An Efficient Pseudo Random Number Generator for Cryptographic Applications

K. Chandra Sekhar, K. Saritha Raj

Abstract: ***LFSR based Pseudo Random Sequence Generator (PRSG) technique is used for various cryptography applications such as Data Encryption keys, Bank Security communication channels etc. The total number of Random States generated using LFSR are 2^n-1 and depends on the Feedback Polynomial used in the design. Linear Feedback Shift Register(LFSR) counter is very effective when compared to other counters used in cryptographic applications especially in terms of Hardware, speed of operation and it is also less prone to Glitches. In this paper we implemented LFSR counter and it is compared with Binary and Gray counters to observe the performance of the counter in terms of Hardware and Speed. The analysis is conceded out to find number of gates, Memory and Speed requirement as the number of bits gets increased.***

Keywords: LFSR, Pseudo Random Sequence Generator, Feedback Polynomial.

I. INTRODUCTION

There are various methods for generating Pseudo-Random numbers and most of them are based, on linear congruential equations which require a number of time consuming arithmetic operations. In contrast, the use of Linear Feedback Shift Registers permits very fast generation of Binary sequences. Shift register sequences of Maximum length (m-sequences) are well suited to simulate truly random sequences . The target device we have used is Xilinx Spartan XC3S 500e and performed simulation and synthesis using Xilinx . FPGA is a predesigned re-configurable IC . It can be re-configured any number of times according to the specification of design. The FPGA configuration is generally defined using a hardware description language (HDL), similar to that used for an Application-Specific Integrated Circuit (ASIC) . The HDLs are VHDL and Verilog. We preferred Verilog HDL for programming because it is widely used and less complex.

A. Linear Feedback Shift Register

LFSR is most often a shift register whose input bit is driven by the exclusive-or (XOR) of some bits of the overall shift register value. The initial value of the LFSR is called the seed[1]. Because the register has a finite number of possible states, it must eventually enter a repeating cycle.LFSR with a well-chosen feedback function can produce a sequence of bits which appears random and which has a very long cycle. Applications of LFSRs include generating pseudo-random numbers, pseudo-noise sequences, fast digital counters, and whitening sequences.

Manuscript Received on October 2014.

K. Chandra Sekhar, Dept. of Electronics and Communication, MVGR College of Engineering, Vizianagaram, India.

Mrs. K. Saritha Raj, Dept. of Electronics and Communication, MVGR College of Engineering, Vizianagaram, India.

B. LFSR as a Counter

The repeating sequence of states of an LFSR allows it to be used as a clock divider, or as a counter when a non-binary sequence is acceptable as is often the case where computer index or framing locations need to be machine-readable. LFSR counters have simpler feedback logic than natural binary counters or Gray code counters, and it can operate at higher clock rates[2]. However it is necessary to ensure that the LFSR never enters an all-zeros state. One can obtain any other period by adding to an LFSR that has a longer period some logic that shortens the sequence by skipping some states.

C. LFSR Counter vs Other Counters

Binary counters generally use flip-flops, half adders, and a high-speed carry chain. The delay associated with a Binary counter depends on the number of bits in the adder/carry chain circuit. In contrast, LFSR counters use only flip-flops and XOR gates. Their delay is independent of the number of bits in the counter. Counters such as Binary, Gray suffer problem of power consumption, glitches, speed, and delay because they are implemented with techniques which have above drawbacks[3]. They produce not only glitches, which increase power consumption but also complexity of design. The propagation delay of results of existing techniques is more which reduces speed & performance of system[4].

II. MAXIMUM LENGTH LINEAR FEEDBACK SHIFT REGISTER(LFSR)

Maximum-length Linear Feedback Shift Register produces an m-sequence (i.e. it cycles through all possible 2^n-1 states within the Shift Register. The sequence of numbers generated by this method is random and the period of the sequence is (2^n - 1), where n is the number of Shift Registers used in the design. Note that the only signal necessary to generate the test patterns is the clock. Any long LFSR counter generates a long pseudo-random sequence of zeros and ones[2]. The sequence is not exactly random since it repeats eventually, and it also follows a mathematically predictable sequence. But for most practical purposes it can be considered random. An n-bit LFSR counter can have a maximum sequence length of 2^n-1. In that case, it goes through all possible code permutations except one, which would be a lock-up state. LFSR outputs are
traditionally labeled 1 through n, with 1 being the first stage of the shift register, and n being the last stage[4]. This is different from the conventional 0 to (n-1) notation for binary counters.

A. Rules for selecting Maximum Length Feedback Polynomial

Linear Feedback Shift Registers produce the Maximum Length sequence, when the characteristic polynomial used in the design is of Maximum Length. The choice of LFSR

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

length, gate type, LFSR type, maximum length logic, and tap positions allows the user to control the implementation and feedback of the LFSR, which, in turn, controls the sequence of repeating values the LFSR will iterate through[5]. Out of which Maximum length logic plays a crucial role. Hence proper care should be taken while choosing a Maximum length feedback polynomial. The following things have to be noted while selecting Maximum Length Feedback Polynomial

- The initial value of the LFSR is called the seed. The seed value can be anything except all 0s i.e., the Pseudo Random sequence must start in a non-zero sequence.
- The 'One' in the Maximum length Feedback polynomial sequence corresponds to the principal input of the shift register.
- LFSR will only be Maximum length if the numbers of taps are even.
- Tap values in maximal LFSR should be relatively prime.
- The first and last taps should always be connected as input and output taps respectively.
- There can be more than one Maximum-length tap sequence for a given LFSR length.. If the tap sequence, in an n-bit LFSR, is $[n, A, B, C, 0]$, then the corresponding 'mirror' sequence is $[n, n - C, n - B, n - A, 0]$.

III. IMPLEMENTATION OF LFSR BASED PRNSG

Pseudo Random Number Sequence Generator is generated in Verilog HDL according to the following circuit based on the concept of shift register.

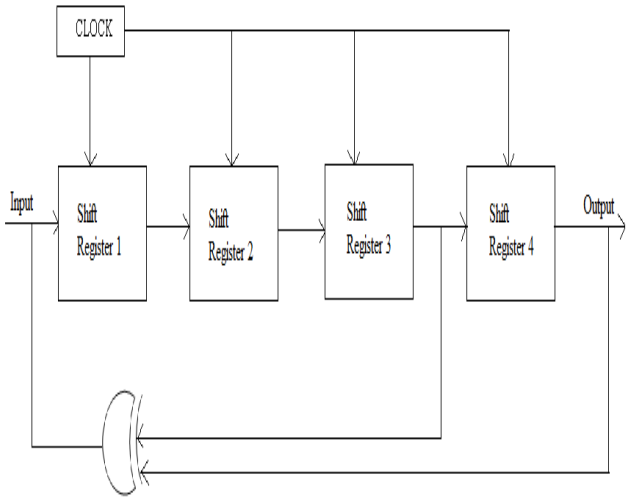

Figure 1. Block Diagram of 4 Bit LFSR Counter

A.Operation of LFSR Counter

When the clock is active, the seed value ('1') is fed to first Shift Register and is stored in the first shift register. Since in the initial cycle no operation is performed on registers, all the other Registers contain '0's and in the later cycles as the values are shifted and Exored simultaneously, new patterns are generated as the output and a total of 2^n -1 random patterns are generated.

IV. RESULTS AND COMPARISON

A. Simulation Results

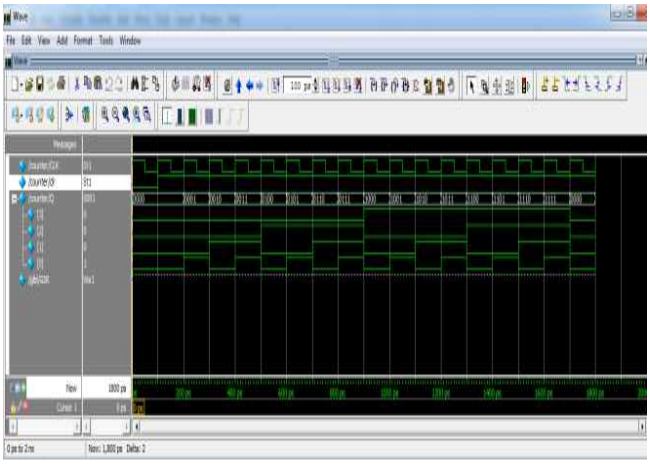

Figure 2: Simulation results for 4 Bit Binary Counter

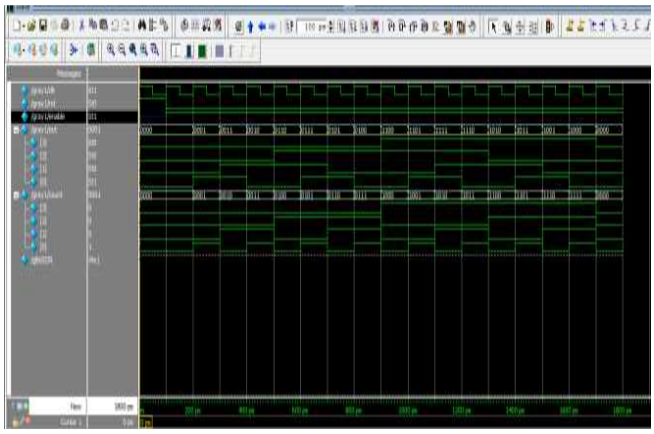

Figure 3: Simulation results for 4 Bit Gray Counter

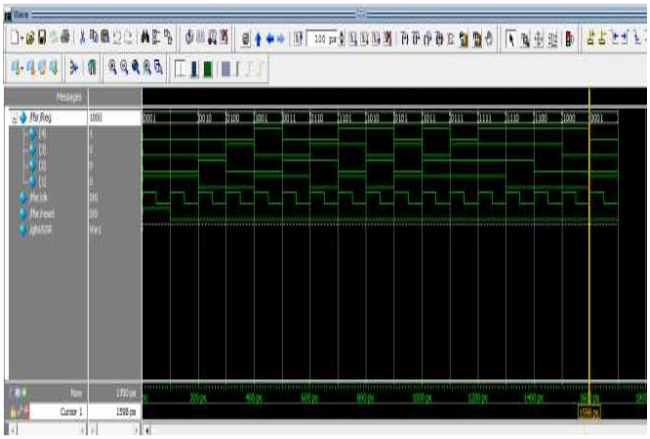

Figure 4: Simulation results for 4 Bit LFSR Counter

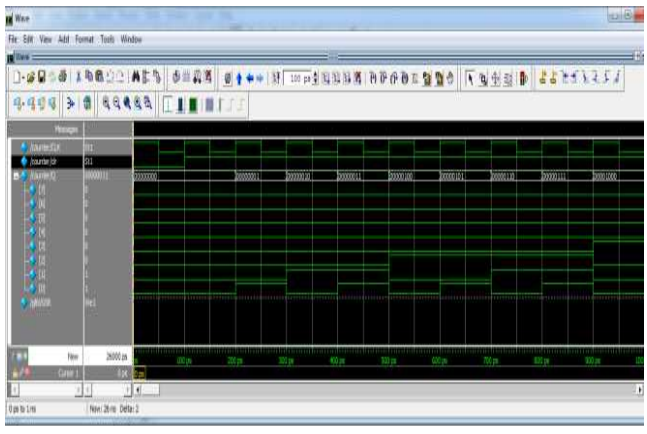

Figure 5: Simulation results for 8 Bit Binary Counter

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

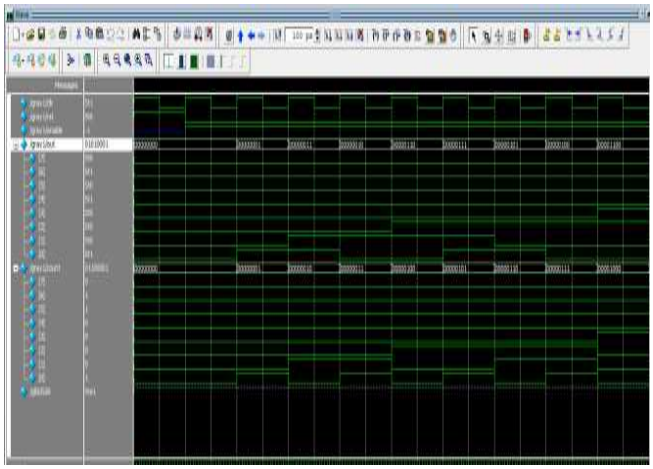

Figure 6: Simulation results for 8 Bit Gray Counter

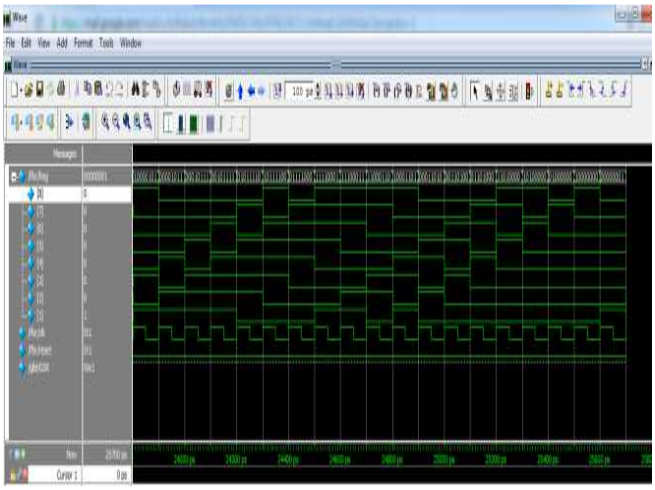

Figure 7: Simulation results for 8 Bit LFSR Counter

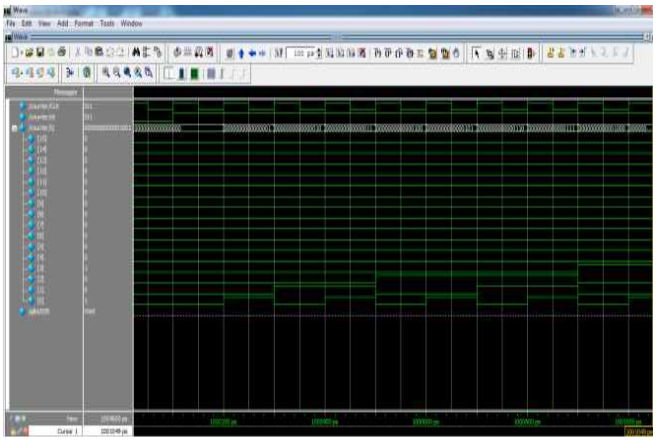

Figure 8: Simulation results for 16 Bit Binary Counter

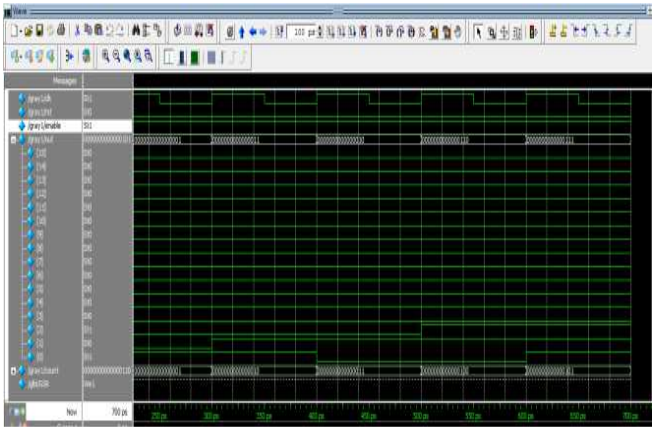

Figure 9: Simulation results for 16 Bit Gray Counter

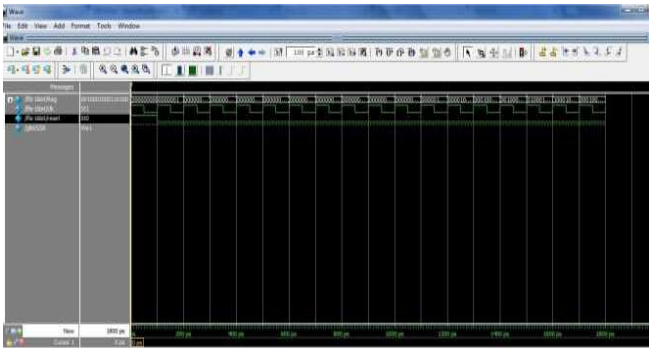

Figure 10: Simulation results for 16 Bit LFSR Counter

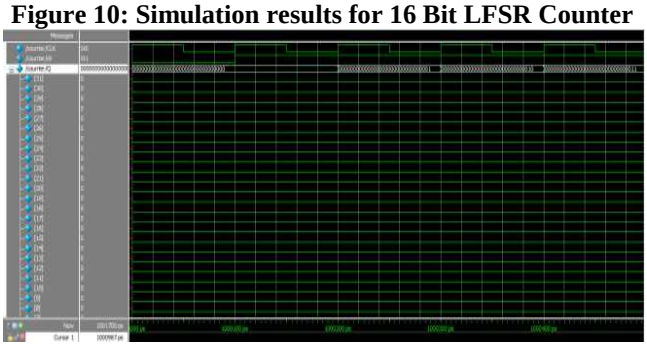

Figure 11: Simulation results for 32 Bit Binary Counter

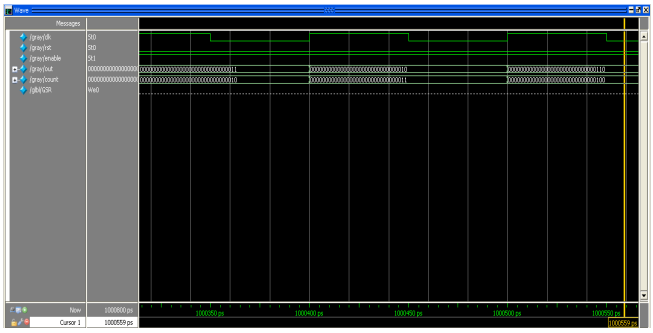

Figure 12: Simulation results for 32 Bit Gray Counter

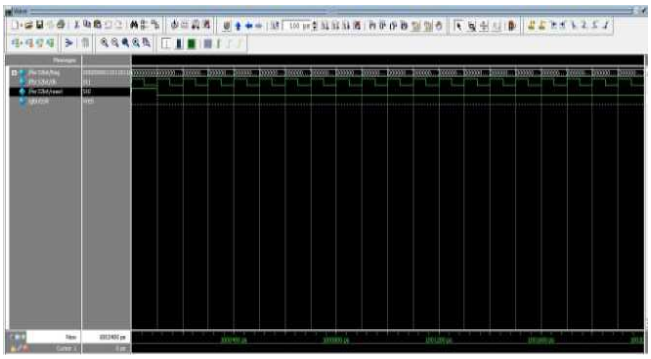

Figure 13: Simulation results for 32 Bit LFSR Counter

B. Comparison of different Counters

Table 1: Design Summary reports for 4 bit Counters

Parameter	Binary Counter	Gray Counter	LFSR Counter
No of Slices	02	03	02
No of Flip Flops	04	04	04
No of 4 i/p LUT'S	04	06	01
Total Pins	06	07	06
Delay	6.621 ns	7.726ns	6.534ns
No of GCLK	01	01	01

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

Table 2: Design Summary reports for 8 bit Counters

Parameter	Binary Counter	Gray Counter	LFSR Counter
No of Slices	04	08	04
No of Flip Flops	08	08	08
No of 4 i/p LUT'S	08	15	01
Total Pins	10	11	10
Delay	6.607 ns	7.799 ns	6.534 ns
No of GCLK	01	01	01

Table 3: Design Summary reports for 16 bit Counters

Parameter	Binary Counter	Gray Counter	LFSR Counter
No of Slices	08	17	09
No of Flip Flops	16	16	16
No of 4 i/p LUT'S	16	31	01
Total Pins	18	19	18
Delay	6.843 ns	8.035 ns	6.534 ns
No of GCLK	01	01	01

Table 4: Design Summary reports for 32 bit Counters

Parameter	Binary Counter	Gray Counter	LFSR Counter
No of Slices	17	34	09
No of Flip Flops	32	32	32
No of 4 i/p LUT'S	33	63	01
Total Pins	34	35	18
Delay	9.929 ns	10.268 ns	6.534 ns
No of GCLK	01	01	01

V. CONCLUSION

LFSR Counter is advantageous over other counters in terms of hardware, speed and area and it is preferable in maintaining good logic density in fabrication process, power optimization, reducing the propagation delay & glitches. The Synthesis and Simulation result of Linear Feedback Shift Register (LFSR) shows that it can generate maximum random output. Definitely 32 bit LFSR Counter will generate a very large Pseudo Random Number sequence which is more secure than other Counters which is very much useful in Cryptographic applications but practically many Cryptographic applications are just limited to 8 bit and 16 bit.

REFERENCES

[1] Rajendra S.Katti, Xiaoyu Ruan and Hareesh Khattri, "Multiple output Low Power Linear Feedback Shift Register Design," IEEE Transactions on Circuits and Systems-I, vol. 53, No.7 July 2006.

[2] Panda Amit K, Rajput P, Shukla B, "FPGA Implementation of 8, 16 and 32 Bit LFSR with Maximum Length Feedback Polynomial using VHDL", *2012 International Conference on* Communication Systems and Network Technologies.

[3] Shiv Dutta Mishra, Prof. Anurag Shrivastav "Design and Analysis of FPGA based cryptographic N-bit parallel LFSR", *International Journal of Latest Trends in Engineering & Technology (IJLTET), NOV 2013*, Vol. 3, Issue 2, ISSN. 2278-621X.

[4] Goresky, M. and Klapper, A.M. Fibonacci and Galois representations of feedback-with-carry shift registers, *IEEE Transactions on Information Theory*, Nov 2002, Volume**:** 48, On page(s): 2826 – 2836.

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

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.