DESIGN OF 8 AND16 BIT LFSR WITH MAXIMUM LENGTH FEEDBACK POLYNOMIAL USING VERILOG HDL

[1]PURUSHOTTAM Y. CHAWKE, [2]R.V.KSHIRSAGAR

[1]M-Tech [VLSI], PCE, Nagpur, [2]Prof., PCE, Nagpur

Abstract- This article is mainly designed for generating pseudo-random sequence using the Linear Feedback Shift Register (LFSR). This pseudo-sequence is mainly used for communication purposes such as cryptographic, encoder and decoder application in coded format to ensure network security. For hardware implementation FPGA can be used, as its faster logic development, its flexibility as we reconfigure design many times. The implemented design can be tested and verify for desired result of different length sequence. Here in this work 8 and 16 bit LFSR is designed by using Verilog HDL language to study their performance and randomness. LFSR is a shift register whose random state at the output depends on the feedback polynomial. So it can count maximum 2n-1 states and produce pseudo-random number of the output. By using FPGA, comparing 8 and 16 bit LFSR on the basis of memory, gates.

Index Terms- 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 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 and its implementation on FPGA. As we change the feedback polynomial the output random sequence also changing.

The 8 and 16-bit length sequence using Verilog HDL implemented on FPGA kit. Also the comparison between two 8 and 16-bit on the basis of synthesis and simulation result. The simulation and synthesis on Xilinx ISE 13.2 the HDL languages are: VHDL and Verilog. We prefer Verilog HDL because of its flexibility of writing commands. FPGA can implement any logical expression i.e. it 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. This feedback function is called a maximum length feedback polynomial.

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.

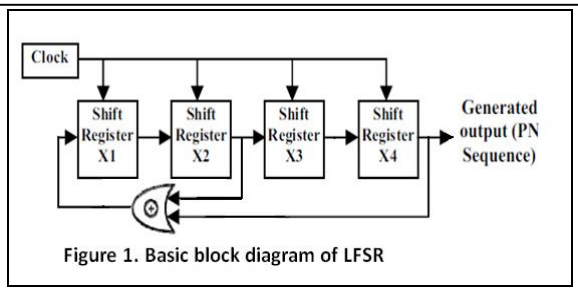

Figure 1. Basic block diagram of LFSR

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.

V. 8-BIT LFSR ITS DESIGN AND 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 timing simulation is shown in fig.4.

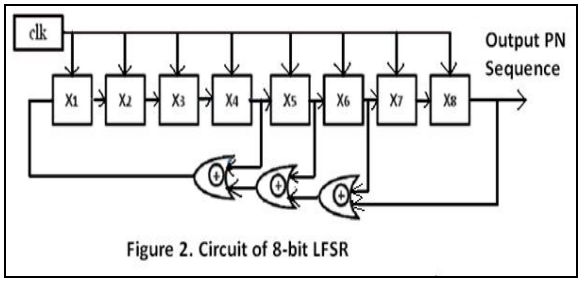

Figure 2. Circuit of 8-bit LFSR

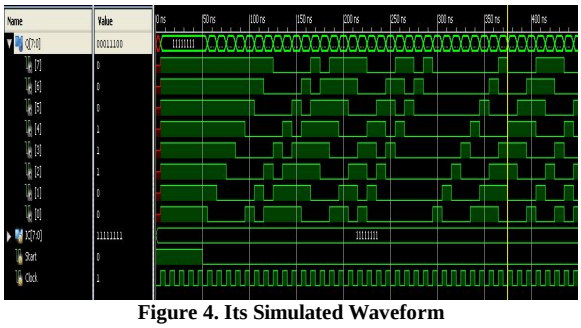
Figure 4. Its Simulated Waveform

VI. 16-BIT LFSR ITS DESIGN AND 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 3 shows circuit of 16-bit LFSR with maximum length feedback polynomial. Its timing simulation is shown in fig.5

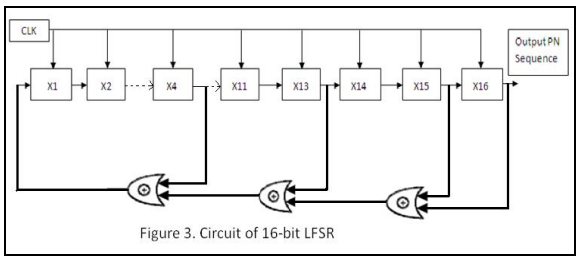

Figure 3. Circuit of 16-bit LFSR

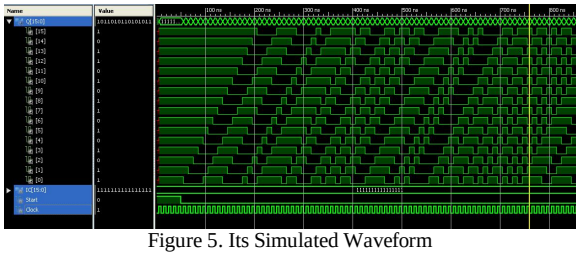
Figure 5. Its Simulated Waveform

VII. TIMING SIMULATION

Sr. No.	Performance	8-bit LFSR	16-bit LFSR
1	total random states	255	65535
2	shift register	08	16
3	x-or gate	01	01
4	number of slices	04	10
5	no. of slice flip-flop	08	16
6	number of 4 input LUT	08	16
7	gclk	01	01

CONCLUSION

Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions. Authors are strongly encouraged not to call out multiple figures or tables in the conclusion—these should be referenced in the body of the paper.

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

★★★