International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Design of Reversible LFSR for Cryptographic Application

*O.Swapna **G.Babu

*M.TECH student, Dept of ECE, Vaagdevi College of Engineering
*Associate Professor, Dept of ECE , Vaagdevi College of Engineering

Abstract—

Reversible technology is the best low power technology to transmit the data from one state to another state. Perhaps it's better to study the reversible technology because which have less power consumption than conventional models. This research can apply for some technologies such as low power VLSI, quantum computing Nano technology, QCA. Here we are designing the reversible LFSR (Linear feedback shift register) and parallel signature analyser(PSA) to find the delay, power and garbage values. To realization of LFSR here we have some designs such as Serial in serial out(SISO), Serial in parallel out(SIPO) which represents the delay, power and garbage values better than existed designs.

Key words: SISO, SIPO, Reversible LFSR, PSA, Reversible technology

I. INTRODUCTION

The power dissipation of devices is increasing with the technological advancement day-by-day, thereby creating it the major limitation of technology. Reversible logic gates due to its ability to cut back power dissipation attracted researcher's attention. Irreversible gates turn out energy loss due to the knowledge bits lost throughout computation method.

Information loss happens thanks to less no. of generated output signals than what's applied. in line with R. Landauer's principle, given in 1961, irreversible logic gates dissipates KTln2 joules of energy for the loss of 1-bit information, wherever K is that the Boltzmann constant and T is that the absolute temperature at that operationisperformed thatmeansthat theability dissipation is directly proportional to the number of data bit loss. Charles

Bennet, In 1973, planned that, to avoid cooling, logic circuit must be designed from reversible circuit since there no information loss happens. At first, within the style of reversible logic circuits, style was restricted to combinatory logic circuits and it had been simply because of the convention that the feedback isn't allowed within the reversible computing.

But, in 1980, Toffoli has shown that the feedback is allowed in reversible computing.

In line with Toffoli, a consecutive network is reversible if its combinatory half is reversible. The recent works specialise in optimizing the reversible consecutive styles in terms of variety ofreversible gates and garbage outputs. The shift registers ar the most thoroughly used useful devices in digital system style for multiple bits storing & shifting of the same if needed. In this paper, we have a tendency to ar presenting reversible realization of 2 shift registers naming Serial-in Serial-out and Serial-in Parallel-out for his or her application in planning sequence generator. we'll additionally gift novelreversible desin of Linear Feedback register (LFSR) and Parallel Signal instrument (PSA). In computing, the input little bit of LFSR could be a linear perform of its last state. The beginning worth of the LFSR is termed seed, and due to the settled operation of the register, the bit stream produced is totally determined by its current (or previous) state. The paper is organized as follows. Section II offers an overview of the connected work & the aim of the work. Section III highlights the essential reversible gates that includes a brand new medium frequency gate with its quantum illustration. Reversible register ar mentioned in section IV with a comparison of them against previous works. Using reversibility, however pulse generation will be done is shown on section V employing a explicit example. Section VI & VII describes Reversible LFSR & PSA severally thereby mentioning however they'll generate random bit pattern. Conclusion with future scope is mentioned on section VIII.

II. RELATED WORK

The construct of a reversible memory cell was 1st shown by Fredkin and Toffoli, in 1982, where, design of a JK latch was introduced. Later, in 1996, Picton developed

a style of clock lessSR-latch victimisation 2 crosscoupled NOR gate, wherever NOR gates were designed from Fredkin gate. All the reversible latches like D-Latch, TLatch etc. beside their flip-flop and master-slave configuration were introduced for the primary time in 2005 by Thapliyal et.al.

In 2006, Rice introduced a SR-latch without fan out drawback obtainable within the style by Picton and after designed different latches from SR.In 2007, Thapliyal and Vinod planned a more robust style of reversible flip-flops than by Rice in terms of range of reversible gates getting used and garbage outputs. A more detailed analysis of SR-latch was bestowed by Rice in 2008. a more robust style of all reversible latches (except SRlatch) along with their flip-flops than that of Thapliyal(2005) and Rice (2006) were bestowed by Chuang and Wang. Morita (2008) gave a quick note on however a universal reversible laptop may well be made up ofreversiblelogic parts andreversible successive circuits,butno sensible hardware style was bestowed. This gave a direction of creating RAM because it is that the elementary storage for ADP system. In 2009, Hafiz bestowed a unique design of reversible FPGA. In 2011, Morrison designed a static and dynamic RAM arrays with reversible logic. In this work, we've got developed novel design of Shift Registers to possess a reversible operation on LFSR with reduced quantum value and minimum delay.

III.INTRODUCTION OF REVERSIBLE GATES

Paste your text here and click on "Next" to observe this text editor in chief do it's factor. don't have any text to check don't have any text toThe laws of physics ar primarily reversible. If any physical process (f) relates input (x, y) and outputs (z) specified, Z=f(x,y), the laws of changeability ensures that for any given output, z the inputs, x & y ar deductible. however, the classical computers violate this law of changeability. for instance, in an and performance, for output z = zero, the inputs can't be exactly deductive as there three sets of inputs that create z = zero.We assume the followings to explain a generalized reversible gate:i) Set of domain variable ={X1,X2,….Xn} ii) Set

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

of controls = C & the no. of components in C defines the breadth of gate

There ar some reversible basic gates that we tend to ar progressing to use in style of Registers and ar as follows:

A. Not Gate:

NOT gate could be a easy one input and one output (1*1) reversible gate that performs inversion of input. It has unit quantum value and unit delay (i.e.)

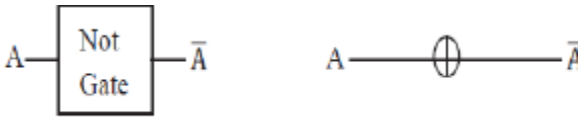


Fig. 1: NOT gate and its quantum representation

B. Controlled-V and Controlled-V+ Gate:

Controlled V and V+ ar the essential gates. In the controlled-V gate once the management signal A = zero, then the input B on track line can have the controlled half unchanged, that's Q = B. When A = 1, then the unitary operation V is applied to the input B, and output are going to be Q = V(B).

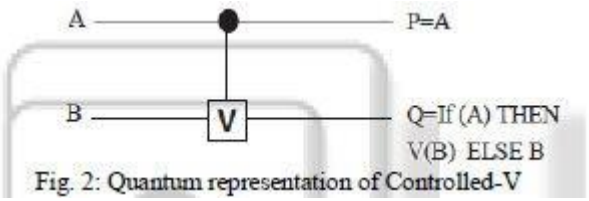


Fig. 2: Quantum representation of Controlled-V

Fig. 3: Quantum Representation of Controlled-V+

The V and V+ gates have the subsequent properties:

V×V = NOT

V×V+ = V+×V = I

V+×V+ = NOT

C. Controlled-NOT Gate/ Richard Phillips Feynman Gate

It is a 2*2 reversible gate. CNOT Gate, also known as Richard Phillips Feynman Gate and is employed to beat the fan-out problem since it are often used for repetition the knowledge. CNOT gate has unit quantum value and unit delay.

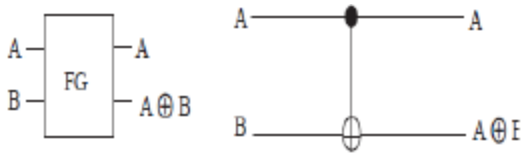


Fig. 4: Feynman Gate & its Quantum representation

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

C. Toffoli Gate:

Toffoli gate could be a 3*3 reversible gate with quantum value of five and delay. it's referred to as conjointly universal reversible gate

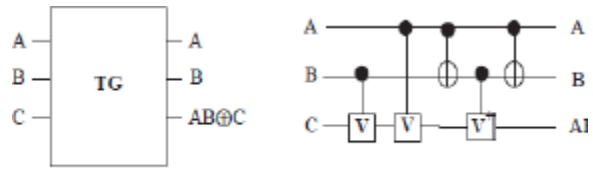


Fig. 5: Toffoli gate and its Quantum representation

D. Fredkin Gate:

Fredkin Gate is additionally a 3*3 gate. it's five quantum value and delay is 5. When A = 0, the opposite 2 inputs B and C is simply derived to the output. however once A = one, B and C is swapped within the output. Hence, it's conjointly termed as a controlled swap gate. Basic logic perform are often implemented victimization this gate and referred to as universal reversible gate.

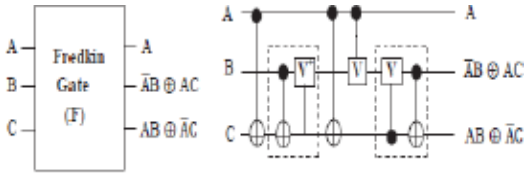


Fig. 6: Fredkin Gate and its Quntum representation

E. Peres Gate:

Peres gate could be a 4-input and 4-output (4*4) reversible gate. It has a minimum quantum value among the 4*4 reversible gate and is up to four and delay is 4□. the subsequent figure shows the Peres gate and its quantum illustration.

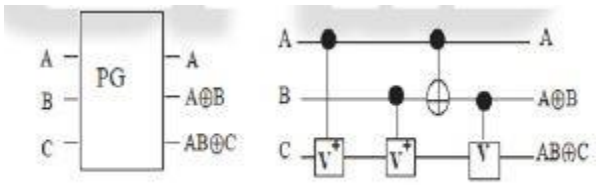


Fig. 7: Peres and its quantum representation

F. Modified Fredkin (Mf) Gate:

It is the planned changed version of 3*3 Fredkin gate with a quantum value of four and a delay of 4. When A = 0, it does the same as Fredkin Gate, however once A = one, B and complement of C is swapped within the output. Quantum representation of this gate is

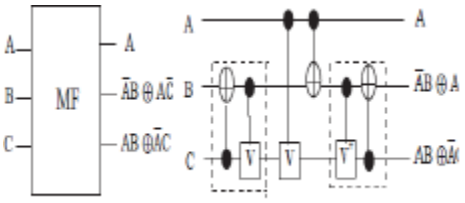


Fig. 8: MF gate and Quantum representation

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

IV. REVERSIBLE SHIFT REGISTER

Flip-flops ar the essential memory part used for storage of single bit information. To store a lot of range of bits, combination of FF is employed and referred to as shift registers. Loading of information might be serial or parallel. In serial loading, information shifted from one FF to a different in serial kind, i.e. 1-bit at a time, upon triggering clock. In parallel loading, all data-bits seem in parallel kind at a time upon triggering clock. during this section, we have planned Serial-in Serial-out and Serial-in Parallelout shift registers. to style reversible register for Pulse generation we tend to ar victimization master-slave D-FF block diagram.

Reversible D-FF: Characteristic equation of reversible D-Latch are often written as Q+=D wherever output is up to its input worth. The characteristic equation of clock enabled reversible D-Latch (D-FF) are often written as

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

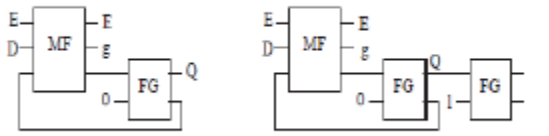


Fig. 9: Clock enabled D-FF with output Q and Q

Figure nine shows the clock alter D-latch (QC = 5) where output Q+=D for E=1 and output Q+=Q for E=0 output stay in its previous state. For the input D=1 and Q=0, the output of radio frequency gate once E=1 is Q+=1 that is applied to FG gate to produce feedback The planned Master-Slave configuration of D-FF is shown in figure ten.

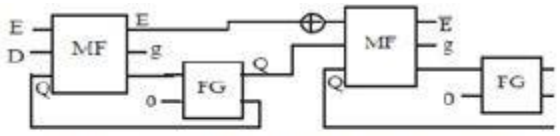


Fig. 10: Master Salve D-FF using MM Gate

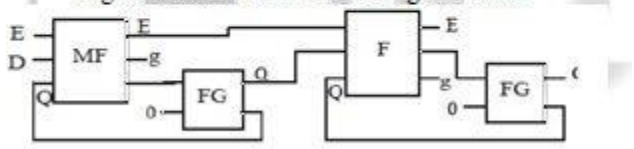


Fig. 11: Master Salve D-FF using MM and F gate

Figure ten shows the planning of master slave D-FF victimization radio frequency gate & Richard Phillips Feynman gate. Since this style turn out a clock inversion at the output of slave FF, to use clock pulse to

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

subsequent FF during a register, we'd like to use NOT gate to convert ~E into E. Hence, tobeat this downsidewe planned areplacement style shown in figure eleven commutation radio frequency gate by Fredkin gate in Slave FF since Fredkin gate doesn't require clock inversion and produces clock pulse as what's applied to its input. This planned style (i.e. figure 11), is used for Master-slave D-FF to appreciate registers.

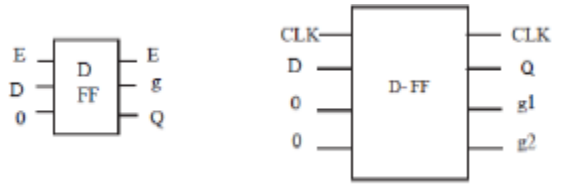


Fig. 12: Block diagram of D-FF and Master Salve D-FF

A. Proposed Reversible Serial-In Serial-Out (Siso) Shift Register:

Serial-inSerial-out register accepts information inserial kind and produces output serially. For N-bit register it takes n-1 clock pulse to store information serially and n-clock pulse to generate output. The subsequent figure thirteen & fourteen shows the reversible N-bit serial-in serial-out register for edge triggering & pulse triggering applications.

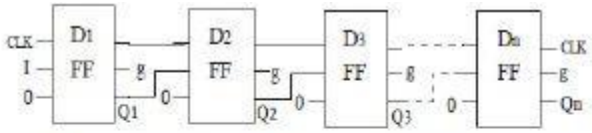


Fig.13. Edge-triggered N-bit SISO registers using D-FF

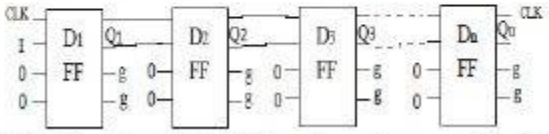


Fig.14. Pulse-triggered N-bit SISO registers using master-slave D-FF

When serial information is applied, every new bit is entered into initial FF upon application of every clock pulse. The bit that was previously hold on by initial FF transferred to second FF on application of second clock pulse and n-1 FF bit transferred to n–bit FF on application of n-1 clock pulse. The bit that was hold on by last FF, i.e. n-FF, is outputted on the application of n clock pulse. The planned style of SISO is optimized in terms of Quantum value, delay and garbage output.

B. Proposed Reversible Serial-In Parallel-Out (Sipo) Shift Register:

SIPO takes {input information | input file | computer file} serially and also the data

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

hold on within the register produces output in parallel kind. information input seems on register step-by-step basis whereas once information is hold on in register then all output seems in their various FF at a time.

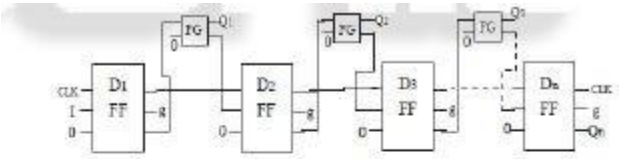


Fig.15. Edge-triggered N-bit SIPO registers using D-FF

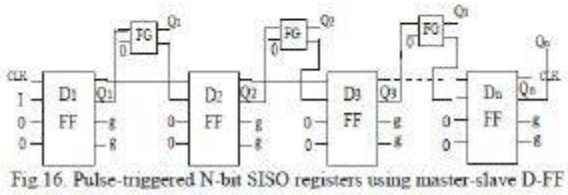


Fig.16. Pulse-triggered N-bit SISO registers using master-slave D-FF

It takes n-1 clock pulse to store information in register and one clock pulse to supply output. within the higher than figure fifteen information input is same as in SISO register and output seems as information, stored in register on one clock pulse.This planned style is additionally optimized in terms of quantum cost, delay and garbage outputs.

V. PROPOSED REVERSIBLE LFSR

Linear Feedback register (LFSR) is employed to get periodic sequence, however it doesn't turn out all zero sequence until it starts from all zero. A LFSR are often made by doing exclusive-OR on the outputs of 2 or a lot of of the FFs along and applying this output to 1 of the FFs. The figure twenty shows the planning of three bit reversible LFSR Fig.20. Realization of pulse triggered reversible LFSR Feynman gate is employed to control exclusive-OR operation on feedback path whereas it's conjointly used between any 2 FFs to copy the output. Q1, Q2 and Q3, at initial purpose of your time should not begin with all zero otherwise, LFSR produces all zero pattern output for each clock pulse applied. If the flip-flops are loaded with a seed worth (anything except all 0s) and if the LFSR is triggered, it'll generate a pseudorandom pattern of 1s and 0s. The pattern count of LFSR equals to 2n–1, wherever n is that the range of flip-flops. The patterns have an about equal range of 1’s Associate in Nursingd 0’s.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

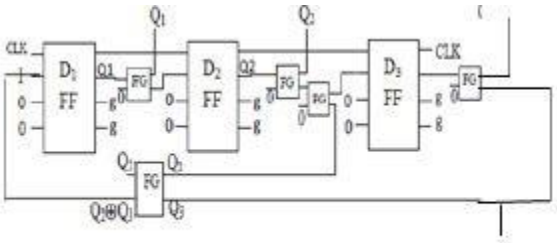
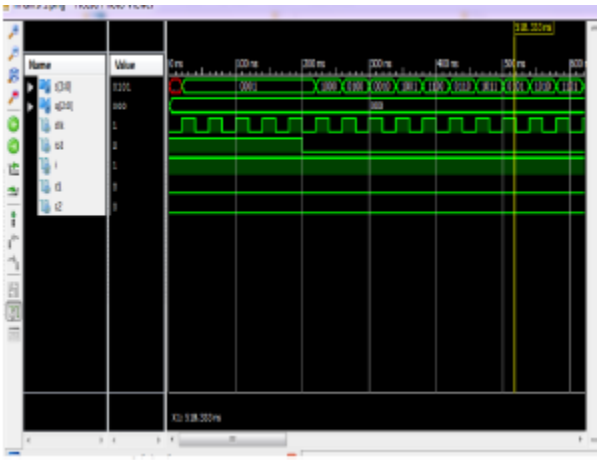


Fig.20. Realization of pulse triggered reversible LFSR



VI.IMPL EMENTATION RESULTS

The propsed design can be implemented by using the simulation tool XILINX ISE 14.7 and Verilog HDL, the proposed design synthesis and simulation results are shown in below.

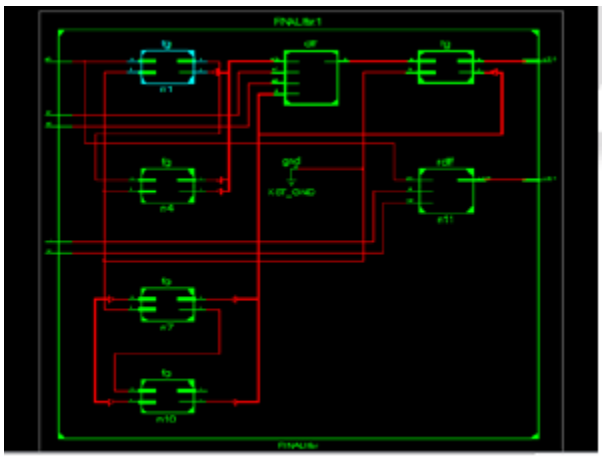


Fig. 21: RTL schmatic diagram

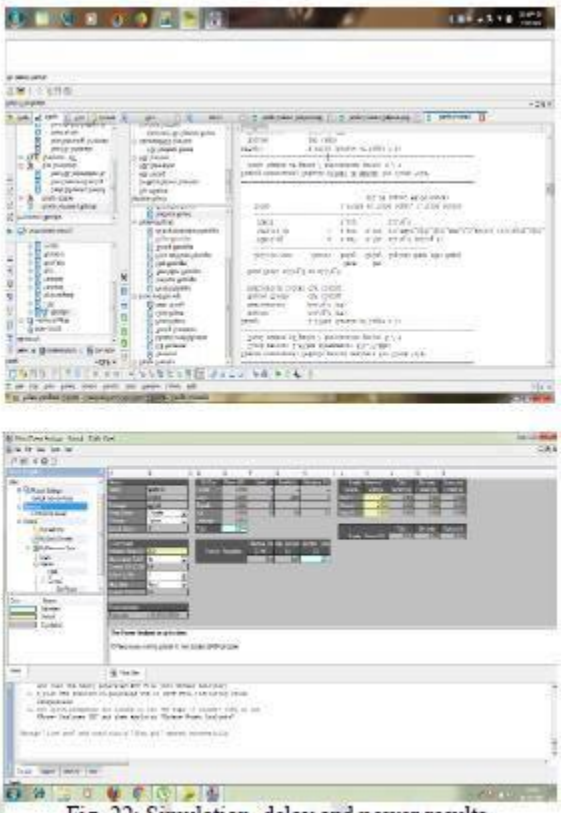


Fig. 22: Simulation, delay and power results.

VII. CONCLUSION

In this project, A novel realization of linear feedback shift registers using reversible logic gates, here we are constructing linear feedback shift registers using reversible logic gates, such that the gates and the area required for the construction of LFSR will be less. 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 beused 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] Tommaso Toffoli, “Reversible Computing,” Automata, Languages and programming, 7th Colloquium of Lecture Notes in ComputerScience, vol. 85, pp. 632-644,1980.

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

AUTHOR 1:-

* **O.Swapna** completed her B tech in S.R Engineering College in 2014 and pursuing M-Tech in Vaagdevi College of Engineering

AUTHOR 2:-

****G.Babu** is working as Associate Professor in Dept of ECE, Vaagdevi College of Engineering