International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Special Issue 31(September, 2015), PP. 305-308

DESIGN OF 8 BIT, 16 BIT AND 32 BIT LFSR FOR PN SEQUENCE GENERATION USING VHDL

Siddesh Gaonkar
M.Tech Scholar - VLSI Design and Embedded systems
Department of Electronics and Communication Engineering
NMAM Institute of Technology, Nitte, India
siddeshgaonkar92@gmail.com

***Abstract*: LFSR (Linear Feedback Shift Register) is commonly employed in various cryptography applications to generate pseudo-random numbers. The overall number of random state produced by the LFSR is determined by the feedback polynomial. LFSR is a shift register in which some of their outputs are taken in exclusive-OR format that forms the feedback path. So it capable to generate maximum of 2^n-1 random sequence by using maximum feedback polynomial. In this paper we implement 8, 16 and 32 bit LFSR for PN sequence generation using VHDL to study its performance and analyse the behaviour of its randomness.**

***Keywords*: LFSR, Pseudo-random numbers, TRNG's, PRNG's, VHDL, FPGA.**

I. INTRODUCTION

With the advancement in VLSI technology, CDMA system has become a highly emerging digital technology for wireless systems. For various cryptographic applications, random numbers are very much essential [1]. The random numbers are required for extensive range of application in Science and Engineering which involve statistical random input. A pseudo random number generator is a device that generates a sequence of symbols or numbers that don't have any well-defined pattern. There are two ways used to generate random numbers, they are 1] True random number generators (TRNG's) and 2] Pseudo-random numbers generators (PRNG's). TRNG's is a random number generator that calculate some physical phenomenon which is estimated to be random and then it pay off for the possible biases in the measurement system and PRNG's uses mathematical algorithms which yield sequences of random numbers, which are determined entirely by an primary value called as a seed [1], [2]. But LFSR provides very fast generation of random sequence.
In this paper, with maximum length feedback polynomial 8, 16 and 32 bit LFSR can produce sequences depending on PRNG and its implementation on FPGA using VHDL. The simulation and synthesis is done on Xilinx ISE 13.2.

II. PN SEQUENCE AND ITS PROPERTIES

The PN sequences are binary sequences of length N = 2^n -1 which fulfils a linear recurrence specified by the primitive polynomial of degree n. Pseudo Noise (PN) sequence is a periodic binary sequence that satisfies three different properties they are: Balance, Run, and Autocorrelation property [3], [4], [5]. Such sequences can be generated by using LFSR by means of well-chosen primitive feedback polynomials completed by a definite finite field.
These properties are listed below, they are

A. Balanced property.
B. Run property.
C. Autocorrelation property.

A. Balanced Property:

In every period of Maximum length (ML) sequence, the total number of ones is one additional than the numbers of zeros.

B. Run Property:

A run is defined as a subsequence of identical symbols within the ML sequence. The length of the subsequence is known as the run-length. The number of runs of zeros is equivalent to the number of runs of ones.
The total number of runs = (N+1) / 2.

C. Autocorrelation Property:

The autocorrelation function of a ML sequence is periodic and binary valued.

$$\boldsymbol{r(i)} = \left(\frac{1}{N}\right) * \sum_{i=1}^{N} (\boldsymbol{Cn})(\mathbf{C\,n - i}) \quad (1)$$

Where N=length or period of PN sequence

$$r(i) = \begin{cases} 1 & \text{for } i = 0 \\ -\frac{1}{N} & \text{for } 1 \le |i| \le N-1. \end{cases} \quad (2)$$

i= lag of the autocorrelation sequence.

III. LINEAR FEEDBACK SHIFT REGISTERS

The LFSR is a shift register which sequences through (2^n-1) states, where n represents the number of shift registers used in designing the LFSR. At every rising edge of the clock pulse the contents of the registers are moved one bit position towards right. There is a feedback from the registers or the taps to the left most register of LFSR via a XNOR or XOR gate [1], [2]. A value of all "1"s as seed cannot be used in the instance of an XNOR gate feedback. Similarly a count of totally "0"s as seed is not valid in the instance of an XOR feedback, since the LFSR would continue in locked-up in these state. The initial value given to the LFSR is called as the "seed".

However, an LFSR by means of a well-chosen maximum feedback polynomial will generate a sequence of numbers which seems to be random and takes a very long cycle [1], [6], [7]. The LFSR block diagram is shown in Figure 1.

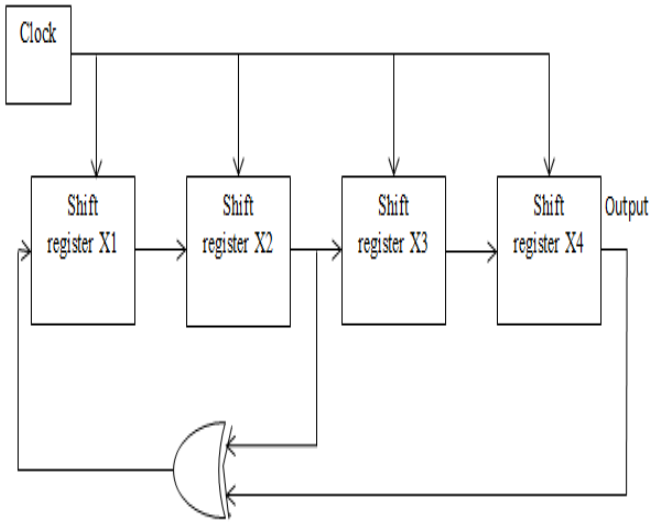


Figure 1: Block diagram of LFSR.

The rules for selecting feedback polynomial are as follows [1], [2]:

A. The 1 in the polynomial never signifies a tap but it represents the input to the first shift register.
B. The power of the terms in the maximum feedback polynomial represents the tap bits. The first bit and the last bit in the feedback polynomial are permanently connected as an input tap and output tap respectively.
C. The LFSR is said to be a maximum length if the number of taps in the feedback polynomial are even.
D. The set of taps taken all together, not pairwise must be relatively prime.

IV. DESIGN OF 8 BIT, 16 BIT AND 32 BIT LFSR

A. Design of 8 Bit LFSR.

The 8 bit LFSR whose maximum feedback polynomial is represented as $X^8+ X^6 + X^5 + X^4 + 1$ will produce 2^8-1 = 255 PN sequence [1], [2]. The block diagram of 8 bit LFSR is shown in Figure 2.

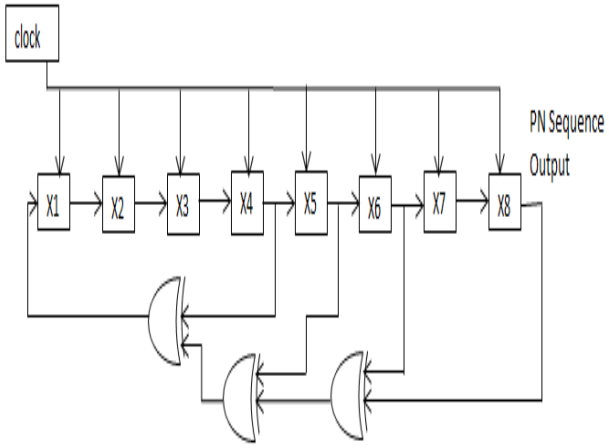


Figure 2: Block diagram of 8 bit LFSR.

B. Design of 16 Bit LFSR.

The 16 bit LFSR whose maximum length feedback polynomial is represented as $X^{16} + X^{14} + X^{13} + X^{11} + 1$ will produces 2^{16}-1 = 65535 PN sequence [1], [2]. The block diagram of 16 bit LFSR is shown in Figure 3.

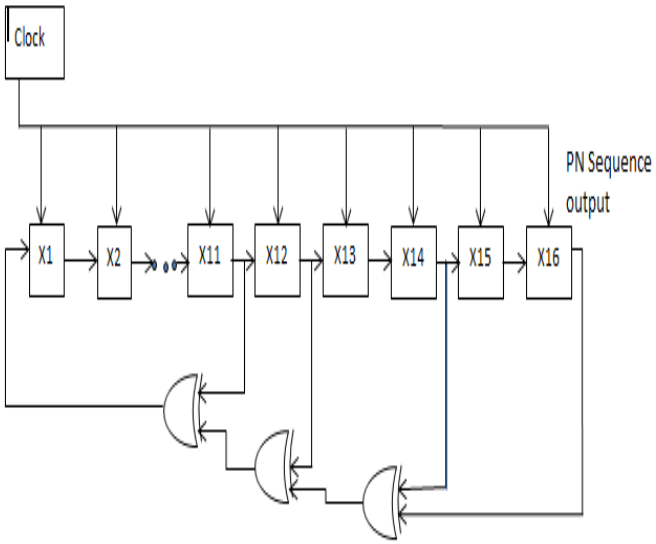


Figure 3: Block diagram of 16 bit LFSR

C. Design of 32 Bit LFSR.

The 32 bit LFSR whose maximum length feedback polynomial is represented as $X^{32} + X^{22} + X^2 + X^1 + 1$ will produce 2^{32}-1 =

4,29,49,67,295 PN sequence [1], [2]. The block diagram of 32 bit LFSR is shown in Figure 4.

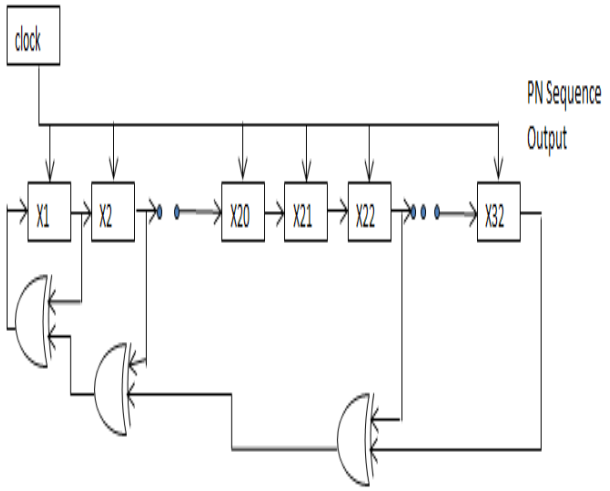
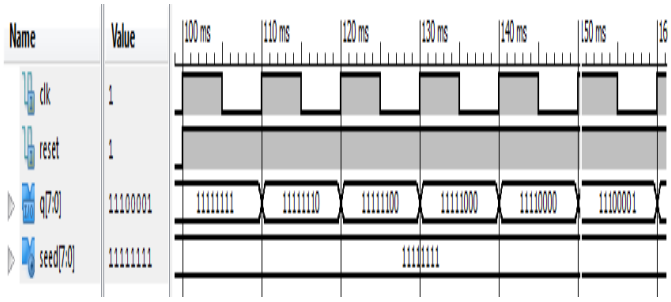


Figure 4: Block diagram of 32 bit LFSR

V. SIMULATION RESULTS

The 8 bit LFSR by means of a well-chosen maximum length feedback polynomial can produce 255 random sequences and it is confirmed from the simulation waveform as shown in the Figure 5.



. Figure 5: Simulation waveform of 8 Bit LFSR.

The 16 bit LFSR by means of a well-chosen maximum length feedback polynomial can produce 65535 random sequences and it is confirmed from the simulation waveform as shown in the Figure 6.

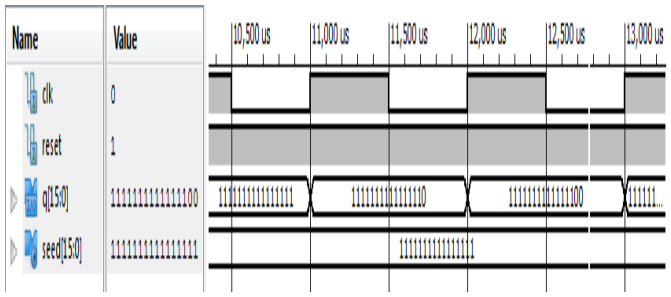


Figure 6: Simulation waveform of 16 Bit LFSR

The 32 bit LFSR by means of a well-chosen maximum length feedback polynomial can produce 4,29,49,67,295 random sequences and it is confirmed from the simulation waveform as shown below in the Figure 7.

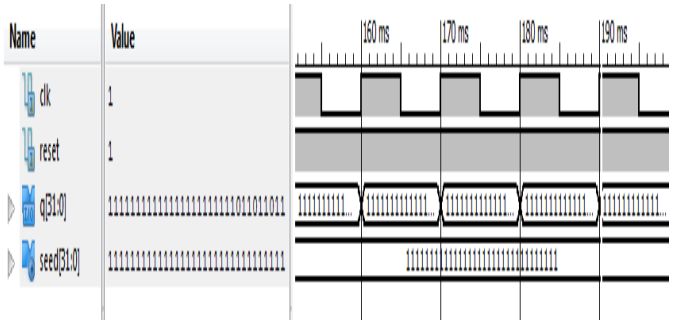


Figure 7: Simulation waveform of 32 Bit LFSR.

TABLE 1: DIFFERENT PERFORMANCE PARAMETERS OF 8, 16 AND 32 BIT LFSR

VI. CONCLUSION

In today's scenario power has become a scarce resource hence proper utilization of power is an important aspect. From the simulation analysis it can be seen that the LFSR with well-chosen maximum feedback polynomial will generate random PN sequence with less amount of power. From the synthesis and simulation result for 8, 16 and 32 bit LFSR will generate maximum randomness using maximum length feedback polynomial. With maximum length feedback polynomial the 64 bit LFSR will produce more randomness, which is much more secure than 8, 16 and 32 bit LFSR. But for practical application 8 bit and 16 bit LFSR is satisfactory for large number of the cryptographic related applications.

REFERENCES

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

[2] Purushottam Y. Chawke, R.V.Kshirsagar, "Design of 8 and16 bit LFSR with maximum length Feedback polynomial using Verilog HDL", *13th IRF International Conference*, ISBN: 978-93-84209-37-7, 20th July-2014, Pune, India..

[3] R.N. Mutagi, "Pseudo noise sequences for engineers", Electronics & Communication Engineering Journal April 1996.

[4] Simon Haykin, Digital communication, JOHN WILEY & SONS INC, second edition, 2009.

[5] Afaq Ahmad, Sayyid Samir Al-Busaidi and Mufeed Juma Al-Musharafi, "Properties of PN Sequences Generated by LFSR – a Generalized Study and Simulation Modelling", Indian Journal of Science and Technology, October 2013.

[6] Kawal .K, Saluja, "linear feedback shift register theory and application", department of electrical and computer engineering, University of Wisconsin-Madison, revised October 1988 updated 1991.

[7] Musher Ahmad and Omar Farooq, "Chaos Based PN Sequence Generator for Cryptographic Applications", International Conference on Multimedia, Signal Processing and Communication Technologies, 978-1-4577-110-7/ 2011.

Sr.No	Performance parameters	8 Bit	16 Bit	32 Bit
1	Total random states	255	65535	42,49,67, 295
2	Shift registers	8	16	32
3	Number of Flip flops	8	16	32
4	gclk	1	1	1
5	Power consumed	40 mW	45 mW	52 mW