JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

LFSR Design on Xilinx Spartan FPGA to Generate Pseudorandom Sequence Number

Debarshi Datta, Bipa Datta
ECE Dept., Brainware Group of Institutions
MAKAUT
Kolkata, India
Debarshidatta7@gmail.com,bipadatta@gmail.com

Himadri Sekhar Dutta
IEEE Member
Kalyani Government Engineering College
Nadia, India
himadri.dutta@gmail.com

***Abstract*— Pseudorandom number generators (PRNGs) are important role in cryptography application. Hardware based Field Programming Gate Arrays (FPGA) is one of the most valuable devices in hardware industry. This paper presents multi bit linear feedback shift register (LFSR) based PRNGs circuit designed with hardware description languages (HDL). In multi bit LFSR system, multiple bits are shift in every clock cycle where a single bit is shift in a conventional LFSR method. This technique is very much applicable in cryptography area. The proposed various bit length multi bit LFSR architectures are synthesized using Xilinx ISE 14.7 and Spartan 6 FPGA to target device XC6SLX45. The result analysis indicates that 128-bit length multi bit LFSR architecture is better performance than other architectures.**

Keywords—LFSR; multibit; FPGA;VHDL;

Introduction

A linear feedback shift register (LFSR) is a common device used in built-in-test pattern generation (TPG) due to its reduced hardware requirements. Its behavior is determined by a characteristic polynomial. LFSRs are constructed by D Flip-Flop and two input XOR/XNOR gates. Targeted FPGA platform In this project, we do a synthesis of LFSR design on SPARTAN FPGA devices, measuring the performance considering the time, area, memory and power. Xilinx Spartan-6 FPGA offers advanced power management technology. The Xilinx, Spartan-6 FPGA family delivers an optimal balance of low risk, low cost, low power, and performance for cost-sensitive applications.

LFSRs can be applied in generating pseudo-random numbers, pseudo-noise sequences, fast digital counters, whitening sequences, cryptography, etc., and they can be implemented in both software and hardware. It uses Ex-OR/Ex-NOR logic gates along with n-bit sequential shift register which stores data in linear fashion in such a way that input is shifted down to output in line. In LFSR feedback-input bit is an output of a linear function of two or more of its taps (previous states). Due to its light weight operation and simple hardware design LFSR is widely used in digital programmable devices like microcontrollers, processors, DSPs, FPGAs, CPLDs, PLDs, etc. in order to get accountably infinite (long) sequences of random numbers.

Physical Random Number Generators (PRNGs) are widely used in cryptography, data science, gaming, music, etc. Their are various recent methods for PRNGs as BBS (Blum Blum Shub), LCG (Linear Congruential Generator), etc. These recent methods are having certain drawbacks such as slow generation of random sequence, takes more time for reseeding, poor quality sequence, having less sequence length period as compared to new method.

To overcome problems such as slow computation, small sequence length, poor quality sequence, slow reseeding, etc. a Linear Feedback Shift Register (LFSR) can be used which is having faster computation, easy implementation, and extended period length which is able to generate random high quality sequence more than four billion.

LFSR project status, device utilization summary and detailed reports showing in figure1.

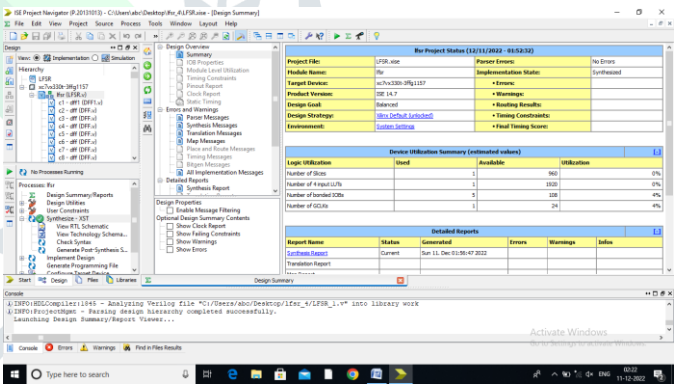

Figure1. Project Status, Summary and Detailed Report

LITERATURE REVIEW

Balwinder Singh et al., in 2009 proposed low power LFSR for generating test patterns which reduces power dissipation. Dynamic power dissipation increases because of more switching activity means more transitions. Correlation increased by generation of intermediate test vectors between successive test patterns. This approach achieved 46% less power dissipation as compared to conventional LFSR. X power analyzer is used by the author to analyze power of proposed design.

Rahul Dashrath Gavas, Geeta U Navalyal (2017) Fast and secure random number generation using low-cost EEG and pseudo random number generator(Department of CSE, KLE Dr, M.S Sheshgiri college of engineering and technology, Belgaum, India.

S. Ehsan Razavi , Javad Royaei, Mehdi Bahadorzadeh (2015) Design a low current and high speed shift register based on D type flip flop

Roshni Oommen, Merin K George, Sharon Joseph (2015) Study and Analysis of Various LFSR Architectures

A. A. Borysenko, O. Y. Horiachev, S. M. Matsenko, O. M. Kobiakov (Sumy state of university)

Standard LFSR

In standard LFSR, the input for the shift register is a feedback of modulo-2 sum of the binary weighted taps, where modulo2 sum is performed using an exclusive-OR (XOR). Architecture of standard LFSR is given in figure2.

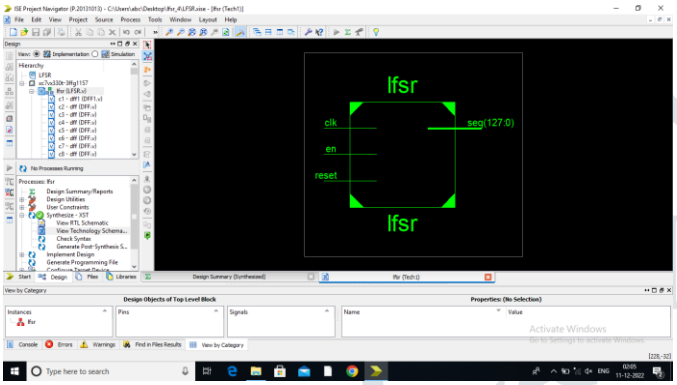

Figure2. Standard LFSR

At input side it has clock, enable and reset and at output side it has sequence from (0 – 127) bit. LFSR is shift register which generates sequence of binary values. The sequences are repetitive in nature known as pseudorandom sequences. Feedback paths are established after registers in the LFSR structure called taps and constitutes exclusive-OR or exclusive-NOR to make random series.

Matrix form of LFSR

LFSR in matrix form represented as X(t+1)=A X(t) .where A is called transition matrix and define LFSR configuration. A matrix is given in the form of h1, h2……..hn-1.

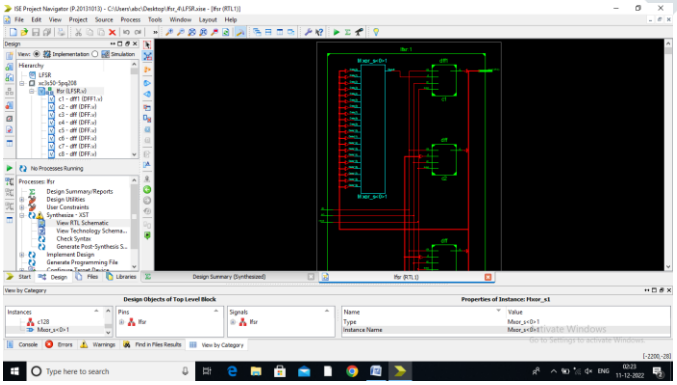

Figure3: LFSR RTL

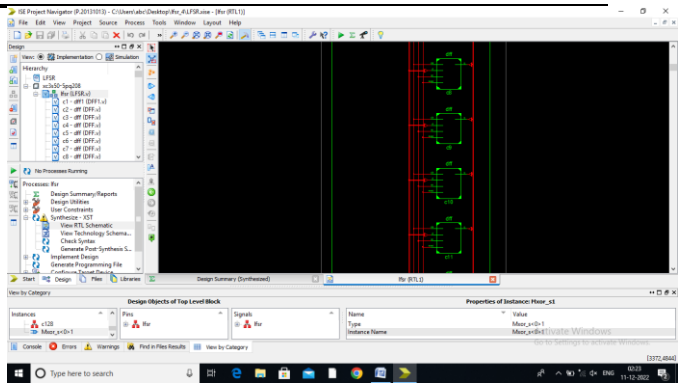

Figure4: LFSR RTL

Figure 3 and figure4 are showing the LFSR RTL for 128 bit.

Block diagram of D-Flip flop

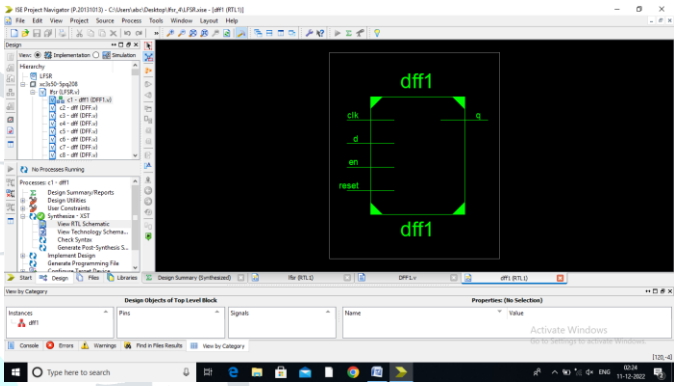

Figure5: D-Flip flop

A D (or Delay) Flip Flop (Figure 5) is a digital electronic circuit used to delay the change of state of its output signal (Q) until the next rising edge of a clock timing input signal occurs.

It has Clock, delay, enable, and reset at the input side and q at the output side.

Simulation Results

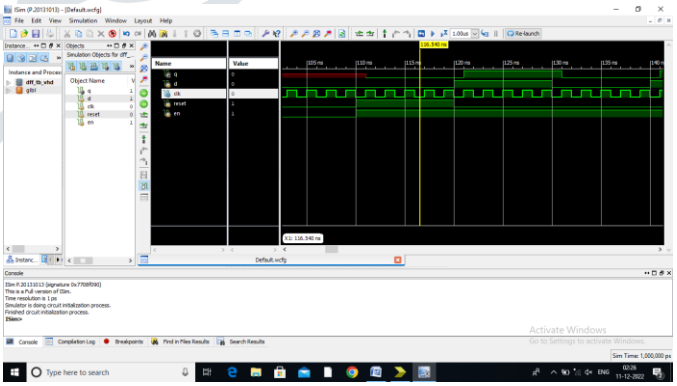

Figure6: Simulation Result (12 -bit) standard LFSR

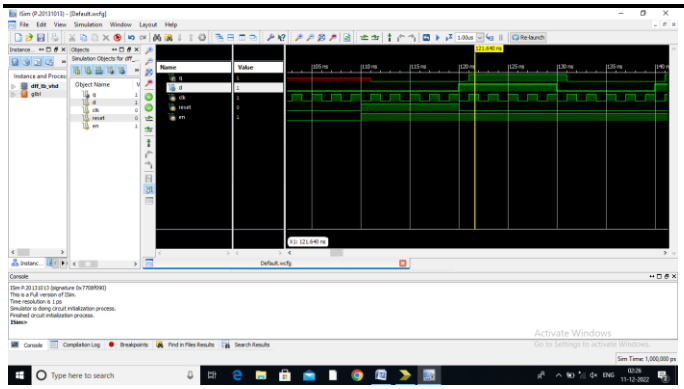

Figure7: Simulation Result of 4-step of length-12 LFSR

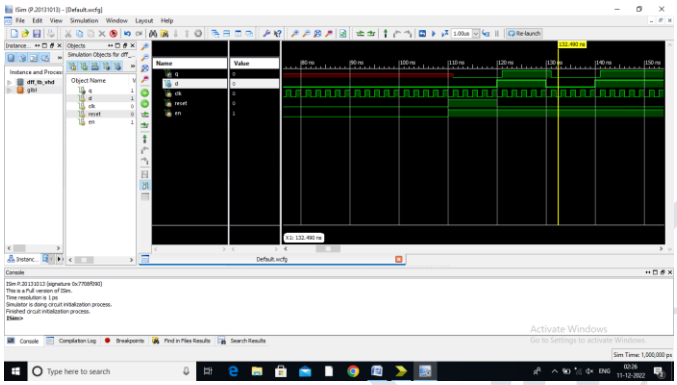

Figure8: Simulation Result of 8-step of length-12 LFSR

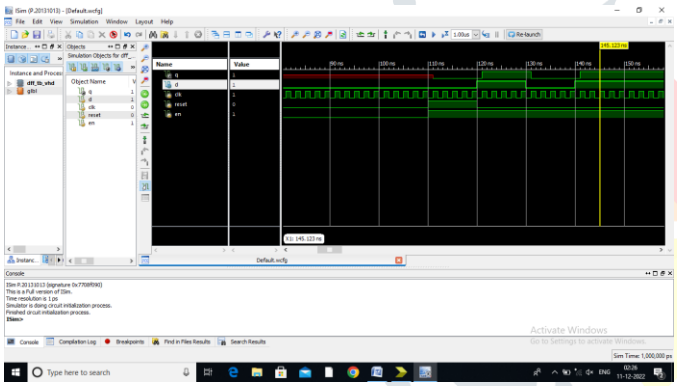

Figure9: Simulation Result of 4-step of length-12 LFSR

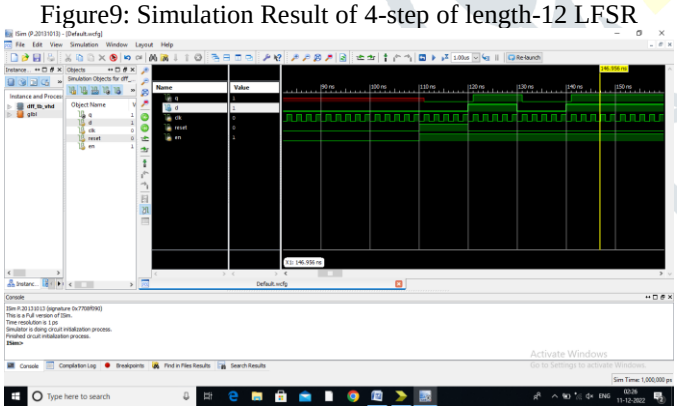

Figure10: Simulation Result (Delay)

Synthesis Parameter	Utilization summary of standard and various steps multi bit LFSR		
	Used in 12- bit standard LFSR	*Used in 4-step length12 LFSR*	*Used in 8-step length12 LFSR*
Number of Slice registers	12	12	12
Number of Slice LUT	5	4	8
Number of LUT Flip flop pairs used	8	12	8

Figure11: Utilization summary of standard and various steps multibit LFSR

Conclusion

Linear feedback shift registers play very important role in many fields like for testing, cryptography, BCH and CRC encoders. In cryptography multi bit LFSR is used because it is more secure as compare to conventional LFSR. When steps is equal to length of LFSR then all bits are based on XOR combination, so multi bit LFSR is used in more secure applications. Parallel LFSR is used to increase throughput of the system. In research papers of parallel LFSRs performance analyzed in terms of number of ones, number of XOR gates, Delay element and Critical path delay. This Area Time product decides the hardware complexity of any system. It depends upon the selected transformation matrix. This paper can help to find best transformation matrix which can reduce hardware complexity in terms of AT value.

REFERENCES

[1] Parhi, K.K., 2004, Eliminating the fanout bottleneck in parallel long BCH encoders, IEEE Transactions on Circuits and

[2] Systems I: Regular Papers, 51(3), pp.512-516.

[3] Kennedy, C. and Reyhani-Masoleh, A., 2009, June. High-speed CRC computations using improved state-space

[4] transformations, In Electro/Information Technology, 2009. eit'09. IEEE International Conference on (pp. 9-14). IEEE.

[5] Ayinala, M. and Parhi, K.K., 2010, October, Efficient parallel VLSI architecture for linear feedback shift registers, In

[6] Signal Processing Systems (SIPS), 2010 IEEE Workshop on (pp. 52-57). IEEE.