Improvement of LFSR Base Random Number Generator In 50nm Technology

Jaikaran Singh[1], Mukesh Tiwari[2] Shradha Sharma[3]

1.Associate Professor, Dept. of ECE , SSSIST, Sehore

2. Professor, Dept. of ECE , SSSIST, Sehore

3. PG Scholar , Dept. of ECE , SSSIST, Sehore

Abstract: Random number generator are use to generate changeable binary sequence use in the secrecy of electronic communications, medical, financial and delicate data of entities connected to these networks.. There are two types of random number generator as pseudo random number i.e. arbitrary but predefined sequence and true random number i.e. irregular, undefined pattern numbers. In this paper we have designed a 4, 8, 12 and 16 bit linear feedback shift register using 50nm technology for random number generator. This generator yields a predefined order of binary 1 and binary 0. A sequence of repeated n*(2^n -1) bits comprise one data sample, and this sample will repeat itself over time.

Keywords: LFSR, PRBS, Maximum Length, Tapping, Throughput bit Rate.

INTRODUCTION

An all-purpose feedback shift register is defined as an n-bit shift register which pseudo-randomly scrolls amid 2^n-1 values. Once it achieves its final state, it will go over the sequence exactly as before. A linear feedback shift register (LFSR) of length L consists of n number of series linked delay flip-flops, each able to store one bit and having one input and one output; and a clock which directs the movement of data. It consists of feedback through XOR logic gate from two or additional flip-flops output points labelled as taps. LFSR is used for unpredictable random number production. When the taps are selected precisely, the LFSR will pass through all probable states exclusive of all 0s state and will generate a utmost length pseudorandom binary sequence (PRBS) named N-sequence. To get the requisite operation, the initial binary state will hoard in LFSR which is generally called as seed. The length and values of sequence produced by LFSR is determined by its feedback and tap selection.

II. LITERATURE SURVEY

Fabio Pareschi, Gianluca Setti worked on general characteristics of an RNG and highlighted the drawbacks of the classical solutions, showing how they can be rise above by the chaos-based approach. They also re-examined pipeline ADCs, in particular the 1& 1/2 bit per stage architecture which showed to be the best suited for the reuse of building blocks in chaos-based true random generators[3].

Walter Aloisi and Rosario Mita work on a method to lessen the power consumption of the trendy linear feedback shift register. The proposed design is based on the gated clock design approach and it can offer a considerable power reduction, depending on technological characteristics of the utilized gates using SPECTRE simulations in CADENCE environment by using the 0.35-m technology. Simulation results have revealed a power reduction of about 10% with a mean error of about 3% with respect to hypothetical derivations [6].

David B. Thomas, and Wayne Luk work on Field-programmable gate array (FPGA) optimized random number generators (RNGs) are more resource efficient than software-optimized RNGs because they can obtain benefit of bitwise operations and FPGA-specific features [2].

III. LFSR TAPING OPERATION

The output of one or more flip-flop is feedback to the input of initial flip-flop through XOR gate. This flip-flops output is called as tap. Taps are opted based on the primitive polynomial. If all the output bits of flip-flops is at binary '0' then it keep on shifting to all 0s indefinitely, so it is required to initialize the register with sequence of either a logic 0 or a logic 1 called as seed.

When the seed enter in LFSR following operation executes:

i. The feedback through XOR reallocates the data from previous register to next register and forms part of the output sequence;
ii. The data of stage n-1 is moved to stage for all n, 1<=n<=L-1.
iii. The new data through XOR gate is feedback bit sj which is calculated by summing up together modulo 2 the previous contents of a fixed subset of stages 0, 1.....L-1.

iv. Their sequences rapidly diverge as clock pulses are applied.

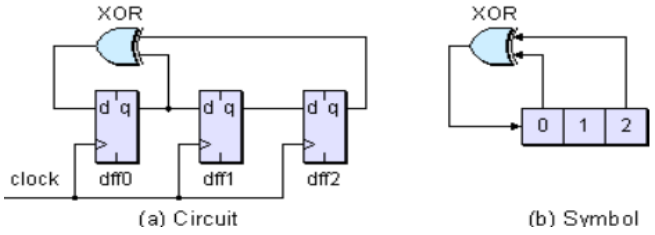

Fig.1 A realization of an LFSR with D flip-flops

A design of an LFSR with D flip-flops is shown in Fig 1. This linear feedback shift register consist of three D flip-flops. All flip-flops are synchronized by the common clock signal. At every clock edge the digits of the flip-flops are shifted by one place to the right. In Figure, the LFSR has 3 stages, which means that the length L-3. The feedback polynomial realized by this LFSR is

$$F(x) = 1+ x+ x^3 .$$

An LFSR can be exclusively determined by its feedback function. Every new digit of the output series is expressed as a function of the n previous digits in n stages. The feedback function is a linear repetition of order n:

$$F(t) = p1a(t-1) \text{ XOR } p2(t-2) \text{ XOR}.....pn(t-n)$$

In order to analyze each register more effortlessly, the linear recurrence of the register is often mapped to a formal polynomial, which is called feedback polynomial of the register. The feedback polynomial consequent to the linear recurrence is shown below:

$$F(x) = 1+ a1x+a2\ x^2 + \ldots\ldots\ldots\ldots + anx^n$$

Frequently, the reciprocal of the feedback polynomial is also used, which is called characteristic polynomial.

The feedback polynomial of a linear feedback shift register can be categorized into three categories: reducible polynomials, irreducible polynomials and primitive polynomials. It is good strategy to use LFSRs with primitive feedback polynomials in cryptography. The linear feedback shift register with a reducible polynomial has the property that the length of the period of the output sequence depends on the initial condition. The linear feedback shift register with irreducible feedback polynomial has the property that the length of the period of the output sequence does not depend on the initial condition, but is a factor of 2^L-1 where L is the length of the LFSR.

IV. METHODOLOGY

The 4, 8, 12, 16 bit linear feedback shift register is designed using delay flip-flop in 50nm technology. The channel length of NMOS and PMOS transistor is 0.05um and channel width is 0.1um. The delay flip-flop has been designed using transmission gate logic implemented in Microwind layout simulator:

1. Increased number of bits in Random Number generator by generating the sequence using a Linear feedback shift register.
2. Create maximum shift register length.
3. Long-period generators to be implemented using only a small amount of logic.

V. TIMING SIMULATION

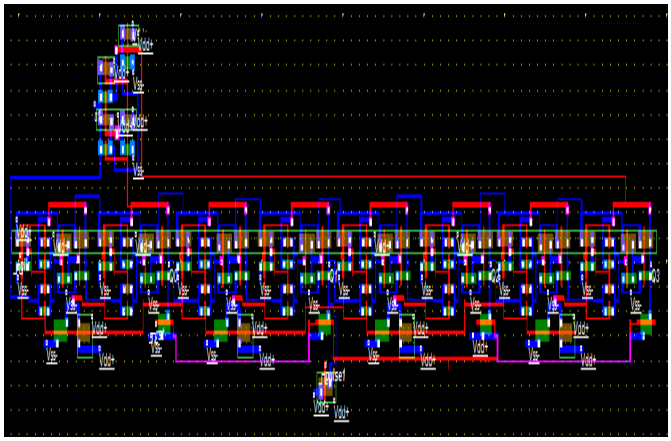

Fig.2 CMOS Layout Design of 4 bit Linear Feedback Shift Register with the polynomial of $f(x) = 1+ x+ x^{4.}$

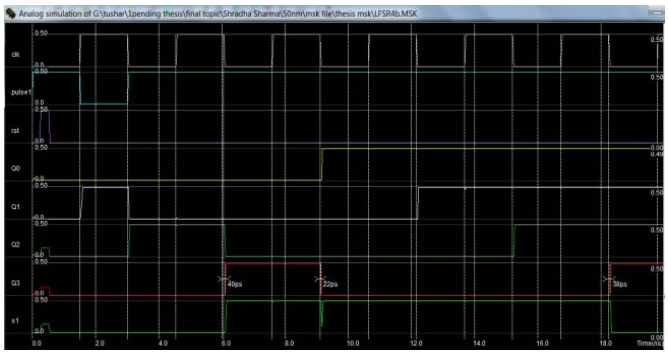

Fig.3 Timing simulation of 4 bit Linear Feedback Shift Register with the polynomial of $f(x) = 1+ x+ x^{4.}$

In 20ns scale total 5 random number of 4 bit each. This gives 20 bits in 20ns scale. That gives $50X10^6$ random scales of 20ns in 1 second. The total bit rate is 1000Mb/sec. The random sequence of 4 bit Linear Feedback Shift Register with the polynomial of $f(x) = 1+ x+ x^{4.}$ is 0010-0100-1000-0001-0011-0111-1111-1110-1101-1010-0101-1011-0110-…….

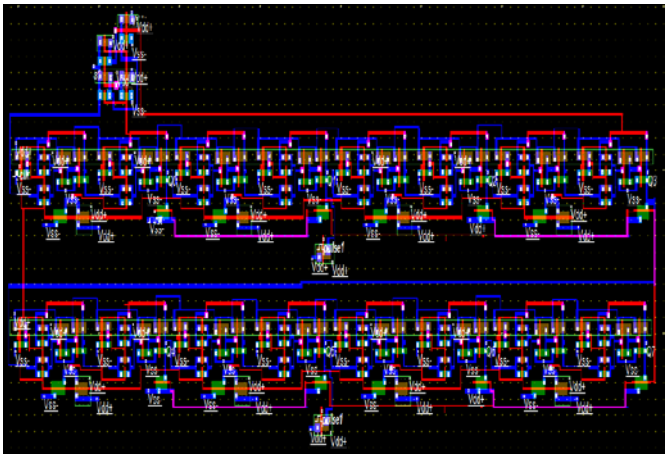

Fig.4 CMOS Layout Design of 8 bit Linear Feedback Shift Register with the polynomial of f(x) = 1+ x+ x^4 . Possibly Extended to f(x) = 1+ x+ x^4 + x^5 + x^8

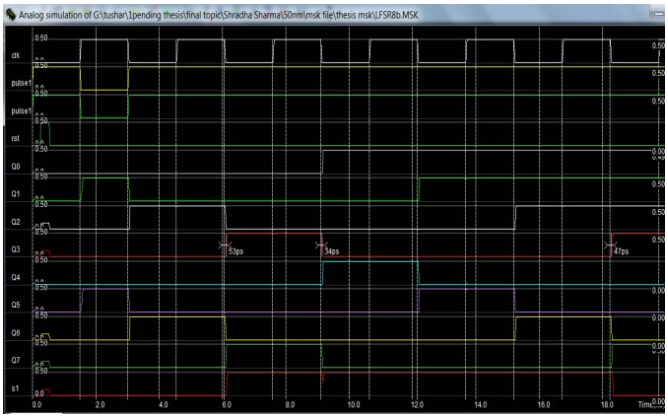

Fig.5 Timing simulation of 8 bit Linear Feedback Shift Register with the polynomial f(x) = 1+ x+ x^4 .

In 20ns scale total 5 random number of 8 bit each. This gives 40 bits in 20ns scale. That gives 50X10^6 random scales of 20ns in 1 second the total bit rate is 2000Mb/sec.

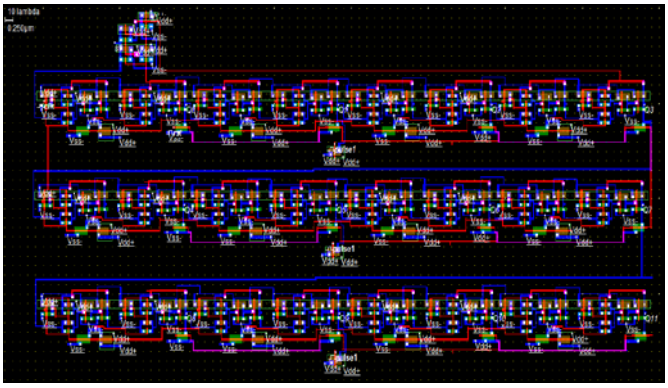

Fig.6 CMOS Layout Design of 12 bit Linear Feedback Shift Register with the polynomial of f(x) = 1+ x+ x^4 . Possibly Extended to f(x) = 1+ x+ x^4 + x^5 + x^8 + x^9 + x^{12}.

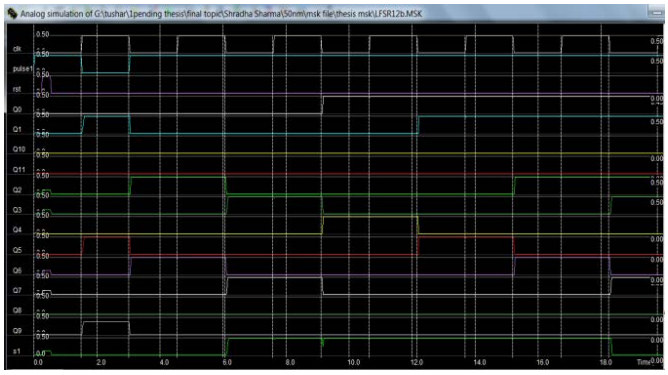

Fig.7 Timing Simulation of 12 bit Linear Feedback Shift Register with the polynomial of f(x) = 1+ x+ x^4 .

In 20ns scale total 5 random number of 12 bit each. This gives 60 bits in 20ns scale. That gives 50X10^6 random scales of 20ns in 1 second. The total bit rate is 3000Mb/sec.

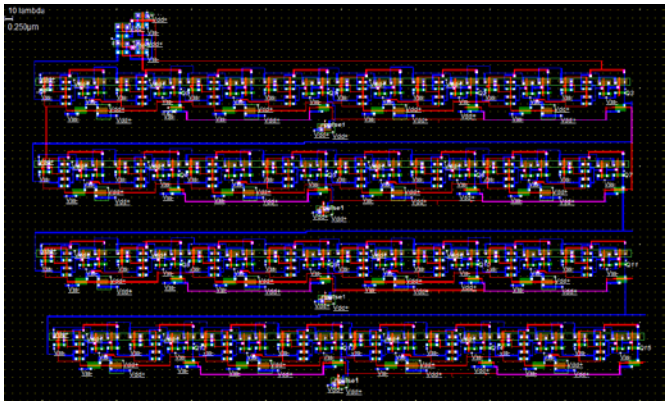

Fig.8 CMOS Layout Design of 16 bit Linear Feedback Shift Register with the polynomial of f(x) = 1+ x+ x^4 . Possibly Extended to f(x) = 1+ x+ x^4 + x^5 + x^8 + x^9 + x^{12} + x^{13} + x^{16}.

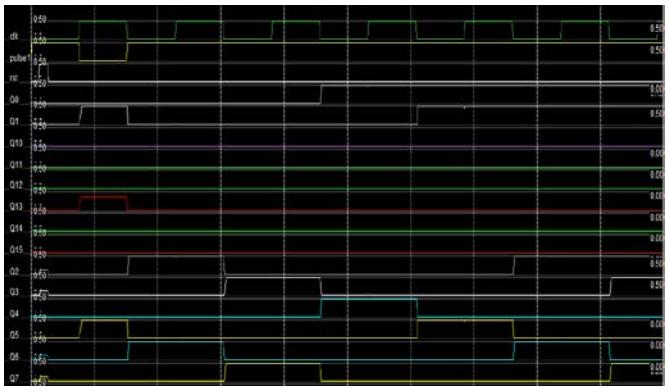

Fig.9 Timing Simulation of 16 bit Linear Feedback Shift Register with the polynomial of f f(x) = 1+ x+ x^4 .

In 20ns scale total 5 random number of 16 bit each. This gives 80 bits in 20ns scale. That gives $50X10^6$ random scales of 20ns in 1 second. The total bit rate is 4000Mb/sec.

Similarly In 20ns scale total 5 random number of 32 bit each. This gives 160 bits in 20ns scale. That gives $50X10^6$ random numbers in 1 second. The total bit rate is 8000Mb/sec.

RNG	Output Bit Rate Mb/s	Power	Technology	Output Bit Rate Mb/s	Power	Technology
	[1]			Our Work		
4 Bit RNG	40	29mW	0.35 um	1000	1.838uW	50nm
8 Bit RNG	80	22mW	0.18 um	2000	3.601uW	50nm
12 Bit RNG	-	-	-	3000	6.547uW	50nm
16 Bit RNG	160	-	0.09 um	4000	9.436uW	50nm
32 Bit RNG	320	-	50nm	8000	-	50nm

VI. CONCLUSION

The random number generated by 4 bit LFSR having the output bit rate i.e. throughput of 1000Mb/s with the power consumption of 1.838uW. The increase in bit length of LFSR will improve the bit rate with same latency of LFSR. For 16 bit random number the throughput is increased to 4000Mb/s with the power consumption of 9.436uW.

REFERENCES

[1] Yuan Li, Paul Chow, Jiang Jiang, Minxuan Zhang, and Shaojun Wei "Software/Hardware Parallel Long-Period Random Number Generation Framework Based on the WELL Method" IEEE Transactions On Very Large Scale Integration (VLSI) Systems year 2013.

[2] 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.

[3] Fabio Pareschi, Gianluca Setti, and Riccardo Rovatti "Implementation and Testing of High-Speed CMOS True Random Number Generators Based on Chaotic Systems" IEEE Transactions On Circuits And Systems—I: Regular Papers, Vol. 57, No. 12, Pp No. 3124 December 2010.

[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] Toni Stojanovski and Ljupˇco Kocarev "Chaos-Based Random Number Generators—Part I: Analysis" IEEE Transactions On Circuits And Systems—I: Fundamental Theory And Applications, Vol. 48, No. 3, March 2001pp no. 281.

[9] Hong-Sik Kim, Yongjoon Kim,and Sungho Kang " Test-Decompression Mechanism Using a Variable-Length Multiple-Polynomial LFSR" IEEE Transactions On Very Large Scale Integration (VLSI) Systems, Vol. 11, No. 4, August 2003 pp no. 687.