World Academy of Science, Engineering and Technology
International Journal of Electrical and Computer Engineering
Vol:1, No:10, 2007

Development of State Model Theory for External Exclusive NOR Type LFSR Structures

Afaq Ahmad

***Abstract*—**Using state space technique and GF(2) theory, a simulation model for external exclusive NOR type LFSR structures is developed. Through this tool a systematic procedure is devised for computing pseudo-random binary sequences from such structures.

***Keywords*—**LFSR, external exclusive NOR type, recursive binary sequence, initial state - next state, state transition matrix.

I. Introduction

BINARY sequences whose terms depend in a simple manner on their predecessors are of great importance for a variety of applications. Such sequences are easily generated by recursive procedures and popularly known as with many names like Recursive Binary Sequences (RBS), Pseudo Random Binary Sequences (PRBSs), Maximal length sequences (m-sequences), and Pseudo Noise (PN) sequences [1 - 9]. Such kinds of sequences have an advantageous feature from the computational viewpoint, and they tend to have useful structural properties [10 - 19]. Due to only these structural properties, PRBSs have enormous applications for example: Direct Sequence Spread Spectrum (DSSS) [9, 20], Pseudo-random Number (PN) [1 - 20] generation, Built-in Self-Test (BIST) [21 - 40], Encryption – Decryption [41, 42] and Error Detection [3 - 5], [9] and many more.

The PRBSs can be easily generated by the use of simply extended circuits of shift registers, which is popularly known as Linear Feedback Shift Registers (LFSRs). Different types of LFSR structures are being used in various applications. These structures are broadly classified as:

- o External Exclusive OR (EEOR),
- o External Exclusive NOR (EENOR),
- o Internal Exclusive OR (IEOR), and
- o External Exclusive OR (EEOR) types.

Mathematical models of IEOR and EEOR structures are generously discussed in research literatures [1 – 9], [16], [18], [21], [23], [43]. But the theory and model of EENOR type of structure are not available right now although it is highly applicable in VLSI test technology. This paper presents a state model theory for EENOR type LFSR structure. An algorithmic simulation procedure is also described through this paper.

II. LFSR Theory

An LFSR is made up of two parts: a shift register and a feedback function as shown in Fig. 1. The n-bit shift register is a chain sequence of n-bits of D – flip-flops. Each time a new bit is needed to load the first bit of the chains of D type flip-flops (see Fig. 2a, for D type flip-flop). The all others of the bits in the shift register are shifted one bit to the right. The feedback function is simply the Exclusive-NOR (Fig. 2b refers to Exclusive-NOR function) of certain bits of the register. The list of these bits is called feedback tappings. The new left most bit's state (first bit of D – flip-flops) is computed as a function of the existing feedback tappings of feedback function of the shift register. Since the exclusive NOR operation is carried out externally, therefore, such structure is called EENOR type of LFSR structures.

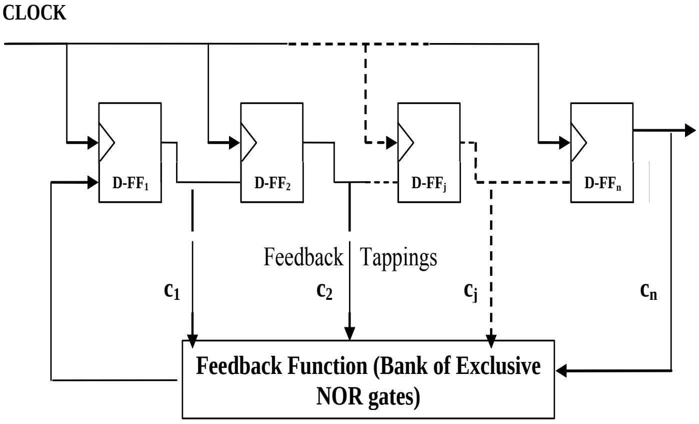


Fig. 1 A General Model of an n-bit LFSR

The output of the feedback shift register is one bit at each clock, often the most significant bit a clock before. The period of a shift register is the length of the output sequence before it starts repeating. An example of such generated sequence is as:

a = [01110100101011010111010010101101], having period p = 16 time unit, is represented in signal form in Fig. 3. Shown in Table I is one such of the patterns produced by the LFSR of 5-bit in size having structure of Fig. 4, with the assumption

Manuscript received October 6, 2005. This work was supported in part by the internal research grant of Sultan Qaboos University, Oman under Grant IG/ENG/ECED/04/04. The acknowledgements are due to authorities of the University for providing research support grant.

A. Ahmad is with the Department of Electrical & Computer Engineering, College of Engineering, Sultan Qaboos University, P.O. Box 33 Al-Khod, Muscat, Sultanate of Oman 123; Tel: + 968 24415327 Fax: + 968 24413454; E-mail: afaq@squ.edu.om

that the bit pattern of 00001 was used as an initial state and feedback tappings are taken from 3rd and 5th bits of flip-flops.

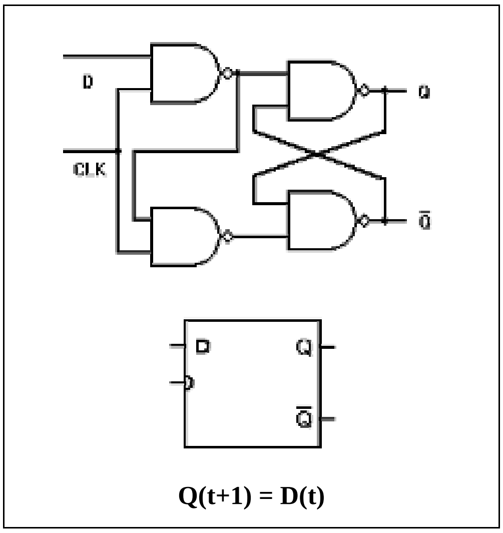
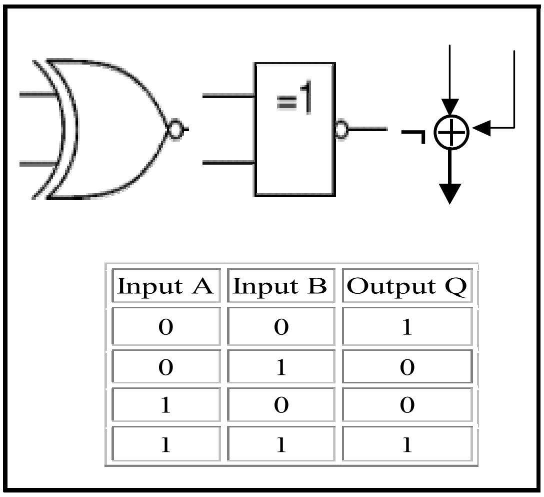


Fig. 2a Theory and model of D type flip-flop



Input A	Input B	Output Q
0	0	1
0	1	0
1	0	0
1	1	1

Fig. 2b Theory and model of exclusive or function

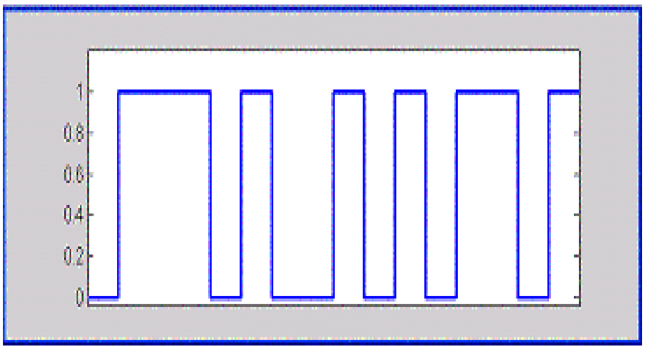


Fig. 3 waveform of the PRBS

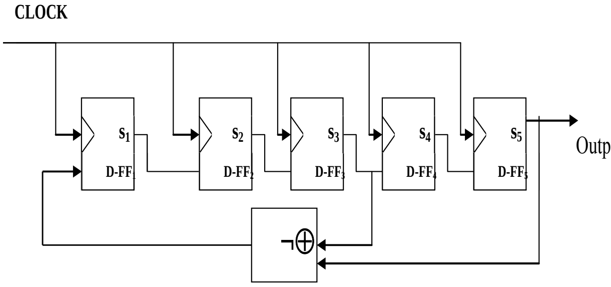


Fig. 4 a 5-bit LFSR

TABLE I
PRBS GENERATED BY LFSR STRUCTURE OF FIG. 4

Clock	D-FF1	D-FF2	D-FF3	D-FF4	D-FF5	Comment
0	0	0	0	0	1	Seed
1	0	0	0	0	0	
2	1	0	0	0	0	
3	1	1	0	0	0	
4	1	1	1	0	0	
5	0	1	1	1	0	
6	0	0	1	1	1	
7	1	0	0	1	1	
8	0	1	0	0	1	
9	0	0	1	0	0	
10	0	0	0	1	0	
11	1	0	0	0	1	
12	0	1	0	0	0	
13	1	0	1	0	0	
14	0	1	0	1	0	
15	1	0	1	0	1	
16	1	1	0	1	0	
17	1	1	1	0	1	
18	1	1	1	1	0	
19	0	1	1	1	1	
20	1	0	1	1	1	
21	1	1	0	1	1	
22	0	1	1	0	1	
23	1	0	1	1	0	
24	0	1	0	1	1	
25	0	0	1	0	1	
26	1	0	0	1	0	
27	1	1	0	0	1	
28	0	1	1	0	0	
29	0	0	1	1	0	
30	0	0	0	1	1	
31	0	0	0	0	1	Starts repeating
Period of Pseudorandom PRBS is 31 (which is 2^5-1). The generated sequence is of maximal length.						
Pseudorandom PRBS (1 0 0 0 0 0 1 1 1 0 0 1 0 0 0 1 0 1 0 1 1 1 1 0 1 1 0 1 0 0 1)						

III. LFSR STATE MODEL

Let, for an n-stage LFSR shown in Fig. 1, [A] represents the state transition matrix of an n × n order. Let the state at any time ‘t’ be represented by vector $[S(t)]=[s_1(t), s_2(t), ...,s_n(t)]$ (which is effectively the contents of the LFSR) where each s_j represents the state of the j^{th} stage of the LFSR. Further, let the LFSR stage is numbered from 1 to n, proceeding in the same direction as the shifting occurs. Let the present state of the LFSR be represented by [S(t)] and, one clock later, the next state by [S(t+1)]; then the relationship between the two states is given by:

$$\begin{bmatrix} s_1(t+1) \\ s_2(t+1) \\ : \\ s_j(t+1) \\ : \\ s_{n-1}(t+1) \\ s_n(t+1) \end{bmatrix} = \begin{bmatrix} c_1\neg & c_2\neg & c_3\neg & : & c_{n-2}\neg & c_{n-1}\neg & 1 \\ 1 & 0 & 0 & : & 0 & 0 & 0 \\ 0 & 1 & 0 & : & 0 & 0 & 0 \\ 0 & 0 & 1 & : & 0 & 0 & 0 \\ : & : & : & : & : & : & : \\ 0 & 0 & 0 & : & 1 & 0 & 0 \\ 0 & 0 & 0 & : & 0 & 1 & 0 \end{bmatrix} * \begin{bmatrix} s_1(t) \\ s_2(t) \\ : \\ s_j(t) \\ : \\ s_{n-1}(t) \\ s_n(t) \end{bmatrix} \quad (1)$$

Where $c_j\neg = 0$ or 1, for $1 \le j \le n-1$, depends upon the existence or absence of the tap connections to the EENOR bank from the respective output of the flip-flops. And, since the last bit of the LFSR is always connected, therefore, $c_n\neg = 1$. The connection vector (CON) can be represented as, CON = [$c_1\neg$ $c_2\neg$ ….. $c_{n-1}\neg$ $c_n\neg$ }.

Equation (1) can be written as

$$[S(t+1)] = [A][S(t)] \quad (2)$$

If [S] = [S(0)] represents a particular initial loading of the LFSR, then the sequence of states through which the LFSR will pass during successive times is given by

$[S(t)], [A][S(t)], [A]^2[S(t)], [A]^3[S(t)], \dots$

Let the matrix 'period' be the smallest integer p for which $[A]^p = I$, where I is an identity matrix. Then $[A]^p[S(t)] = [S(t)]$ for any non zero initial vector [S(0)], indicating the 'cycle length (or period)' of the LFSR is p.

Thus, on the basis of this property of periodicity of LFSR and Equation (3), it follows that

$$[S(t)] = [S(t+p)] = [A]^p[S(t)] \quad (3)$$

IV. GF(2) for EENOR and Computation Method

GF(2) multiplication and addition operations are described in Table II. The Table III contains developed models for EENOR multiplication and addition operations for the purpose of simulating Equation 1. Finally, the whole process for computing the next state sequences through state space model is summarized below in the form of an algorithm.

TABLE II
GF(2) ADDITION AND MULTIPLICATION OPERATIONS

	+		x	
	0	1	0	1
0	0	1	0	0
1	1	0	0	1

TABLE III
¬GF(2) ADDITION AND MULTIPLICATION OPERATIONS

	+		x		
	0	1	c_i	0	1
0	1	0	0	0	0
1	0	1	1	1	0

Algorithm

(For an n-bit LFSR)

STEP 1:

Check if CON has total number of c_j's as odd number, then, Go To STEP 3, else Go To STEP 2.

STEP 2:

Compute the value of $s_1(t+1)$ by using the Equation 4 described below. The computation is carried out using GF(2) table for multiplication and ¬ GF(2) for addition as described in Table 2 and 3 respectively. For computing $s_i(t+1)$, for j = 2, 3, 4 ….., n; Go To STEP 4.

$$s_{1(t+1)} = \sum_{j=1}^{n} c_j * s_{j(t)} \quad (4)$$

STEP 3:

Compute the value of $s_1(t+1)$ as using the Equation 4 given above. The computation is carried out using tables GF(2) for addition and ¬ GF(2) for multiplication as described in Table 2 and 3 respectively. For computing $s_{i(t+1)}$, for j = 2, 3, 4 ….., n; Go To STEP 4.

STEP 4:

For other values of $s_i(t+1)$, for j = 2, 3, 4 ….., n; can be computed using Equation 5 as given below where the operations of addition and multiplications are carried out using. GF(2) as given in Table II.

for j = 2, 3, 4 ….., n;

$$s_j(t+1) = s_{j-1}(t) \quad (5)$$

STEP 5:

STOP

V. Computation – An Example

To demonstrate the procedure of algorithm below is an example to make the steps more elaborative.

Let n = 4, CON = [0 1 1 1] which has 3 (odd) total entries. Assume S = [1 0 1 1] = $(D)_{Hex}$

s_1(next state) = 0*1 + 1*0 + 1*1 + 1*1
s_1(next state) = 0 + 1 + 0 +0 = 1
s_2(next state) = s_1(previous state) = 1
s_3(next state) = s_2(previous state) = 0
s_4(next state) = s_3(previous state) = 1

Thus, S(next state) = [1 1 0 1] = $(B)_{Hex}$ which can be verified from the Table IV (check upon s_0 and s_1 in column II of the table).

Let us consider another CON = [0 0 1 1] which has 2 (even) total entries. Assume S = [1 1 0 0] = $(03)_{Hex}$

s_1(next state) = 0*1 + 0*1 + 1*0 + 1*0
s_1(next state) = 0 + 0 + 0 + 0 = 1
s_2(next state) = s_1(previous state) = 1
s_3(next state) = s_2(previous state) = 1
s_4(next state) = s_3(previous state) = 0

Thus, S(next state) = [1 1 1 0] = $(7)_{Hex}$ which can be verified from the Table IV (check upon s_0 and s_1 in column III of the table).

For n = 2 to 32 EENOR LFSR structures are tested and results are verified. It is difficult to present the results, however, in Table V, the simulation results for n = 3, with all possible initial states (2^n), and all possible CONs (2^{n-1}) are given to put confidence in the readers.

TABLE IV
AN EXAMPLE OF COMPUTATION FOR A 4-BIT LFSR

	CON = [0 1 1 1]	CON = [0 0 1 1]
States	s_0 = [1 0 1 1] = $(D)_{Hex}$	s_0 = [1 1 0 0] = $(3)_{Hex}$
s_0	D	3
s_1	B	7
s_2	7	E
s_3	F	D
s_4	E	B
s_5	C	6
s_6	9	C
s_7	2	9
s_8	4	2
s_9	8	5
s_{10}	0	A
s_{11}	1	4
s_{12}	3	8
s_{13}	6	0
s_{14}	D	1

TABLE V
AN EXAMPLE OF COMPUTATION FOR A 3-BIT LFSR

s_0	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
s_1	1	3	5	7	0	2	4	6	1	3	4	6	0	2	5	
s_2	3	7		6	1		0	4	3	6	0	5	1	4	2	
s_3	7	6		4	3		1	0	6	5	1	2	3	0	4	
s_4	6	4		0	7		3	1	5	2	3	4	6	1	0	
s_5	4	0		1	6		7	3	2	4	6	0	5	3	1	

States (in Hex)	CON = [1 0 1]								CON = [1 1 1]							
s_0	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
s_1	1	2	5	6	0	3	4		1	2	4	7	0	3	5	6
s_2	2	5	3	4	1	6	0		2	4	0	6	1	7	3	5
s_3	5	3	6	0	2	4	1									
s_4	3	6	4	1	5	0	2									
s_5	6	4	0	2	3	1	5									

VI. CONCLUSION

A state model theory for an external exclusive NOR based LFSR structure is developed. Based upon which an algorithm is developed to compute the PRBSs. Since a unified approach is not adapted in mdeling the LFSRs therefore, this is an orientation to that direction. In future it is highly desired to observe a standard approach for modeling any kind of LFSR i.e. internal or external structures with exclusive OR or NOR based feedbacks. Currently, a lot of scope of research is highly demanding due to outburst applications of LFSRs.

REFERENCES

[1] N. Zierler & J. Brillhart, “On Primitive Trinomials (Mod 2),” *Information and Control* 13, pp. 541-554, 1968

[2] N. Zierler & J. Brillhart, “On Primitive Trinomials (Mod 2), II,” *Information and Control* 14, pp. 566-569, 1969

[3] S. W. Golomb, “Shift Register Sequence”, Second Edition - *Holden-Day*, 1982

[4] R.E. Blahut, “Theory and Practice of Error Control Codes”, *Addison-Wesley*, MA, 1983

[5] W. W. Peterson and E. J. Weldon, Jr., “Error-Correcting Codes”, Second Edition - *The MIT Press*, 1984

[6] P. H. Bardell, “Design Considerations for Parallel Pseudorandom Pattern Generators,” JETTA, Vol. 1, No. 1, pp. 73-87, Feb. 1990

[7] P.H. Bardell, "Design considerations for parallel pseudorandom pattern generators," *Journal of Electronic Testing and Applications*, Vol. 1, No. 1, pp. 73-87, 1990

[8] A Ahmad, A. Al-Lawati, “Reducing Test Time Via An Optimal Selection of LFSR Feedback Taps”, *IEEE Proceedings - IEEE Catalog 01EX467C (ISSPA’01- Malaysia)*, August, pp. 1-4, 2001

[9] A. Ahmad, Z. Nadir, F. A.Khan, “FPGA Based Design Of Faster PN Generators For The Use Of CDMA Applications” *Proceedings Wireless and Optical Communications Networks (WOCN 2004), IFIP TC6/ IEEE*, June 7 – 9, pp 272 – 275, 2004

[10] L.T. Wang and E.J. McCluskey, "Linear feedback shift register design using cyclic codes," *IEEE Transactions on Computers*, Vol. C-37, No. 10, pp. 1302-1306, 1987

[11] T.W. Williams, W. Daehn, M. Gruetzner and C.W Starke, "Bounds and Analysis of Aliasing Errors in Linear Feedback Shift Registers", IEEE Trans. Computer Aided-Design, Vol. CAD-7 No. 1, Jan., pp. 75-83, 1988

[12] N. K Nanda., A. Ahmad and V.C. Gaindhar, (1989) ‘Shift register modification for multipurpose use in combinational circuit testing,’ *International Journal of Electronics* (UK), vol.66, no.6, pp.875-878, 1989

[13] A. Ahmad, N. K. Nanda and K Garg, "Are Primitive Polynomials Always Best in Signature Analysis?", *IEEE Design & Test of Computers*, Vol. 7, No. 4, Aug. 1990, pp. 36-38.

[14] S. Hellebrand, S. Tarnick, J. Rajski and B. Courtois, "Generation of vector patterns through reseeding of multiple-polynomial linear feedback shift registers," in *Proceedings of IEEE International Test Conference*, , pp. 120-129, 1992

[15] J. Savir and W.H. McAnney, "A multiple seed linear feedback shift register," *IEEE Transaction on Computers*, Vol. 41, No. 2, pp. 250-252, 1992

[16] A. Ahmad, “Critical role of polynomial seeds on the effectiveness of an LFSR-based testing technique,” *International Journal of Electronics* (UK), vol.77, no.2, pp.127-137, 1994

[17] A. Ahmad, “Achievement of higher testability goals through the modification of shift register in LFSR based testing,” International Journal of Electronics (UK), vol. 82, no. 3, pp. 249-260, 1997

[18] A. Ahmad, M. J. Al-Musharafi, S. Al-Busaidi, “Study And Implementation Of Properties Of m-Sequences In MATLAB-SIMULINK – A Pass/Fail Test Tool For Designs Of Random Generators”, *SQU Journal of Scientific Research – Science and Technology*, vol. 7, part 1, June 2002, pp. 147 –156.

[19] C. V. Krishna, A. Jas, N. A. Touba, “Achieving high encoding efficiency with partial dynamic LFSR reseeding”, *ACM Transactions on Design Automation of Electronic Systems*, Volume 9 , Issue 4 (October), pp. 500 – 516, 2004

[20] A. Guha and L.L. Kinney, "Relating the cyclic behavior of linear and intra-inverted feedback shift registers," *IEEE Transactions on Computers*, Vol. C-41, No. 9, 1992, pp. 1088-1100.

[21] R.A. Frohwerk, "Signature analysis: A new digital field service method," *Hewlett-Packard Journal*, Vol. 28, No. 9, pp. 2-8, 1977

[22] B. Konemann, J. Mucha and G. Zwiehoff, "Built-in logic block observation technique," *Digest of Papers 1979 Test Conference*, pp. 37-41,1979

[23] .J.E. Smith, "Measures of the effectiveness of fault signature analysis," *IEEE Transactions on Computers*, Vol. C-29, No. 6, pp. 510-514, 1980

[24] Z. Barzilai, D. Coppersmith and A.L. Rosenberg, "Exhaustive generation of bit patterns with applications to VLSI self-testing," *IEEE Transactions on Computers*, Vol. C-32, No. 2, pp. 190-194, 1983

[25] T. W. Williams, "VLSI Testing", *IEEE Computer*, Vol. C-17, No. 10, Oct., pp. 126-136, 1984

[26] S.B. Akers, "On the use of linear sums in exhaustive testing," *Digest of Papers 15th Annual International Fault-Tolerant Computing Symposium*, pp. 148-153, 1985

[27] E. J. McCluskey, "Built-In Self-Test Techniques", *IEEE Design & Test of Computers*, Vol. 2, No. 2, April 1985, pp. 21-28.

[28] C.L. Chen, "Linear dependencies in linear feedback shift registers," *IEEE Transactions on Computers*, Vol. C-35, No. 12, pp. 1086-1088, 1986

[29] P.H. Bardell, W.H. McAnney and J. Savir, *Built-in Test for VLSI: Pseudorandom Techniques*, Wiley, New York, 1987

[30] P. H. Bardell, W.H. McAnney, and J. Savir, Built-In-Test for VLSI, New York: John Wiley, 1987

[31] W.B. Jone and C.A. Papachristou, "A coordinated approach to partitioning and test pattern generation for pseudo-exhaustive testing," in *Proceedings of 26th ACM/IEEE Design Automation Conference*, pp. 525-530, 1989

[32] M. Abramovici, M.A. Breuer and A.D. Friedman, *Digital Systems Testing and Testable Design*, Computer Science Press, New York, 1990.

[33] R. Raina and P.N. Marinos, "Signature analysis with modified linear feedback shift registers (M-LFSRs)," in *Proceedings of Fault-Tolerant Computing: 21st International Symposium*, pp. 88-95, 1991

[34] S. Venkataraman, J. Rajski, S. Hellebrand and S. Tarnick, "An efficient BIST scheme based on reseeding of multiple polynomial linear feedback shift registers," in *Proceedings of ICCAD-93*, pp. 572-577, 1993

[35] R. Srinivasan, S.K. Gupta and M.A. Breuer, "Novel test pattern generators for pseudo-exhaustive testing," in *Proceedings IEEE International Test Conference*, pp. 1041-1050, 1993

[36] S. Venkataramann, J. Rajski, S. Hellebrand, and S. Tamic, "An Efficient BIST Scheme Based on Reseeding of Multiple Polynomial Linear Feedback Shift Register", *Proc. Int'l. Conf. on Computer -Aided Design (ICCAD)*, pp. 572-577, 1993

[37] C.A. Chen and S.K. Gupta, "A methodology to design efficient BIST test pattern generators," in *Proceedings of IEEE International Test Conference*, pp. 814-823, 1995

[38] C.A. Chen and S.K. Gupta, "BIST test pattern generators for two-pattern testing - theory and design algorithms," *IEEE Transactions on Computers*, Vol. 45, No. 3, pp. 257-269, 1996

[39] N. A. Touba and E. J. McCluskey, "RP-SYN: Synthesis of Random-Pattern Testable Circuits with Test Point Insertion", *IEEE Trans. Computer- Aided Design*, Vol. CAD-18, No. 8, Aug. 1999, pp. 1202-1213.

[40] A. Ahmad, "Constant Error Masking Behavior of An Internal X-OR Type Signature Analyzer Due To The Changed Polynomial Seeds", Journal Of Computers & Electrical Engineering (PERGAMON, Elsevier Science), Vol. 28, No. 6, pp. 577 - 588, 2002

[41] A. Ahmad, M. J. Al-Musharafi., S. Al-Busaidi, "Design and study of a Strong Stream Crypto-System Model for e-Commerce", International Council for Computer Communication Publishers – Washington DC, USA (The ACM Library), pp. 619 – 630, 2002

[42] T. Jamil, A. Ahmad, (April 2002) "An Investigation in to the Application of Linear Feedback Shift Registers for Steganography", Proceedings IEEE SoutheastCon2002, April, pp. 239-244, 2002

[43] A. Ahmad, A. M Elabdalla, "An efficient method to determine linear feedback connections in shift registers that generate maximal length pseudo-random up and down binary sequences," Computer & Electrical Engineering -An Int'l Journal (USA), vol. 23, no. 1, pp. 33-39, 1997

Afaq Ahmad: Born in India (Azamgarh). Ahmad obtained BSc Eng, MSc Eng, DLLR and Ph.D degrees in electrical, control, industrial and computer engineering respectively.

He has a professional experience of about 30 years which includes teaching undergraduate and post graduate, BS and MS projects, MS and Ph.D dissertations. He has vast experience of consultancies, research projects, and community services. He has pioneering experiences of computerized examinations, curriculum design, timetabling. He is author of about 60 research papers in journals and conference proceedings of international repute. Currently, his research interests are in Fault-Tolerant Computing, VLSI Testing and Fault Diagnosis including Coding theory.

Dr. Afaq Ahmad is Fellow (Life Fellow-ship) member of Institution of Electronics and Telecommunication Engineers (IETE), India. Dr. Ahmad is also Member (Life Member-ship) of System Society of India (SSI). Dr. Ahmad is Member of IEEE (USA) as well.