International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 5 479 - 480

Design of Pseudo Random Binary Sequence Generator using VHDL

[1]Ashwini .M. Kaurase, [2]Rashmi .S. Deshmukh, [3]Tejashree .S.Lohar
[1, 2, 3]Dept of E&TC, Government College of Engg., Jalgaon ,Maharashtra
[1]*ashwinikaurase11@gmail.com*, [2]*rsdeshmukh09@gmail.com*, [3] *tejashreelohar20@gmail.com*

***Abstract*—** Pseudo Random binary Sequence Generator technique are used for various cryptographic applications and for designing encoder, decoder in different communication channel . The implementation of PRBS generator is based on the linear feedback shift register (LFSR).The total number of random state generated by the LFSR depends on the feedback polynomial. It is nothing but a simple counter so it can count maximum of 2^{n-1} cycle by using maximum feedback polynomial. In this paper, the entire design of the PRBS generator is implemented using VHDL.

Keywords*-PRBS, LFSR.*

*****

I. INTRODUCTION:

Today cryptography is an integral part of our lives. The list of public applications is long, and many spring from the use of internet. This global communication system has provided us not only with new buzz words such as “24/7 shopping”, “one-click-buy” and “JIT-services” but also with a new and convenient ways of performing tasks .In addition, confidentiality of communication, many new tasks like data integrity, message authentication, or non-repudiation have been added. Pseudorandom number generators (PRNGs) are used in modern cryptography to transform a small initial value into a long sequence of seemingly random bits[2][There are various methods for generating pseudorandom numbers are known. Most of them are based, on linear congruential equations, which require a number of time consuming arithmetic operations, the hardware implementation is very complicated and the safety performance is poor to be used in cryptography[6][7]. Most of them are based on Blum Blum Shub (BBS) method for generating PN sequence as it is non periodic cryptographically secure method .But performance is poor as the time required is more and memory utilization is more in BBS as no. of flip-flops required are more. In contrast, many designs for PRNGs are based on linear feedback shift registers (LFSRs), which can be constructed in such a way as to have optimal statistical and periodical properties and permits very fast generation of binary PN sequences.

Pseudo random binary sequence is nothing but a random sequence of binary numbers. It is ‘random’ because the value of an element of the sequence is independent of the values of element of any other sequence. It is 'pseudo' in sence as it is deterministic and after N elements it starts to repeat itself, unlike real random sequences. The PRBS generator produces a predefined sequence of 1's and 0's, with 1 and 0 having the same probability. A sequence of consecutive n*(2^n -1) bits comprise one data pattern, and this pattern will repeat itself over time.

II. LINEAR FEEDBACK SHIFT REGISTERS (LFSR)

LFSR is a shift register whose input bit is a linear function of its previous state. The XOR is most commonly used single bit for linear function . Thus, an LFSR is 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 seed. Because the register has a finite number of possible states,as the state is complete it start repeating.. However,an LFSR with a well-chosen feedback function can produce a sequence of bits which appears random and which has avery long cycle. Applications of LFSRs are generating pseudo-random numbers, pseudo-noise sequences, fast digital counters, and whitening sequences. Both hardware and software implementations of LFSRs are same.

A) SELECTION OF TAP POINT

Polynomials over Binary Fields

The most commonly used fields are extensions of the binary field GF(2), and they are calledGalois fields GF(2*m*). Binary arithmetic uses addition and multiplication modulo 2. A polynomial$f(X)$ defined over GF(2) is of the form$f(X) = f_0 + f_1X + f_2X_2 + \ldots + fnXn$(9)where the coefficients *fi* are either 0 or 1. The highest exponent of the variable X is called the degree of the polynomial. There are 2*n* polynomials of degree *n*.

B) IMPLEMENTATION OF LFSR

Pseudo random number sequence generator is generatedin VHDL according to the following circuit based on the concept of shift register..

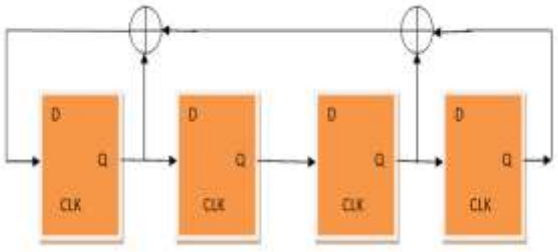

Fig .Basic block diagram of LFSR

Rules for selecting feedback polynomial

The contents of the register, the bits tapped for the feedback function, and the output of the feedback function together describe the state of the LFSR. With each shift, the LFSR moves to a new state.

Any tap sequence will yield at least two state spaces for an LFSR.Tap sequences that yield only two state spaces are referred to as maximal length tap sequences The powers ofthe terms represent the tapped bits, counting from the left.The first and last bits are always connected as an input andoutput tap respectively. LFSR will only be maximum-lengthif the number of taps is even. There must be no commondivisor to all taps.

The state of an LFSR that is n bits long can be any one of 2^n different values. Thelargest state space possible for such an LFSR will be 2^{n-1} . Because each state can have only once succeeding state, an LFSR with amaximal length tap sequence will pass through every non-zero state once and only oncebefore repeating a state.

C) DESIGN & SIMULATION OF 4 BIT LFSR

4-bit LFSR with maximum length feedback polynomial $x^4 + x^1 + 1$ generates 2^4 -1 random outputs,which is verified from the simulation waveform.

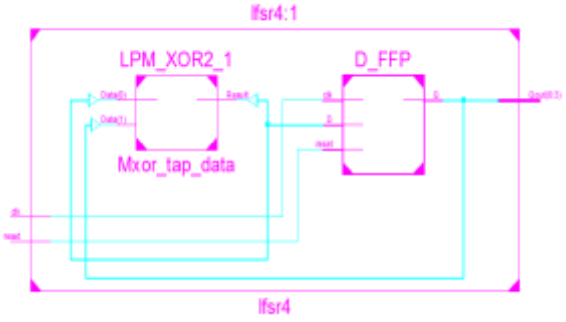

Fig. RTL Schematicc of 4 bit LFSR

D) DESIGN & SIMULATION OF 8 BIT LFSR

8-bit LFSR with maximum length feedback polynomial generates 2^8 -1 random outputs,which is verified from the simulation waveform.

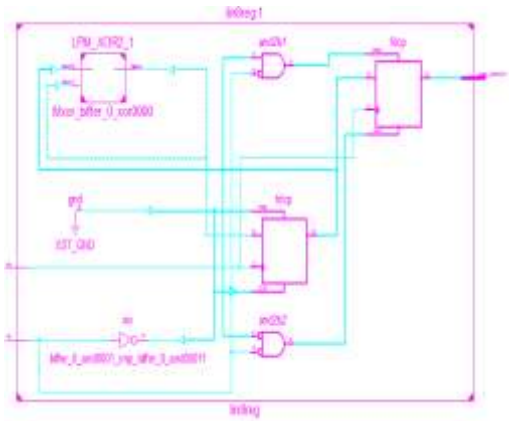

Fig. RTL Schematic of 8 bit LFSR

SIMULATION & SYNTHESIS RESULT

Performance	4 bit	8 bit
Timeto complete total state	105 ns to 225ns	1ns to 538ns
Total no. Random state generating	15	255
Shift register	4	8
Xor gate	01	01
No. Of Slice Flip Flop	8	16
No. Of slices	5	10
No. Of 4 input LUT's	10	18
GClk	01	01
Gate + Net delay	7.165ns	2.730ns
No. Of bonded IOBS	6	10
No. of IOs	6	10

CONCLUSION:

It is clearly found from the synthesis and simulation result that 4 bit & 8 bit LFSR with maximum feedback polynomial can generate maximum random output.
In the practical use 8-bit and 16-bit LFSR is sufficient for different cryptographic applications.

REFERENCES

[1] P.Alfke, "Efficient Shift Registers, LFSR , Counters and Long Pseudo Random Sequence Generators," XAPP 052, July 7, 1996
[2] M. Goresky and A. M. Klapper, "Arithmetic cross correlation of feed back with carry shiftregister sequences," *IEEE Trans.Inform. Theory*, vol. 43(pp. 1342–1346) July 1997
[3] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung.Network informationflow. :*IEEE Transactions on Information Theory, 46(4):1204–1216, Jul 2000.*
[4] PatrikEdhal, *On LFSR-based Stream Ciphers (PhD), 2003*
[5] Ding Jun, Li Na, GuoYixiong, "A high-performance pseudo-random number generator based on FPGA" *2009 International Conference on Wireless Networks and Information Systems*
[6] 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*