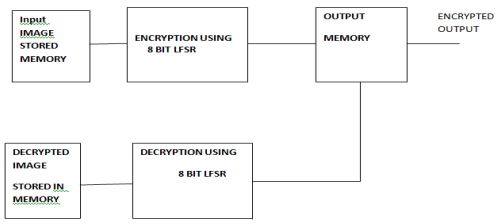

Fig12:Realization of Reversible LFSR for encryption and decryption

V. SIMULATION RESULTS

Flow Status	Successful - Tue May 16 12:33:21 2017
Quartus II Version	9.1 Build 350 03/24/2010 SP 2 SJ Web Edition
Revision Name	LFSR
Top-level Entity Name	top
Family	Stratix II
Met timing requirements	No
Logic utilization	1 %
Combinational ALUTs	144 / 12,480 (1 %)
Dedicated logic registers	55 / 12,480 (< 1 %)
Total registers	55
Total pins	103 / 343 (30 %)
Total virtual pins	0
Total block memory bits	1,536 / 419,328 (< 1 %)
DSP block 9-bit elements	0 / 96 (0 %)
Total PLLs	0 / 6 (0 %)
Total DLLs	0 / 2 (0 %)
Device	EP2S15F484C3
Timing Models	Final

Fig13 Design summary for proposed top 8 bit reversible LFSR for image encryption

The above figure is representation of design summary for proposed 8 bit reversible LFSR for image encryption.8 bit reversible LFSR is implemented in one of the FPGA Family is QUARTUS II version and StratixII family. The above 8 bit reversible LFSR takes 144 combinational ALUTs,55 dedicated logic registers and totally 103 Input and output pins to functioning the 8 bit reversible LFSR .

The above 8 bit reversible LFSR takes <1% logic utilization with device used is EP2S15F484C3 and this design has been used 1,536 memory bits and zero DSP elements.

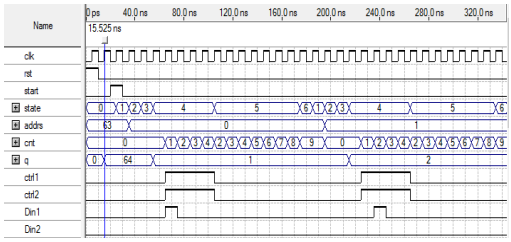

Fig 5.2 Simulation results for proposed 8 bit reversible LFSR for image encryption

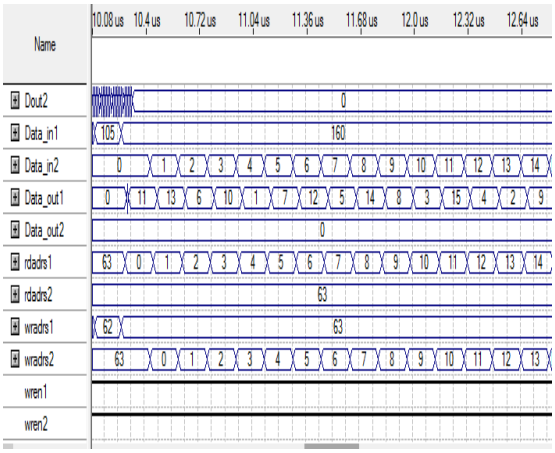

Fig5.3 Simulation results for proposed 8 bit reversible LFSR for image encryption

VI. CONCLUSION

Due to the comments feature, a LFSR can produce a sequence of random bits which has a totally lengthy cycle. The repeating series of bit patterns of an LFSR permits it for use as a frequency divider or as a counter while a non-binary sample is suitable. In this assignment, we've confirmed novel structure of pulse triggered and facet brought about SISO & SIPO registers and analyzed their quantum cost, delay and garbage in terms of a few lemmas. Usingthe registers we have proven an instance of collection pulse generation with minimized delay & fee. Lastly, we have found out reversible architecture of LFSR and PSA which can be used for random bit generation. Due to the benefit in production, the unconventional architecture of LFSR & PSA may be utilized in navy cryptography. However, as the reversible LFSR is a linear system, it results in most clean cryptanalysis. This venture of eight bit reversible LFSR for photograph encryption and decryption is designed in VHDL and synthesized and simulated in ALTERA QUATRUS –II 9.1.From the effects it's miles obvious that the proposed layout used fifty five Combinational ALUTs and 1,536 blocked reminiscence bits.

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] Tommaso Toffoli, “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. Srin1ivas, 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, 700-709,2008.