International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 2 Issue: 11 3337 - 3339

Design of 8 and 16 Bit LFSR with Maximum Length Feedback Polynomial & Its pipelined Structure Using Verilog HDL

Dr.R.V.Kshirsagar
Electronics Department
Priyadarshini College of Engineering
Nagpur, India
ravi_kshirsagar@yahoo.com

Purushottam Y. Chawke
Electronics Department
Priyadarshini College of Engineering
Nagpur, India
purushpll@gmail.com

***Abstract*—** This paper is mainly concerned with the design of random sequences using Linear Feedback Shift Register (LFSR). This pseudo sequences is mainly used for various communication purposes. The other application such as banking, cryptographic, encoder & decoder. For hardware prototype FPGA is used because of its flexibility to reconfigure design many times. LFSR is a shift register whose output random state depends upon feedback polynomial. But by using pipelined architecture we can reduce the timing of random pattern generated at output by reducing the critical path. It can count maximum 2^n-1 states and produce pseudo-random number at the output. Finally, comparing the simple and pipelined architecture of 8 & 16-bit LFSR.

Keywords- *LFSR, FPGA, Verilog HDL, pseudo-random number, TRNG, PRNG.*

*****

I. INTRODUCTION

For various cryptographic applications, random numbers are necessary. The generated sequence is uniformly distributed or non-uniformly distributed. Random numbers are needed for a wide range of application in Science and Engineering which require statistical random input.

The random number generator that produces a sequence of number i.e. appears random. The two types of generator have used 1] True random number generator [TRNG]; 2] Pseudorandom number generator [PRNG]. TRNG generator used for generating random data, but have existed. PRNG which uses a computational method based on certain algorithms produces random sequences that repeats are known as PRNG. This PRNG is achieved by LFSR whose input is a linear function of the previous state and the linear congruence algorithm. Using a linear congruence algorithm require time consuming operation and its hardware implementation is very complicated. But using LFSR which is made up of shift register permits very fast generation of random sequences. With maximum length feedback polynomial, here 8 and 16 bit LFSR can produce sequences based on PRNG. As we change the feedback polynomial the output random sequence also changing. But by using simple architecture & as we go on increasing the feedback polynomial the time required to generate the random sequences is large. Hence, here a pipelined architecture is used to increase the critical path & reduce the time at output. The simulation and synthesis on Xilinx ISE 13.2. The HDL language used is Verilog. We prefer Verilog HDL because of its flexibility of writing commands. FPGA is a predefined reconfigurable IC. It can be reconfigured any number of times. Therefore, FPGA kit is used for rapid prototype development as compared to ASIC hence; FPGA kit can be used to implement the design.

II. METHODOLOGY

A. Linear Feedback Shift Register

As we have already defined an LFSR is a shift register whose input bit is a linear function of the previous bit. Therefore linear operation of single bit is exclusive-or (X-OR) operation is used. The initial value in the LFSR is called seed. Thus by changing the value of seed, the sequence at the output is also change. As register having a finite number of states, it may enter a repeating cycle. Thus LFSR having properly chosen feedback function can produce sequence of random patterns at the output of a repeating cycle. For faster response at output here pipelined structure is used. Pipelined structure increases the critical path & reduces the time required at output.

III. LFSR PRNG

Figure 1 shows the basic block diagram of LFSR based on shift register. The feedback from different shift register which influence the input is called taps. This feedback arrangement can be expressed in finite field arithmetic as a polynomial mod 2. The period of sequence is 2^n-1, where n is number of shift register.

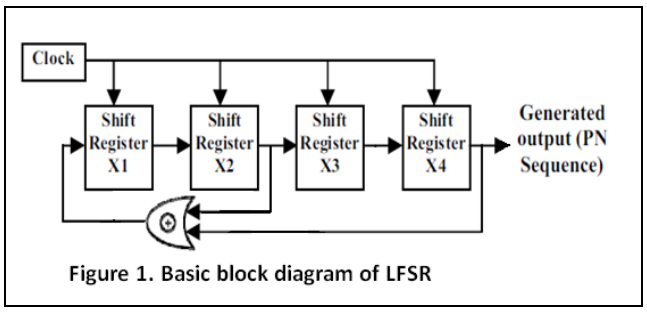

Figure 1. Basic block diagram of LFSR

IV. RULES FOR SELECTING FEEDBACK POLYNOMIAL

- The 'one' in the polynomial correspond to input to the first bit.
- The powers of polynomial term represent tapped bits, counting from left. The first and last bits are always connected as an input and output tap respectively.
- The maximum length can only be possible if the number of taps is even and there must be no common divisor to all taps.

 ISSN: 2321-8169
3337 - 3339

V. 8 BIT LFSR ITS DESIGN & SIMULATION

8-bit LFSR with maximum length feedback polynomial $X^8+X^6+X^5+X^4+1$, that generates $2^8-1=255$ random outputs. Figure 2 shows circuit of 8-bit LFSR with maximum length feedback polynomial & its pipelined structure of fig.3 along with timing simulation is shown in fig.4.

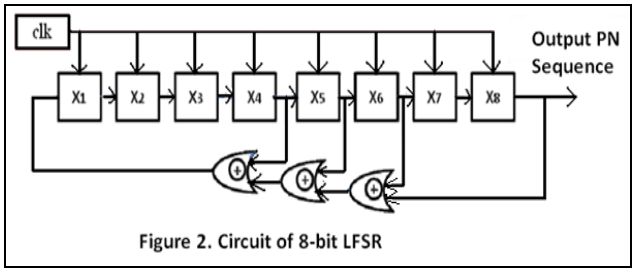

Figure 2. Circuit of 8-bit LFSR

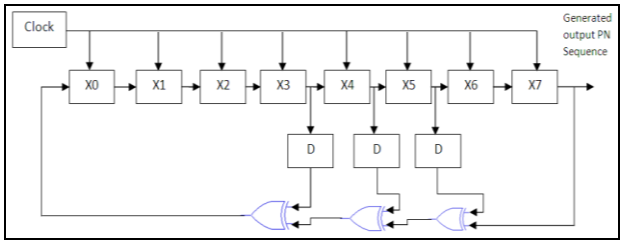

Figure 3. 8-bit Pipelined Structure

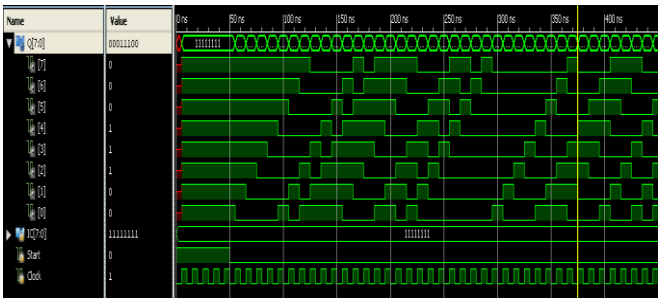

Fig: 4 Timing simulation for 8-bit LFSR

VI. 16 BIT LFSR ITS DESIGN & SIMULATION

16-bit LFSR with maximum length feedback polynomial $X^{16}+X^{15}+X^{13}+X^4+1$, that generates $2^{16}-1=65535$ random outputs. Figure 5 shows circuit of 16-bit LFSR with maximum length feedback polynomial & its pipelined structure of fig.6 along with timing simulation is shown in fig.7.

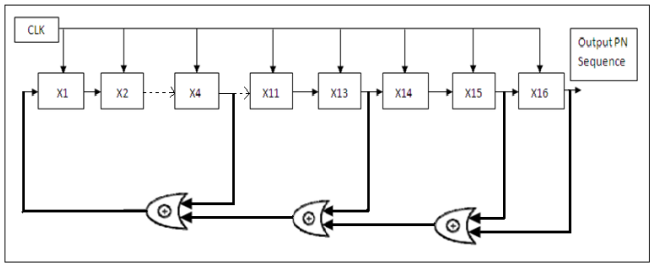

Figure 5. 16-bit LFSR

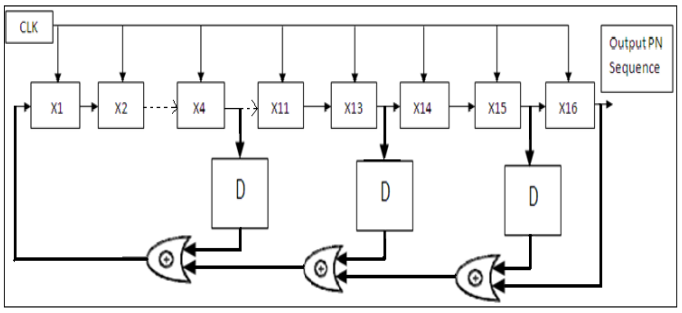

Figure 6. 16-bit Pipelined Structure

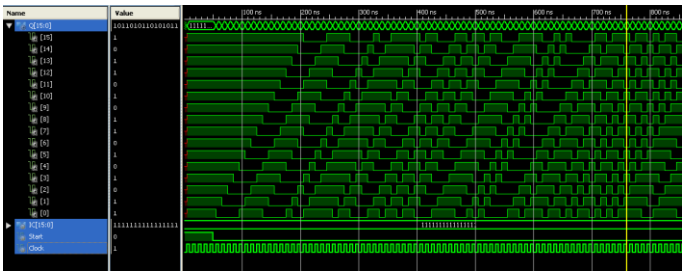

Fig: 7 Timing simulation for 16-bit LFSR

VII. SYNTHESIS AND TIMING SIMULATION

Sr. No.	Performance	8-bit LFSR	8-bit LFSR Pipelined	16-bit LFSR	16-bit LFSR Pipelined
1	total random states	255	255	65535	65535
2	shift register	08	08	16	16
3	x-or gate	03	03	03	03
4	number of slices	04	05	10	19
5	no. of slice flip-flop	08	08	16	32
6	number of 4 input LUT	08	09	16	33
7	gclk	01	01	01	01
8	Clock	1.589	1.357	1.556	1.486

VIII. CONCLUSIONS

As the 8 & 16-bit LFSR produces a random pattern at output, but by using pipelining i.e inserting a latches in the feed forward cutset, reduces the critical path & hence increases the sampling rate.

REFERENCES

[1] Sewak K, Rajput P, Panda Amit K, "FPGA Implementation of 16 bit BBS and LFSR PN Sequence Generator: A Comparative Study", In Proce. of the IEEE Student Conference on Electrical, Electronics and Computer Sciences 2012, 1-2 Mar 2012, NIT Bhopal, India.

[2] Panda Amit K, Rajput P, Shukla B, "Design of Multi Bit LFSR PNRG and Performance comparison on FPGA using VHDL", International Journal of Advances in Engineering & Technology (IJAET), Mar 2012, Vol. 3, Issue 1, pp. 566-571.

[3] Amit Kumar Panda, Praveena Rajput, Bhawna Shukla"FPGA Implementation of of 8,16 And 32 Bit LFSR with Maximum Length Feedback Polynomial using "VHDL" 2012 International

Conference on Communication Systems and Network Technologies.

[4] Katti, R.S. Srinivasan, S.K., "Efficient hardware implementation of a new pseudo-random bit sequence generator" IEEE International Symposium on Circuits and Systems, 2009. ISCAS 2009.

[5] Ding Jun, Li Na, Guo Yixiong, "A high-performance pseudo-random number generator based on FPGA" 2009 International Conference on Wireless Networks and Information Systems.

[6] Lember, A.W.L.Eastman:"High Speed generation of Maximal Length Sequences" IEEE trans. Computers, Short notes, VOL c-20, PP227-229,1981.

[7] Hurd,W.J:"Efficient generation of statistically Good Pseudonoise by Linearly Interconnected Shift Registers", IEEE trans. Computer, VOL C-20.PP 146-152 Feb 1989.

[8] Claudio Mucci, Luca Vanzolini, Ilario Mirimin, Daniele Gazzola, Antonio Deledda, Sebastian Goller_, Joachim Knaeblein_, Axel Schneider_, Luca Ciccarelli_, Fabio Campi, "Implementation of Parallel LFSR-based Applications on an A daptive DSP featuring a Pipelined Configurable Gate Array" 978-3-9810801-3-1/DATE08 © 2008 EDAA.

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