REVIEW ON STANDARD AND MULTIBIT LINEAR FEEDBACK SHIFT REGISTER

[1]Rita Mahajan, [2]Komal Devi, [3]Deepak Bagai
[1]Assistant Professor, [2]M.Tech Student, [3]Professor
[1]ECE Department
[1]Punjab Engineering College (Deemed to be university), Chandigarh, India

Abstract- Linear feedback shift registers have many applications. Serial LFSR is used as test pattern generator in BIST. There are many applications of LFSR discussed in the paper. In multibit LFSR multiple bits shifts at every rising edge of clock pulse whereas in serial LFSR only one bit is shifted at every rising edge of clock. As multiple bit shifts in Multibit LFSR, this LFSR is more secure as compare to serial LFSR. So it is useful in cryptography area where security is main concern.

These serial LFSR and multi bit LFSR are simulated and synthesized using **Xilinx ISE 14.7.** These designs are programmed using Verilog HDL.MATLAB simulations are used to evaluate matrix operations on higher order matrices. All operations on matrix are based on modulo-2 addition.

***Index terms*- LFSR, standard, Multibit**

I. INTRODUCTION

A linear feedback shift register (LFSR) is a shift register whose input bit is a linear function of its previous state. The only linear functions of single bits are xor and inverse xor; thus it is a shift register whose input bit is driven by the exclusive-or (xor) of some bits of the overall shift register value. Some of the outputs are combined in exclusive-OR configuration to form a feedback mechanism. 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 pseudo random pattern of 1s and 0s. Note that the only signal necessary to generate the test patterns is the clock.

There are two implementation styles of LFSRs, Galois implementation and Fibonacci implementation. In Fibonacci implementation style XOR gate is present in the feedback path, therefore this style is also known as an out-of-line, simple type (S-type), standard or external feedback LFSR. LFSR in matrix form represented as X(t+1)=A X(t) where A is called transition matrix and define LFSR configuration.

In modular LFSR XOR gate is present in between flip-flops. The difference in modular LFSR compared to standard LFSR is due to the positions of the XOR gates in the feedback function. Modular LFSR works faster than standard LFSR, because it has at most one XOR gate between adjacent flip-flops, while there can be several levels of XOR gates in the feedback of standard LFSR. Since the XOR gate is in the shift register path, the Galois implementation is also known as an in-line,internal feedback or modular type (M-type) LFSR. Applications of LFSR are in Cryptography, used as a counter, used in testing for pattern generation and used as BCH and CRC encoder.

The rest of this paper is organized as follows. Section II gives Literature review of the papers which includes the study which has been done in the field of LFSR. Section III introduces the concept of matrix formation of standard LFSR according to presence of gates present in the circuit and concept of multibit LFSR. simulation results of standard and multibit LFSR are discussed in Section IV. Conclusion is drawn from the section V.

II. LITERATURE REVIEW

Keshab K. Parhi in 2004 proposed scheme for parallel BCH encoders to eliminate the effect of large fanout. Long BCH encoders suffer from effect of large fanout which further reduce clock speed. For eliminating this effect author proposed new scheme for parallel LFSR which is based on look-ahead computations and retiming and achieved speedup of 132% as compared to original parallel BCH encoders. [1]

Balwinder Singh et al., in 2009 proposed low power LFSR for generating test patterns which reduces power dissipation. Dynamic power dissipation increases because of more switching activity means more transitions. Correlation increased by generation of intermediate test vectors between successive test patterns. This approach achieved 46% less power dissipation as compared to conventional LFSR. Xpower analyser is used by the author to analyse power of proposed design. [2]

Christopher Kennedy & Arash Reyhani-Masoleh in 2009 proposed method to find vector space for frequently referenced generator polynomial when input size is equal to degree of generator polynomial. This method is proposed to obtain high speed CRC computation architecture. In this paper comparison between two vectors done in terms of number of ones, number of XOR gates, number of flip flops and pipeline stages. One vector is simple means first element is ‘1’ , all others are ‘0’ and other vector is calculated according to paper. Theoretical results are verified using computer algebra system. ASIC implementation after using this vector space gave improvement in both area and timing as compared to previous. [3]

Manohar Ayinala & Keshab K. Parhi in 2010 proposed new formulation to modify LFSR into form of an IIR filter. For reduction in critical path two techniques i.e. pipelining and retiming used by them. The comparison between proposed and previous architecture done in terms of number of XOR gates, number of delay elements and critical path for different parallelism levels (L). Proposed design achieves throughput rate at reduced hardware cost. [4]

Manohar Ayinala & Keshab K. Parhi in 2011 have given contribution in two folds. First they presented mathematical proof for linear transformation to transform LFSR into equivalent state space transformation. After using this transformation method authors achieved a full speed-up as compared to serial LFSR architectures. But speed up achieved at cost of an increase in hardware overhead. Second contribution for LFSR architecture is to give new formulation to modify LFSR into form of IIR filter. Authors proposed parallel architectures based on parallel IIR filter design, pipelining and designing algorithms. According to this approach architecture have both feedforward and feedback paths. After that they applied combined parallel and pipelining technique. This proposed scheme achieve better area time product as compare to previous design. [5]

D. Muthiah & A. Arockia Bazil Raj in 2012 proposed high speed parallel architecture which is based on pipelining and retiming algorithms for reducing critical path. In this paper BER is calculated for proposed design. This scheme can be applied to any generator polynomial. This design achieved better AT value, reduced critical path and increased throughput rate at the same time. [6]

Jaehwan Jung et al. in 2015 proposed new parallel architecture for LFSR. In previous architectures values computed from past input messages and register output but in this paper the output is calculated according to feedback values. This architecture is based on transposed LFSR. The proposed architecture achieved high speed low complexity blocks for BCH and CRC encoders. Area time product improves by 59% as compared to previous architectures. [7]

Guanghui Hu et al. in 2017 proposed a new technique for construction of transformation matrix using more efficient searching algorithm. It reduces hardware efficiency around 35%. Authors proposed parallel architecture based upon this improved state space transformation. Area Time product is calculated in this paper for various generator

polynomials and then compared with previous parallel architectures. This paper give very small value of Area Time product which is main requirement to reduce hardware complexity. Method to find improved transformation matrix is given in the paper. [8]

Debarshi Datta et al. in 2017 Authors designed multibit LFSR based PRNGs circuit using VHDL. These multibit LFSRs are synthesized using Xilinx ISE 14.7 and SPARTAN 6 FPGA to target device XC6SLX45. Authors decided to use FPGA because hardware based random number generators are faster. VHDL is used to design different length multibit LFSR. According to analysis of their proposed design result analysis 16-step 32 bit length multibit LFSR give better performance in terms of slice delay product. [9]

Anjan Kumar et al. in 2017 synthesized and simulated 4-bit LFSR on Artix-7 board by using different Input-Output standards. These standards include LVCMOS_18, HSTL_I_18, HSTL_II_18, SSTL_I_18 and SSTL_II_18. Amount of power calculated on CDMA uplink and downlink average operating frequencies. Authors found LVCMOS_18 IO standard as most power efficient standard.In this paper XNOR is used in place of XOR gate. [10]

Madhushree K & Niju Rajan in 2017 proposed a new technique to reduce dynamic power consumption in the designed circuit. This technique is called clock gating technique. System clock signal consumes main part of the dynamic power. Less power consumption is the critical requirement while designing any circuit. Authors compared the designed LFSR using clock gating technique with the serial LFSR. After using this technique 71.63% reduction in dynamic power is achieved and gain improvement in speed. [11]

Tejas Thubrikar et al. in 2017 authors proposed 32-bit test pattern generator for testing VLSI Design. This test pattern generator is designed with linear feedback shift register and with extra combination circuitry required. This TPG achieved low power consumption because the low transition LFSR is used to achieve this purpose. Low transition means switching activity between test vectors are reduced which further reduces power consumption. The paper is implemented using Xilinx tool and Verilog HDL. Total power consumption in the proposed design reduced by 50.06% as compared to conventional LFSR. [12]

III. STANDARD AND MULTIBIT LFSR

A] Standard LFSR

In standard LFSR, the input for the shift register is a feedback of modulo-2 sum of the binary weighted taps, where modulo-2 sum is performed using an exclusive-OR (XOR). Architecture of standard LFSR is given in Fig. 1.

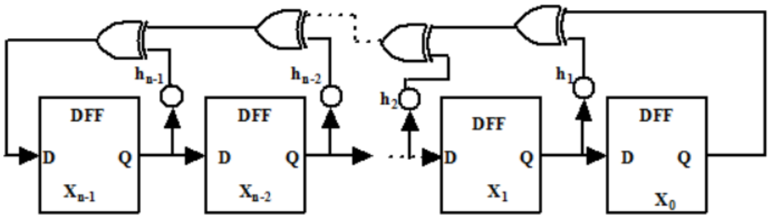

Fig. 1. Standard LFSR

The input side of the LFSR is the register Xn-1 and the output is the register X_0. When weight of h is "1" , a feedback function will be considered, when the weight is "0" then there will be no feedback (no connection). Only two exceptions that h0 and h□ should be always "1" and thus always connected directly.

B] Matrix form of LFSR

LFSR in matrix form represented as X(t+1)=A X(t) .where A is called transition matrix and define LFSR configuration. A matrix is given by fig. 2 in the form of h1,h2……..hn-1.

$$\begin{bmatrix} X_0(t+1) \\ X_1(t+1) \\ \cdots\cdots\cdots \\ X_{n-3}(t+1) \\ X_{n-2}(t+1) \\ X_{n-1}(t+1) \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0\ldots\ldots0 & & 0 \\ 0 & 0 & 1\ldots\ldots0 & & 0 \\ \cdots & \cdots & \cdots\cdots & \cdots & \cdots \\ 0 & 0 & 0\ldots\ldots1 & & 0 \\ 0 & 0 & 0\ldots\ldots0 & & 1 \\ 1 & h_1 & h_2 & h_{n-2} & h_{n-1} \end{bmatrix} \begin{bmatrix} X_0(t) \\ X_1(t) \\ \cdots\cdots\cdots \\ X_{n-3}(t) \\ X_{n-2}(t) \\ X_{n-1}(t) \end{bmatrix}$$

Fig. 2. Matrix representation of standard LFSR

LFSR can be described by characteristics polynomial given by the following equation.

$$\mathbf{f(x)=1+h_1.x+h_2.x^2+h_3.x^3+\ldots\ldots\ldots\ldots\ldots\ldots+hn_{-1}.x^{n-1}+x^n}$$

C] Concept of Multibit LFSR

In standard LFSR one bit shift at each rising edge of clock edge and n number of clock cycles are required to generate n number of random binary bits. But in multibit LFSR only one clock cycle is required to shift n number of bits. State space method can be used to find LFSR equation which is represented by X(t+1)=A.X(t). [8]

Consider characteristics equation of CRC-12 given as $f=x^{12} + x^{11} + x^3 + x^2 + x + 1$ and transition matrix A for this equation is given in Table 1.

Table 1: Transition Matrix of Standard LFSR

New Value	Transition Matrix (A)	Actual Value
X_0 (t+1)	010000000000	X_0 (t)
X_1 (t+1)	001000000000	X_1 (t)
X_2 (t+1)	000100000000	X_2 (t)
X_3 (t+1)	000010000000	X_3 (t)
X_4 (t+1)	000001000000	X_4 (t)
X_5 (t+1)	000000100000	X_5 (t)
X_6 (t+1)	000000010000	X_6 (t)
X_7 (t+1)	000000001000	X_7 (t)
X_8 (t+1)	000000000100	X_8 (t)
X_9 (t+1)	000000000010	X_9 (t)
X_{10} (t+1)	000000000001	X_{10} (t)
X_{11} (t+1)	111100000001	X_{11} (t)

Next states can be calculated from above using above relation of transition matrix. X(t+2) = A. X(t+1) = A.A.X(t) = A^2.X(t). In this case 2 bits shifts with one clock cycle. Depending upon the requirement of number of bits shift per clock cycle, transition matrix is calculated. The calculations of matrix is based upon modulo-2. For above LFSR equation A^4 is calculated using MATLAB simulations. This is known as 4-step at once and matrix A^4 mod- 2 is given by Table 2.

Table 2: Matrix for Four-step at once

	000010000000
	000001000000
	000000100000
	000000010000
	000000001000
	000000000100

A^4 mod 2	000000000010
	000000000001
	111100000001
	100010000001
	101101000001
	101010100001

From the matrix it is clear that 4 bits are obtained using XOR combination of other states but in case of standard only one bit is calculated using XOR of other.

IV. SIMULATION RESULTS

Serial LFSR in Verilog has been synthesized and simulated. Fig. 3 shows simulation waveforms of 12-bit serial LFSR for above equation $f = x^{12} + x^{11} + x^3 + x^2 + x + 1$. [7] Seed value is 010010010001, then the value of DFF changes at every positive edge of clock.

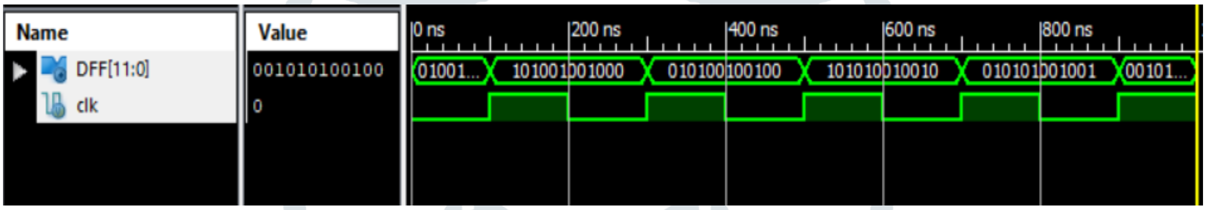

Fig. 3. Simulation results of 12-bit standard LFSR

Next multibit LFSR for different steps has been synthesized and simulated and simulation waveform of four-step of length-12, Eight-step of length-12 and 12-step of length-12 LFSR is given in Figures [4,5,6] .

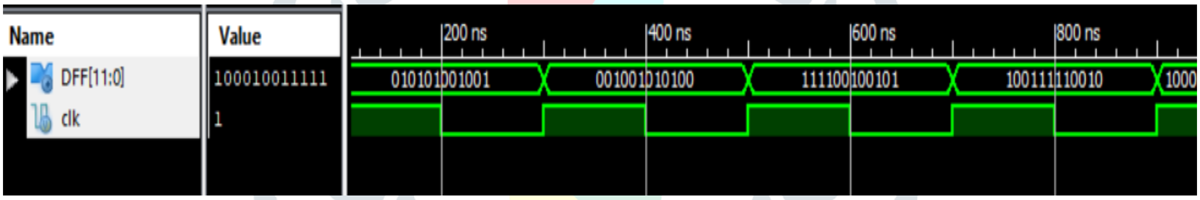

Figure 4 Simulation results of 4-step of length-12 LFSR

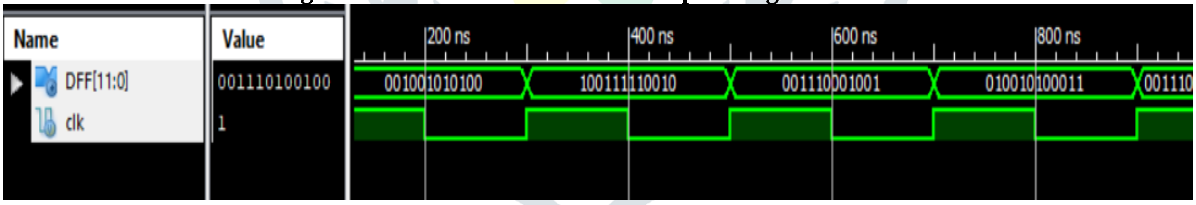

Figure 5 Simulation results of 8-step of length-12 LFSR

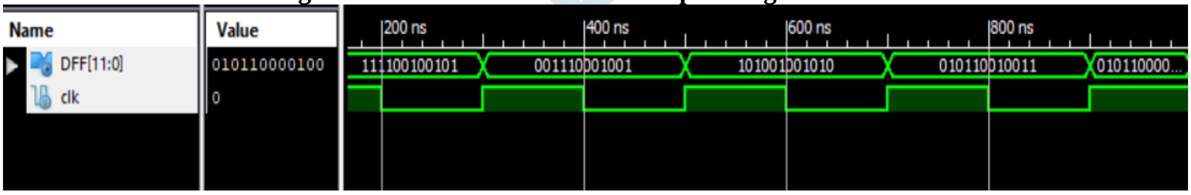

Figure 6 Simulation results of 12-step of length-12 LFSR

Comparison table of all the parameters like number of slice registers, number of slice LUT, number of LUT Flip flop pair used and number of IOB for standard and multibit LFSR is given below in Table 3.

Table 3: Utilization summary of standard and various steps multibit LFSR

Synthesis Parameter	Used in 12-bit standard LFSR	Used in 4-step length-12 LFSR	Used in 8-step length-12 LFSR	Used in 12-step length-12 LFSR

Number of Slice registers	12	12	12	12
Number of Slice LUT	5	4	8	12
Number of LUT Flip flop pairs used	8	12	8	12
Number of IOBs	13	13	13	13

V. CONCLUSION

Linear feedback shift registers play very important role in many fields like for testing, cryptography, BCH and CRC encoders. In cryptography multibit LFSR is used because it is more secure as compare to conventional LFSR. When steps is equal to length of LFSR then all bits are based on XOR combination, so multibit LFSR is used in more secure applications. Parallel LFSR is used to increase throughput of the system. In research papers of parallel LFSRs performance analysed in terms of number of ones, number of XOR gates, Delay element and Critical path delay. This Area Time product decides the hardware complexity of any system. It depends upon the selected transformation matrix. This paper can help to find best transformation matrix which can reduce hardware complexity in terms of AT value.

REFERENCES

[1] Parhi, K.K., 2004, Eliminating the fanout bottleneck in parallel long BCH encoders, *IEEE Transactions on Circuits and Systems I: Regular Papers*, *51*(3), pp.512-516.

[2] Kennedy, C. and Reyhani-Masoleh, A., 2009, June. High-speed CRC computations using improved state-space transformations, In *Electro/Information Technology, 2009. eit'09. IEEE International Conference on* (pp. 9-14). IEEE.

[3] Ayinala, M. and Parhi, K.K., 2010, October, Efficient parallel VLSI architecture for linear feedback shift registers, In *Signal Processing Systems (SIPS), 2010 IEEE Workshop on* (pp. 52-57). IEEE.

[4] Ayinala, M. and Parhi, K.K., 2011, High-speed parallel architectures for linear feedback shift registers, *IEEE transactions on signal processing*, *59*(9), pp.4459-4469.

[5] Muthiah, D. and Raj, A.A.B., 2012, February, Implementation of high-speed LFSR design with parallel architectures, In *Computing, Communication and Applications (ICCCA), 2012 International Conference on* (pp. 1-6). IEEE.

[6] Jung, J., Yoo, H., Lee, Y. and Park, I.C., 2015, Efficient parallel architecture for linear feedback shift registers, *IEEE Transactions on Circuits and Systems II: Express Briefs*, *62*(11), pp.1068-1072.

[7] Hu, G., Sha, J. & Wang, Z., 2017, High-Speed Parallel LFSR Architectures Based on Improved State-Space Transformations, *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, *25*(3), pp 1159-1163.

[8] Datta, D., Datta, B. and Dutta, H.S., 2017, March. Design and implementation of multibit LFSR on FPGA to generate pseudorandom sequence number,In *Devices for Integrated Circuit (DevIC), 2017* (pp. 346-349). IEEE.

[9] Kumar, A., Saraswat, S. and Aggarwal, T., 2017, July, Design of 4-bit LFSR on FPGA, In *Computing, Communication and Networking Technologies (ICCCNT), 2017 International Conference on* (pp. 1-6).IEEE.

[10] Madhushree, K. and Rajan, N., 2017, March, Dynamic power optimization of LFSR using clock gating, In *Innovations in Information, Embedded and Communication Systems (ICIIECS), 2017 International Conference on* (pp. 1-4). IEEE.

[11] Thubrikar, T., Kakde, S., Gaidhani, S., Kamble, S. and Shah, N., 2017, April, Design and implementation of low power test pattern generator using low transitions LFSR, In *Communication and Signal Processing (ICCSP), 2017 International Conference on* (pp. 0467-0471). IEEE.

[12] Devika, K.N. and Bhakthavatchalu, R., 2017, April, Design of reconfigurable LFSR for VLSI IC testing in ASIC and FPGA, In *Communication and Signal Processing (ICCSP), 2017 International Conference on* (pp. 0928-0932). IEEE.