Synthesis and Realization of Linear Feedback Shift Register Using Reversible Logic

J. Tejaswini
M.Tech,
ViswaBharathi PG College of Engineering and Technology.

Ramya Krishna
Assistant Professor,
ViswaBharathi PG College of Engineering and Technology.

Abstract:
Reversible logic is playing an important role in research areas and has found its applications in low power CMOS VLSI, Nanotechnology and Quantum computation. 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. Reversible logic is considered as a computing paradigm in which there is a one-to-one mapping between the input and the output vectors. In this paper we discuss with reversible circuits and reversibility which in future will be considered as a trend for low power design. Combinational circuits were the primary ones to be implemented using this technique. Later on few researches also contributed toward sequential circuits. In this paper we implement a reversible LFSR that dissipate less power than the conventional LFSR circuitry, 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 with existing designs. As a prior work, literature survey has been done.

Keywords:
Reversible logic, Quantum Computing, Linear Feedback Shift Register;

I. INTRODUCTION:
Energy loss is an important consideration in digital circuit design, also known as circuit synthesis. With the number of chip components doubling every 18 months, as per Moore’s Law, the Irreversible Technologies would dissipate a lot of heat and reduce circuit life.

It is here the Reversible Logic comes into action in not only recovering the lost information but also dissipating less heat. Landauer’s principle states that logic computations that are not reversible necessarily generates KT*ln2 joules of heat energy for every bit of information that is lost, where k is the Boltzmann’s constant and T is the absolute temperature at which the computation is performed. For room temperature T, the amount of dissipating heat is small (2.9x10^-21 joules) but not negligible [1]. Bennett showed that KTln2 energy dissipation would not occur if computation is carried out in a reversible way [2]. In the year 1994 Shor [5] did a remarkable research work in creating an algorithm using reversibility for factorizing large number with better efficiency when compared to the classical computing theory. After this the work on reversible computing has been started by more people in different fields such as nanotechnology, quantum computers and CMOS VLSI. 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). 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.
II. LITERATURE SURVEY:
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 cross coupled 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 SR-latch) 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. BASIC DEFINITIONS RELATED TO REVERSIBLE LOGIC:
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).

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).

In the controlled-V+ 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, \( Q = V+(B) \).

Hence, it is also termed as a controlled swap gate. Basic logic function can be implemented using this gate and called universal reversible gate.

**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. 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 Parallel-out 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

\[
Q^{+} = D \cdot E + E \cdot Q
\]  

(1)

Figure 9 shows the clock enable D-latch and D-FF with output \( Q \) and \( Q^{+} \).

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.

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.

![Fig 12. Block diagram of D-FF and Master Slave D-FF](image)

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.

![Fig 13. Edge-triggered N-bit SISO registers using D-FF](image)

![Fig 14. Pulse-triggered N-bit SISO registers using master-slave D-FF](image)

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 \( n-1 \) 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.

TABLE I. A COMPARISON OF 4-BIT SISO SHIFT REGISTER

<table>
<thead>
<tr>
<th>SISO</th>
<th>Quantum Cost (Qc)</th>
<th>Delay (D)</th>
<th>Garbage (G)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.V. Amuthakshitha 2013[23]</td>
<td>52</td>
<td>52</td>
<td>8</td>
</tr>
<tr>
<td>Proposed design for edge triggering w.r.t [23]</td>
<td>62</td>
<td>62</td>
<td>50</td>
</tr>
<tr>
<td>% improvement for pulse triggering w.r.t [23]</td>
<td>44</td>
<td>44</td>
<td>8</td>
</tr>
</tbody>
</table>

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 n-bit 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 figure 15 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

<table>
<thead>
<tr>
<th>SIPO</th>
<th>Quantum Cost (Qc)</th>
<th>Delay (D)</th>
<th>Garbage (G)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.V. Amuthakshitha 2013[23]</td>
<td>52</td>
<td>52</td>
<td>8</td>
</tr>
<tr>
<td>Proposed design for edge triggering w.r.t [23]</td>
<td>56</td>
<td>56</td>
<td>50</td>
</tr>
<tr>
<td>% improvement for pulse triggering w.r.t [23]</td>
<td>47</td>
<td>47</td>
<td>8</td>
</tr>
</tbody>
</table>

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

\[ Qc/D = 5n + n - 1 = 6n - 1 \]

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. 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 figure 17 shows the design of 3 bit reversible LFSR

V. 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 figure 17 shows the design of 3 bit reversible LFSR

\[
\text{TABLE III. A 3-BIT REVERSIBLE LFSR PARAMETERS:}
\]

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Proposed Design</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quantum Cost</td>
<td>38</td>
</tr>
<tr>
<td>Delay D</td>
<td>38</td>
</tr>
<tr>
<td>Garbage G</td>
<td>7</td>
</tr>
</tbody>
</table>

VI. 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 18. RTL schematic of pulse triggered reversible LFSR

Fig 19. RTL sub schematic 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 \(2^n−1\), where \(n\) is the number of flip-flops. The patterns have an approximately equal number of 1’s and 0’s.
VII. 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 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. We conclude that the choice of reversible gates and the design approach to carefully select a reversible gate for implementing a particular logic function will significantly impact the quantum cost, delay and garbage outputs of the reversible design.

REFERENCES:


