International Journal of Innovation in Science and Mathematics
Volume 4, Issue 1, ISSN (Online): 2347–9051

Bit Error Rate Testing using Pseudo-Random Bit Sequences Generator

Uttam Kumar Mishra
Student, Department of ECE
LNCT Bhopal, M.P India
Email: uttamkumishra.008@gmail.com

Tarun Verma
Professor, Department of ECE
LNCT Bhopal, M.P India
Email: asst.prof.tarun@gmail.com

Dr. Rita Jain
Head of Department of ECE
LNCT Bhopal, M.P India
Email: ritajain_bpl@yahoo.com

***Abstract* – One of the basic measures of the performance of any digital communication system is Bit error rate (BER) test. For the digital data source, it is common to use a pseudorandom number generator (PRNG). Linear feedback shift registers (LFSRs) are undoubtedly the best known register-based PRNGs. The purpose of this research is to develop a digital true random number generator using linear feedback shift register (LFSR) that can be synthesized using standard digital design tools. Random number generators will be required to protect the medical, financial and personal data of entities connected to these networks. Because of their compactness, fast bit-level operations, and the exponential increase of their period with the width of the shift register, LFSRs have enjoyed success in many hardware-based simulations and digital circuit testing.**

***Keywords* – BER, LFSRs, PRNG, SRAM, BERT, Throughput.**

I. INTRODUCTION

Bit error rate (BER) is the ratio of the number of incorrect to the total number of received bits. For qualifying the reliability of an entire digital communication system from "bits in" to "bits out", BER characteristic is the fundamental measure of the performance of a digital communication system. In digital communication system transmitter transfer the binary sequence formats through channel to the receiver. The receiver receives this signal and recovers the signal in transmitted form. The channel is the medium through wires, or through air. It is the possibility that this transmitted signal may get currupt due to noise. this noise may be man made or it may be generates through electronics devices. The bit error rate that is a bit-error at the output of the receiver, compared with the input of the transmitter, is the measure of system performance use in digital communication.

II. TEST PATTERN/ PRBS GENERATOR:

The deterministic signal random sequence pattern generated by PRBS generator shows the similar property to white noise signals. This is the major advantage of of PRBS pattern in bit error rate testing. The both transmitter and receiver uses their own simillar locally gennerated random sequence. The receiver uses first part of the sequence as the starting bytes for initialization. This first part of the received sequence received correctly, both PRBS generators now are in synchronous and the receiver correlate the transmitter's sequence to its locally generated stream for finding bit errors caused by the communications equipment or the link.

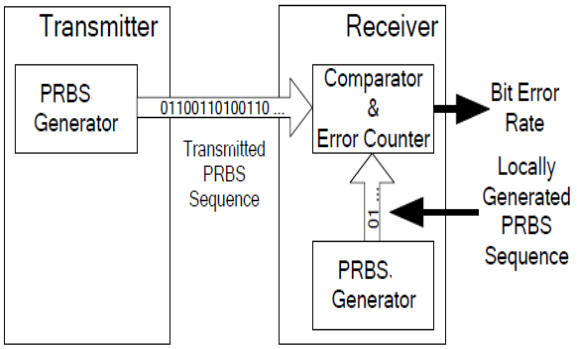

Fig 1 PRBS-based Bit Error Rate Tester (BERT)

For the digital information source, it is common to use a pseudorandom number generator (PRNG). Linear feedback shift registers (LFSRs) are undoubtedly the best known register-based PRNGs. Because of their compactness, fast bit-level operations, and the exponential increase of their period with the width of the shift register, LFSRs have enjoyed success in many hardware-based simulations and digital circuit testing. Linear feedback shift registers make extremely good pseudorandom pattern generators. When the outputs of the flip-flops are loaded with a seed value (anything except all 0s, which would cause the LFSR to produce all 0 patterns) and when the LFSR is clocked, it will generate a pseudorandom pattern of 1s and 0s. Note that the only signal necessary to generate the test patterns is the clock. However, LFSRs produce only a single bit at each clock cycle, which is rather slow for very longrunning simulations. On the other hand, the sequences using LFSRs with parallel outputs have undesirable correlations [1]. The output is a linear function of the previous input. Due to the fact that an LFSR has a finite number of states determined by its length, it implements a repeating cycle of deterministic states, unless a state contains all zeros. In the latter case, the LFSR does not change the state. This likely also is the reason for IEEE 802.3 stating to seed the PRBS pattern generator with an initialization vector different from zero. When built upon the maximum-length polynomial for the shift register of length n, an LFSR cycles through a maximum length sequence (MLS), i. e. produces all possible 2n-1 states. The bit positions influencing the next state are called taps.

International Journal of Innovation in Science and Mathematics
Volume 4, Issue 1, ISSN (Online): 2347–9051

III. WORKING OF LFSR

The basic components of LFSR is series combination of delay flipflops and xor logic gates with the serial binary input stream. It operates at very high clock to increase the throughput and speed. The non linear feedback through xor gateallows shift registers to produce repeat binary sequences , a well-known class of which is the class of Pseudo-Random Binary Sequences. The generator polynomial provides the necessary feedback taps for the LFSR circuit, the feedback causes the value in the shift register to cycle through a set of unique values.

Linear Feedback Shift Registers sequence through (2^n-1) states, where n is the number of registers in the LFSR. At each clock edge, the contents of the registers are shifted right by one position. There is feedback from predefined registers or taps to the left most register through an exclusive-NOR (XNOR) or an exclusive-OR (XOR) gate. A value of all "1"s is illegal in the case of a XNOR feedback. A count of all "0"s is illegal for an XOR feedback. This state is illegal because the counter would remain locked-up in this state. The LFSR shown below is implemented with XNOR feedback. A 4-bit LFSR sequences through (24 - 1) = 15 states (the state 1111 is in the lock-up/illegal state). From (Table 1) the feedback taps are 4, 3. On the other hand, a 4-bit binary up-counter would sequence through 24 = 16 states with no illegal states. LFSR counters are very fast since they use no carry signals. However, the dedicated carry in Virtex devices is rarely a speed limiting factor because it is intrinsically fast. LFSRs can replace conventional binary counters in performance critical applications where the count sequence is not important (e.g., FIFO). LFSRs are also used as pseudo-random bit stream generators. They are important building blocks in the implementation of encryption and decryption algorithms.The list of the bits positions that affect the next state is called the tap sequence. In the diagram below, the sequence is (16,14,13,11)

• The outputs that influence the input are called taps.

• A maximal LFSR produces an n-sequence(i.e. cycles through all possible states within the shift register), unless it contains all zeros, in which case it will never change.The sequence of numbers generated by a LFSR can be considered a binary numeral system just as valid as Gray code or the natural binary code. The tap sequence of an LFSR can be represented as a polynomial mod 2. This means that the coefficients of the polynomial must be 1's or 0's. This is called the feedback polynomial or characteristic polynomial. For example, if the taps are at the 16th, 14th, 13th and 11th bits (as below), the resulting LFSR polynomial is

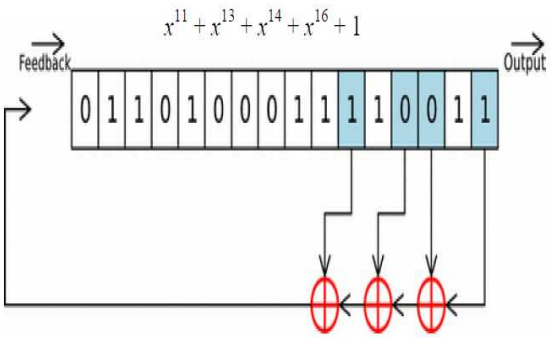

Fig.2. LFSR With 16,14,13,11 Bits As Tap.

A Linear Feedback Shift Register is a sequential shift register with combinational logic that causes it to pseudo-randomly cycle through a sequence of binary values. Linear feedback shift registers have multiple uses in wireless communication systems using LFSR as a functional block .Applications covered in this thesis include:

1. PN number generation by implementing PN generators with the help of LFSR.
2. RS code generators used for random number generation using LFSR.
3. Implementation of BIST with the help of LFSR for testing purposes.

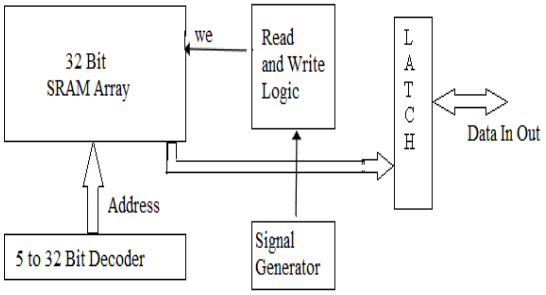

Fig.3. SRAM base system use for RNG sequence Pattern.

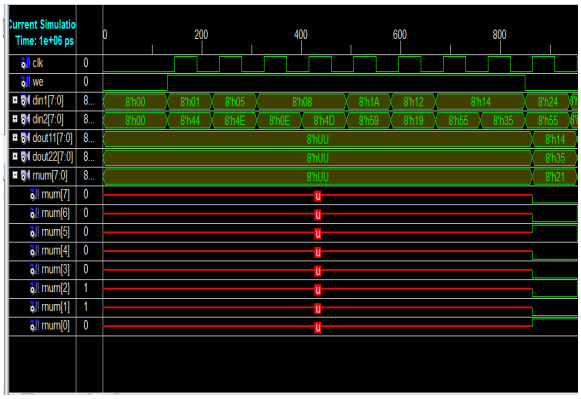

Fig.4. Timing simulation of propose SRAM base RNG writing operation.

The synthesis report of RAM base RNG shows the total 1040 flip flopf, 2 eight bit 64X1 multiplexers and 132 gate count require for design.

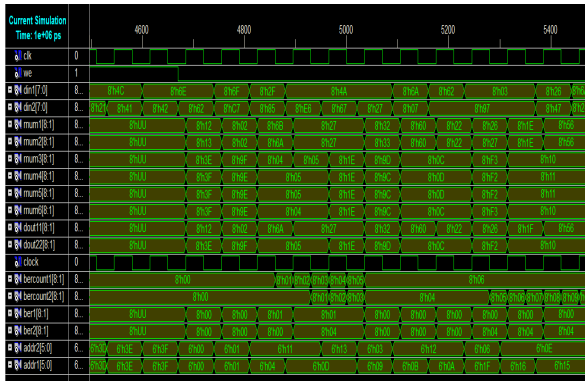

Fig.5. The PRBS sequence pattern with bit error count in timing scale of 4500ns to 5400ns with the computational time of 70ns.

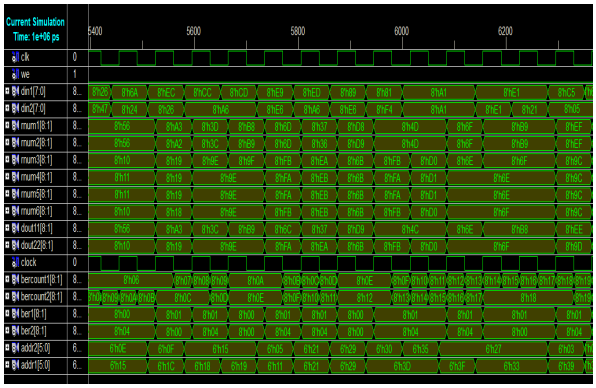

Fig.6. The PRBS sequence pattern with bit error count in timing scale of 5400ns to 6300ns with the computational time of 70ns.

Fig.5 and fig 6 shows the timing simulation for 8 bit random number bit error rate test. Sequence data is write in dual port RAM depends on address. The six byte random number is generates at one clock cycle depends on address signal. The linear feedback signal is concatenate with the initialize sequence at its least significant bit. The clock signal frequency is at 33.33MHz will generates a 6 bytes random number in 30ns time this will create the throughput of 1.66 Gb/sec.

When the shift register rnum1 and rnum2 is fully loaded with the transmitted PRBS, the output of ber1 and ber2 shows the bit error for the rnum1 and rnum2 sequence. In this case, the noise may currupt the rnum1 sequence is XORed with rnum pseudo random pattern and the biet error is counted on bercount register. If the test patterns from 1 LFSR are correctly transmitted by the DUT, then the two inputs of XOR should be the same value in each clock cycle.

Table 1: Parametric Analysis

Module	This Work	[1]	[2]
Freq (MHz)	33.33	52	5
Computational Time (ns)	30	20	-
Throughput Gb/s	1.66	0.4	0.01
RAMs	2	4	2
FFs	84	248	32

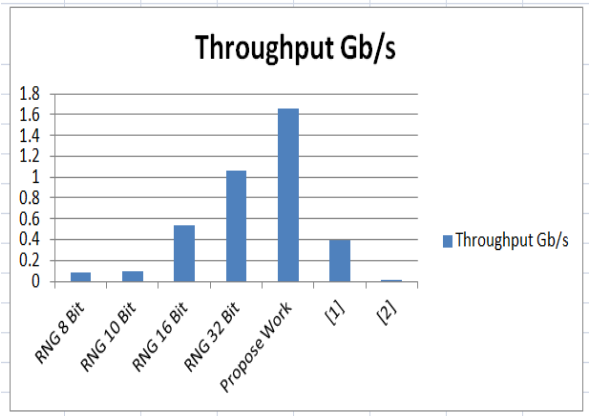

Fig.7. Graphical Analysis of throughput compuatation.

Table 1 shows the comparison of a number of FPGA-based PRNGs, in terms of quality metric, resource usage, and performance. , although consuming more logic resource (this is because of the algorithm complexity), the our random number generator achieves a bit higher throughput. In addition, it is worth to note that the resource usage is less. The computational time of RHG is 30ns with throughput of 1.66Gb/s.

IV. Conclusion

The synthesis report of 16 bit PRBS Generator shows the total gate count of 176 which includes 1 byte register comprising of 17 flipflop and 4 logic gates. Fig 5.6 shows The 16 bit register with a linear feedback through XOR logic gate. Here 16 bit random number is being generated with the help of XOR gate. The most significant digit and least significant digit both are passed through XOR gate and give the 1st bit of the random number and then this equation runs inside in the loop of 16 times to give and 16 bit random number.

The design is implemented using the (VHDL) Very High speed Integrated Circuit hardware description language. The implementation supports a range of parameters to facilitate the experimental evaluation of design choices. A functional, parameterizable implementation is then produced, based on the design specification. When the shift register rnum1 and rnum2 is fully loaded with the transmitted PRBS, the output of ber1 and ber2 shows the bit error for the rnum1 and rnum2 sequence. In this case, the noise may currupt the rnum1 sequence is XORed with rnum pseudo random pattern and

the biet error is counted on bercount register. If the test patterns from 1 LFSR are correctly transmitted by the DUT, then the two inputs of XOR should be the same value in each clock cycle.

REFERENCES

[1] Amirhossein Alimohammad and Saeed Fouladi Fard "FPGA-Based Bit Error Rate Performance Measurement of Wireless Systems" IEEE Transactions On Very Large Scale Integration (Vlsi) Systems pp 1063-8210 year 2013.

[2] Walter Aloisi and Rosario Mita "Gated-Clock Design of Linear-Feedback Shift Registers" IEEE Transactions On Circuits And Systems—Ii: Express Briefs, Vol. 55, No. 6, pp no 546 June 2008 .

[3] David B. Thomas, and Wayne Luk "The LUT-SR Family of Uniform Random Number Generators for FPGA Architectures " IEEE Transactions On Very Large Scale Integration (Vlsi) Systems, Vol. 21, No. 4, April 2013.

[4] Piotr Zbigniew Wieczorek, and Krzysztof Gołofit "Dual-Metastability Time-Competitive True Random Number Generator" Ieee Transactions On Circuits And Systems—I: Regular Papers, Vol. 8, no1. ,year 2013.

[5] Sharmitha.E.K, Sharmitha.E.K, Nisha Angeline. M, Palanisamy.C "High Throughput LFSR Design for BCH Encoder using Sample Period Reduction Technique for MLC NAND based Flash Memories " International Journal of Computer Applications (0975 – 8887) Volume 66– No.10, March 2013.

[6] Walter Aloisi and Rosario Mita "Gated-Clock Design of Linear-Feedback Shift Registers" Ieee Transactions on Circuits and Systems—II: Express Briefs, Vol. 55, No. 6, pp no 546 year june 2008.

[7] Doshi N. A., Dhobale S. B., and Kakade S. R. "LFSR Counter Implementation in CMOS VLSI" World Academy of Science, Engineering and Technology 48 year 2008.

[8] Karthik Visweswariah, Sanjeev R. Kulkarni, and Sergio Verd´u "Source Codes as Random Number Generators" IEEE Transactions On Information Theory, Vol. 44, No. 2, March 1998 pp no. 462.