IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-6, Issue-4 E-ISSN: 2347-2693

FPGA Implementation of Configurable Linear Feedback Shift Register using Verilog

Harsh H. Ghelani[1*], Nilesh L. Jha[2], Rohan Naik[3] Pragya Gupta[4]

[1]Electronics Dept, KJ Somaiya College of Engineering
[2]Electronics Dept, KJ Somaiya College of Engineering
[3]Electronics Dept, KJ Somaiya College of Engineering
[4]Electronics Dept, KJ Somaiya College of Engineering

Available online at: www.ijcseonline.org

Received: 14/Mar/2018, Revised: 20/Mar/2018, Accepted: 05/Apr/2018, Published: 30/Apr/2018

Abstract — The proffered paper is presented on the practical implementation of a Configurable Linear Feedback Shift Register using Verilog and assesses its various parameters with respect to its configurable aspects and physical performance. The practical implementation is configurable with respect to Number of Bits, Seed Value, Number of Taps and Tap Position that increases the randomness of the output thus creating a more pseudo-random cycle. Moreover, reversible logic is explored and analysed and the technology is comprehended in this paper as an emerging technology that can be used to implement the designed Configurable Linear Feedback Shift Register. Reversible logic is said to enhance the power efficiency of a logical circuit than the conventional models and thus eases the migration to emerging technologies of Quantum Computing, Portable Embedded Systems and Low Power VLSI. The chosen target for the hardware realization of the CLFSR is Altera Cyclone II FPGA. Furthermore, simulation and synthesis of the design is done using ModelSim-Altera for Quartus II 12.1 Web Edition.

Index Terms — Configurable Linear Feedback Shift Register, Field Programmable Gate Array, Verilog, Reversible Logic, Shift Register, Random Number Generator.

I. INTRODUCTION

In the current generation of technological advancements and the development of internet-of-things, random number generators are surfacing as an indispensable and crucial feature for cryptography. With the rise of intelligent embedded system, we also have increased vulnerability. Thus, security implemented with additional features is a vital factor in all these systems. A Shift Register is implemented to generate pseudorandom numbers for cryptography application, CRC generator and checker circuit, gold code generator etc.

Due to the requirement of additional security we design the Linear Feedback Shift Register with variable parameters in terms of input seed string, tap positions, bit length etc. This added feature thus makes for a configurable feedback shift register. The proposed system is a much more advanced version of simple linear feedback shift register system as it can adapt to any number of bit technology i.e. operate on strings of any bit size and also configurable number of taps as well as the configurable tap positions help in creating a more random cycle thus it can create a better string of pseudorandom numbers.

One of the major limitation to the technological advancements from 32-bit systems to 64-bit systems is the incompatibility of many systems and devices from one technology to another. This limitation thus makes it much inconvenience to shift a system from one technology to another. Thus, the configurable nature of a Configurable Linear Feedback Shift Register could help overcoming this limitation as it can operate on strings of any number of bits.

Thus, in this paper we propose and design a configurable linear feedback shift register in Verilog for implementation. The Verilog code is implemented on an Altera Cyclone II Field Programmable Gate Array due to its flexibility to the number of inputs as well as to check the on-chip input-output parameters on each implementation thus the best choice for a fast prototype development tool.

The paper ahead is organized as follows. Section II is gives the overview of the related work. LFSR and its various types of implementation is discussed in Section III. Section IV discusses the Configurable implementation of LFSR. Section V highlights a basic reversible gate and the major advantages of reversible technology. The simulation results are discussed in Section VI. Conclusion and the future scope are discussed in Section VII.

II. LITERATURE REVIEW

A Configurable Linear Feedback Shift Register has been discussed before as well as realized on hardware by S Mishra R Tripathi and D Tripathi which focuses on the implementation of CLFSR in VHDL [1] and evaluates its performance with respect to logic, speed and memory requirement.

A Low Power Reconfigurable LFSR was discussed by L Shaer, T Sakakini, R Kanj, A Chehab and A Kayssi deals with the working of LFSR and various methods to reduce the power losses. Which majorly dealt with four types of methods that can reduce power loss in a LFSR. Those are, Reconfigurable LFSR, Power Gating of the XORs, Isolating the inputs to the XORs, Limiting the Number of XORs. We propose another method to reduce power dissipation that is, by using Reversible logic

A concept of the reversible memory cell was first introduced and shown by Fredkin and Toffoli [2] which introduced the design of a JK Latch.

In 2005 Thapliyal et.al. [3] introduced the master-slave and flip-flop configuration of all reversible latches such as D-Latch, T-Latch etc. Similarly, a SR-Latch with no fan-out problem that was available in the design by Picton was introduced by Rice [4] in 2006 which was used to subsequently design other latches using this SR-Latch. In 2008, a brief note on how reversible logic elements and reversible sequential circuits could be used to make a universal reversible computer was given by Morita [5], but a practical hardware design was not presented.

In this paper we have discussed the development of a configurable implementation of the LFSR in Verilog and reversible technology.

III. Linear Feedback Shift Register

A linear feedback shift register is the combination of a series of flip flops and XOR or XNOR logic gates that produces a pseudo random cycle output through a sequence of binary values after certain number of clock cycle.

Although it has a simple structure, the LFSR are based on a more complex mathematical equation and find its applications in many fields.

The initial value given of the Linear feedback shift register is called the input seed sting, and because the operation of the shift register is deterministic, the pseudo random stream of values produced by it is completely determined by its current (or previous) state. In a linear feedback shift register (LFSR), input bit is a linear function of its previous state. Likewise, because of these properties, it has a finite number of possible states after which it will eventually enter a repeating cycle.

However, for a more longer non-repetitive cycle wherein the produced sequence string can appear more random, a well-chosen feedback function of exclusive-not-OR logical gates are used. Therefore, it is a very crucial component in a lot of systems where, it finds applications in important roles such as cryptographic applications, checker circuit, CRC generation, gold code generator, for designing encoders and decoders and for generation of pseudorandom sequence to ensure security.

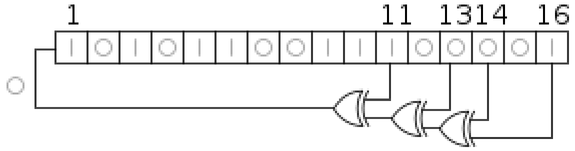


Fig 1: Fibonacci Implementation

In a conventional linear feedback shift register, the number of taps and the feedback function is constant and thus with modifications and changes in technology and string sizes used for applications the conventional LFSR cannot be of much reliability. Whereas, a configurable-LFSR can adapt to these variables as it has configurable and adjustable string size and generates a longer sequence-cycle using a well-defined variable feedback function relative to the size of bits of the string.

A configurable linear feedback shift register can be implemented in two ways, i.e. Galois implementation and Fibonacci implementation.

An Configurable linear feedback shift register can be implemented using either of two styles – Galois or in-line Implementation and Fibonacci or out-of-line implementation. In this paper we have implemented the Fibonacci style of implementation i.e. there are taps on the bits of a LFSR that decide the input string of the next stage as shown in Figure 1.

In Fibonacci Implementation Style, there are taps on the bits of a linear feedback shift register that decide the further generated string in the sequence.

A. Output Stream Properties of Linear Feedback Shift Register

The distribution of ones and zeroes almost equals the statistical expectation value for a truly random sequence. However, the probability of finding exactly this distribution in a sample of a truly random sequence is rather low

LFSR output streams are deterministic. If the present state and the positions of the XOR gates in the LFSR are known, the next state can be predicted.

The output stream is reversible; an LFSR with mirrored taps will cycle through the output sequence in reverse order.

The value consisting of all zeroes cannot appear. Thus, an LFSR of length n cannot be used to generate all 2^n values.

IV. Configurable LFSR

A Configurable linear feedback shift register is the combination of a series of flip flops and XOR or XNOR logic gates where the input string is a linear function (XNOR or XOR) of the previous state linear feedback shift register output and further various linear feedback shift register parameters are configurable. Hence, creating a longer and more efficient pseudo-random cycle of output string whose output depends on the number of stages and the length of seed string of the Configurable linear feedback shift register.

The Configurable linear feedback shift register plays a very vital role in many industries such as security and telecommunication system as random number generator.

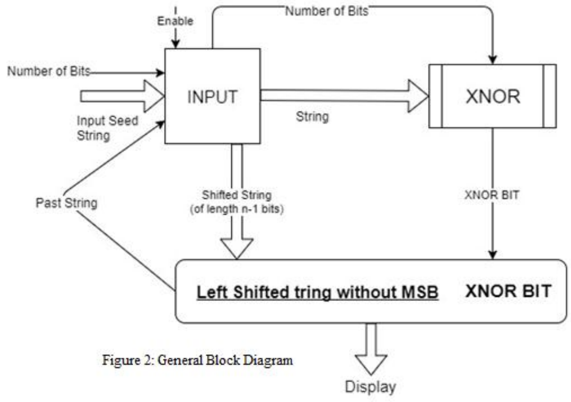


Figure 2: General Block Diagram

There are several configurable parameters of the designed CLFSR like [1]:

1. Number of Bits or Stages of the CLFSR and thus a CLFSR can also be called N-bit LFSR wherein 'N' is a variable value set by the user.
2. Tap positions and Number of Taps in the Configurable linear feedback shift register. Tap is the input line to the XNOR Gate whose output is taken as the input for the next stage of the CLFSR. Thus, varying of tap location and number of taps helps in creating a larger cycle of pseudorandom numbers before the output starts repeating.
3. The initial value or the seed string of the CLFSR of length, 'N' bits.

Figure 1 is the general block diagram of the implemented configurable linear feedback shift register. The different functions of this block diagram are:

Enable Pin- Enable Pin is a one-bit active-high control signal used to start or stop the machine from performing shift operations. Whenever the enable pin is set '1' the CLFSR operates in normal mode. As soon as the enable pin is set '0' the machine completes the current shifting cycle and stops operation.

Input Seed String- This is the initial input string of 'n' bits used for generation of the XNOR Bit and shifting purpose. This string is accepted only once and the string is operated on until enable is set to low. It can also be shown in the following format: Dn, Dn-1... D0 for 'n' number of bits.

Number of Bits (n) - The number of bits is the length of the input seed string that is used to detect the MSB and LSB of the string as well as help on selecting a well-chosen feedback function of exclusive-not-OR logical gates and finding the bits necessary for so. Thus, to create a configurable-LFSR this input is of vital necessity.

Input Block- This block takes all the inputs necessary for operation like the input seed string, string size, enable signal etc. It also has a shift register that left shifts the data for the first stage. After this it takes the newly generated string (of size 'n' bits with the past XNOR Bit) and left shifts it and forwards it to the Display Block. It also sends the 'n' bit string to the XNOR Block with its bit-size for generation of a defined XNOR Bit.

XNOR Block- This block takes the input string and string size from the INPUT Block and using a predefined well-chosen feedback function of exclusive-not-OR logical gates it generates an 'XNOR Bit' that is the LSB of the new shifted string. This is a vital block for a more efficient operation and to achieve longer cycles thus creating a better sequence string that appears random.

Display Block- This block takes the left shifted string from the Input Block and the generated XNOR Bit from the XNOR Block and displays the newly generated string. Further, its send this signal back to the Input Block for generation of the next string in the sequence. It is used to show the bits to the user.

Further, this block can be modified to integrate the CLFSR with applications using it like Checker circuit, CRC generation, generation of pseudorandom sequence to ensure security and many such applications.

As then the new bit to be entered will always stay '0'. This lock-down situation can be avoided and tackled using an XNOR Logic Gate implementation in a configurable linear feedback shift register as even if the string changes to "00000000" for an 8-bit linear feedback shift register the output from any two taps will generate a high signal bit (1) and thus there will be no lockdown. Thus, the repetition of cycles in this method is easier to perform and can be implemented with less errors.

Figure 3 is the flowchart of the process used to implement the Configurable linear feedback shift register. This flowchart is proposed as the technique to implement a N-bit Configurable linear feedback shift register in Verilog.

V. BASIC REVERSIBLE GATE

The number of inputs and outputs in a reversible logic circuit is the same, and there is one-to-one mapping between vectors of inputs and outputs; thus, the input states can be always reconstructed using the output states. A computation is reversible, if it is always possible to uniquely recover the input, given the output. Each gate can be made reversible by adding some additional input and output wires if necessary.

One of the major constraints for the synthesis of reversible logic is that, fan-out is not allowed. Another thing to be kept in mind while designing reversible sequential circuits is that , there combinational parts have to be reversible to allow feedback. A gate with k inputs and k outputs is called a k x k gate.

Reversible circuits have functionality outputs and garbage outputs that are needed only to achieve reversibility.

Three gates, the wire (buffer) gate, the Not gate and the Swap gate are all naturally reversible. Other gates like the Feynman gate, the Toffoli gate and the Fredkin gate are not naturally reversible and hence require garbage outputs to be added.

The simplest reversible gate is the 1x1 NOT gate with zero quantum cost.

Figure 4: Symbol of NOT gate:

The 2x2 Feynman gate is also called controlled-not (CNOT) or “quantum EXOR”, whose functions are realized as

$$P = A$$
$$Q = A \oplus B$$

Where A and B are the inputs, while P and Q are the outputs. Thus, when A = 0 then Q = B and when A = 1 then Q = ~B, this is why it is called controlled not. With B = 0 Feynman gate is used as a fan-out gate or a copying gate (P = A and Q = A).

Figure 5: Symbol for Feynman gate:

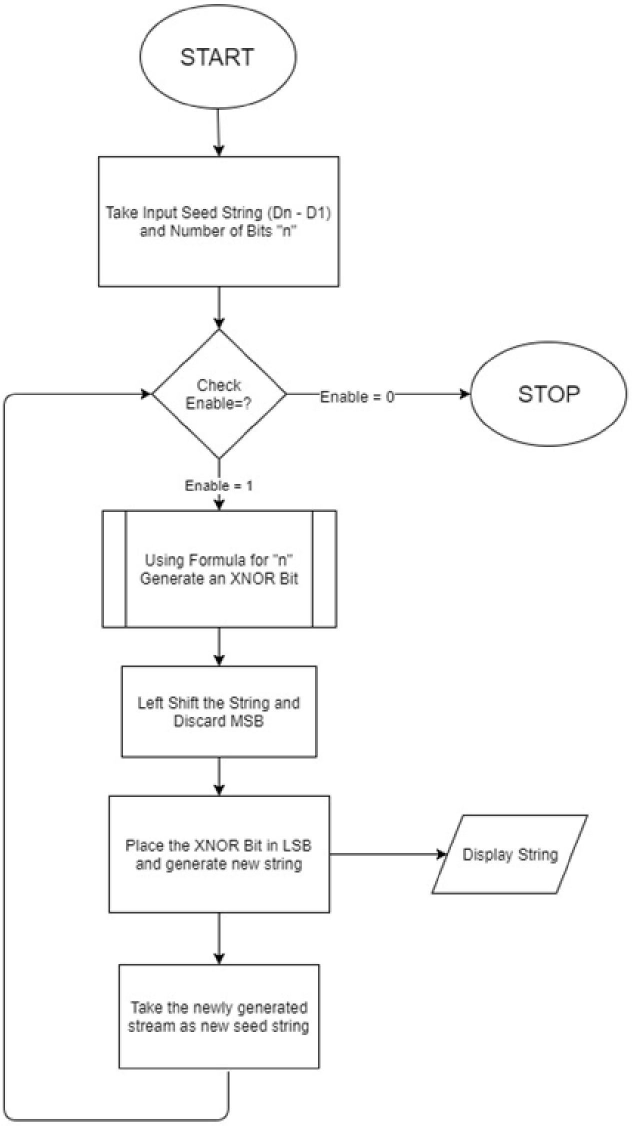
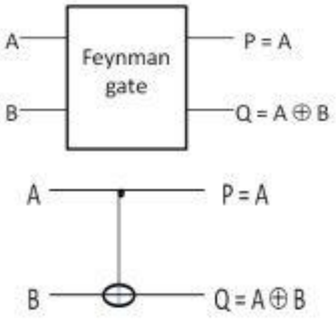

START
Take Input Seed String (Dn - D1) and Number of Bits "n"
Check Enable=?
Enable = 0
STOP
Enable = 1
Using Formula for "n" Generate an XNOR Bit
Left Shift the String and Discard MSB
Place the XNOR Bit in LSB and generate new string
Display String
Take the newly generated stream as new seed string

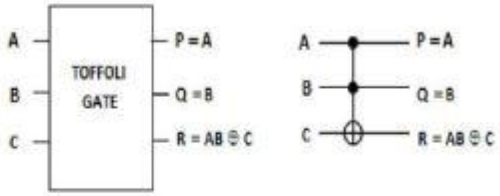
Figure 3: Flowchart of Implementation



The 3x3 Toffoli gate is also known as 3x3 Feynman gate or controlled-controlled-not. From the truth table, it can be seen that when A and B equal one then R = C, this is why this gate is called controlled-controlled-not, because it has two control inputs A and B to invert the third input C. it can be denoted using equations as,

$$P = A$$
$$Q = B$$
$$R = AB \oplus C$$

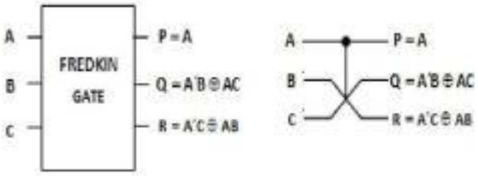
Figure 6: Symbol of Toffoli gate:



The 3x3 Fredkin gate is also called controlled SWAP (CSWAP). The 3x3 Fredkin gate is a permutation gate, it permutes the data inputs of its two multiplexers under control of the control input of these multiplexers. This control input is also an output from the Fredkin gate.

$$P = A$$
$$Q = B \oplus AB \oplus AC$$
$$R = C \oplus AB \oplus AC$$

Figure 7: Symbol of Fredkin gate:



VI. CLFSR Simulation Results

The configurable linear feedback shift register is implemented using XNOR logic gates and Poly String is used for the number and location of taps on the seed string. As we can see that the output stage is a linear XNOR function of the previous output state. Also, the circuit blocks show that the configurable linear feedback shift register is a left shift register.

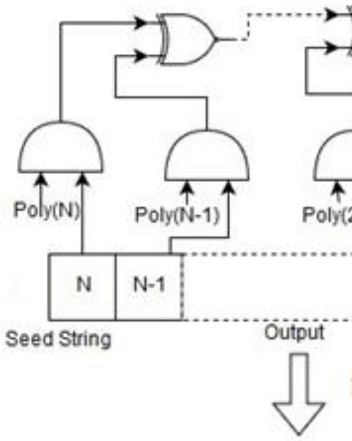
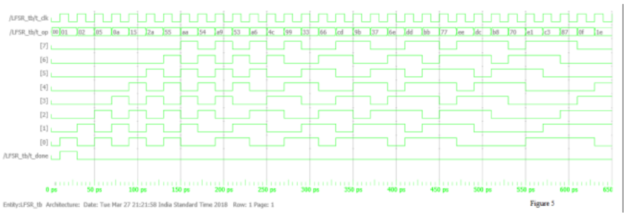
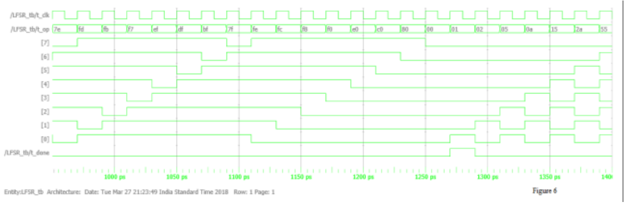


Figure 8 : Implementation Circuit

Further for N=8 the system is simulated and studied using Quartus II and ModelSim Altera. The figures below show the simulation results that will be displayed after each cycle and the clock is set at 10ps.





The simulation shown in Figure 5 and Figure 6 is for N= 8 and the poly is placed at bit 0 and bit 7, i.e. MSB and LSB. Thus, for input seed string = “00000000” and Poly= 10000001. Also, we can see that after many cycles the done bit goes HIGH. This time can be even more increased with the right choice of poly bits by placing proper taps on appropriate bits.

VII. Conclusion and Future scope

Thus, we implemented a configurable linear feedback shift register on Altera Cyclone II DE-1 Board FPGA using Verilog language for programming it and Quartus II and ModelSim Altera for simulation and study purpose. Also, we implement a design that can be altered using a simple algorithm. This configurable behavior is useful to adapt the system/implementation to the technology in which it has to be integrated as well as configurable to the needs and requirements of the user. Thus, it is seen as a better implementation than the conventional linear feedback shift registers in not only being adaptable to various requirements but also to generate a better sequence of pseudorandom numbers.

We also observe the various aspects of reversible technology and reversible logic gates and their implementation for logical circuits. Thus, there is a vast future scope for reversible logic to be integrated with our design of a configurable linear feedback shift register to further study it and understand the profitable aspects of such an implementation.

REFERENCES

[1] Efficient Shift Registers, LFSR Counters, and Long Pseudo-Random Sequence Generators, Application Note, Xilinx Inc.

[2] S Mishra, R Tripathi and D Tripathi, "Implementation of Configurable Linear Feedback Shift Register in VHDL" 9781-1-5090-2118-5/16/$31.00 ©2016 IEEE

[3] Lama Shaer, Tarek Sakakini, Rouwaida Kanj, Ali Chehab and Ayman Kayssi," A Low Power Reconfigurable LFSR "18th Mediterranean Electrotechnical Conference MELECON 2016, Limassol, Cyprus, 18-20 April 2016

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

[5] 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.

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

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

[8] Efficient LFSR, XILINX, XAPP 052 July 7,1996 (Version 1.1)

[9] P. Kaye, R. Laflamme, M. Mosca, An Introduction to Quantum Computing. Oxford University Press Inc., Oxford, 2007

[10] P. Yelekar, S. Chiwande, Introduction to reversible logic gates and its applications, 2nd National Conference on Information and Communication Technology (NCICT) 2011, proceedings published in International Journal of Computer Applications (IJCA)

[11] Reversible logic synthesis methodologies with applications to quantum computing, Springer Publication, 2016, ISBN: 978-3-319-23478-6

Authors Profile

Mr. Harsh Ghelani is the final year student enrolled at *KJ Somaiya College of Engineering, Mumbai* for the course of Bachelor's in technology in Electronics. He is actively involved in research and industrial projects and extra-curricular courses in cryptography, data mining, finance and power electronics.

Mr Nilesh Jha is currently enrolled at *KJ Somaiya College of Engineering, Mumbai* for the course of undergraduate degree in technology. He is actively involved in research projects and a highly active writer on many forums and Quora.

Mr Rohan Naik is an undergraduate student in final year for B. Tech in Electronics Engineering from *KJ Somaiya College of Engineering, Mumbai*. He is actively involved in research projects and a highly active participant in multiple debate groups and MUNs.

Prof Pragya Gupta is currently an assistant professor at *KJ Somaiya College of Engineering, Mumbai* in the Electronics department. With 8 years of industrial and 5 years of teaching experience she is an actively involved in VLSI and MIS research.