International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 3 Issue 7, July-2014, pp: (217-222), Impact Factor: 1.252, Available online at: www.erpublications.com

Design and Synthesis of 32 Bits Linear Feedback Shift Registers Architecture with Power Optimization

Sandeep[1], Dr. Raj kumar Yadav[2], Rajesh kumar[3]
[1,2,3]E.C.E. Department, MRKIET REWARI, INDIA

Abstract: **LFSR based PN number generating technique is used for various cryptography applications for designing with various encoder and decoder architecture. It is used for getting efficient result. Modern field programmable gate arrays (FPGAs) include the resources needed to design efficient LFSR structures. LFSR are used for implementation any logic functions for faster prototype development. It is necessary to implement the existing design of LFSR on FPGA to test and simulation and synthesis result between different lengths. The total no of random state depend on the feedback polynomial. It is a simple counter with count maximum of using feedback polynomial. In this paper power optimized upto 25.9% in FPGA by implementation of 32-bit LFSR & also compared with 8-bit and 16-bit LFSR.**

Keywords: LFSR, FPGA, VHDL, PNSRG, PRBS.

I. Introduction

Use of Linear Feedback Shift Register (LFSR) is being studied extensively by Engineers, Designers and Researchers working in testing design for testability and Build-In Self-Test (BIST) environment. LFSRs are rather attractive structures for use in these environments for some of the following reasons.

LFSRs have a simple and fairly regular structure. Their shift property is easily Integra table in the scan design environment. They are capable of generating exhaustive and/or random vectors and their error detection & error correction properties make them prime candidates for signature analysis, test pattern generation, image size scaling applications etc [1].These applications requires low power dissipations for VLSI circuits. The power dissipation during test mode is 200% more than in normal mode [2]. Hence it was the important aspect to optimize power during testing .So that in the further work Power during testing was reduced up to 46% and output dynamic power reduced upto 44.6% [3].Power dissipation in the test mode is generally greater than in the normal mode as toggling of flip-flops is greater during the test mode, High power consumption during testing results in destruction of circuit reliability. A circuit under test (CUT) mal function can occur due to excessive voltage drop or ground bounce caused by high current in the test mode. Therefore low power dissipation during test application, cost and time for testing are the major goals in the future development of VLSI design [4],[5],[6],[7]. The major drawback of BIST is the delay increase in normal operation due to the insertion of circuits for test and the increase in test time as the number of primary inputs (PIs) Increases. The operation speed of a device increase with decrease in its size, which in turn conceals the increase in delay time. A method called input grouping used to reduce Test length for BIST application [4],[8]. Paper [4] presents an approach to reduce the test time of an external test applied from automatic test equipment by speeding up low activity cycles, keeping the power under control. Based on the signal transitions, which are used to control the power consumption of the Circuit under test, the clock frequency can be varied. Two different methods have been considered for controlling the scan clock frequency: using hardware control and using pre-simulated and stored test data where a dynamically controlled scan clock is used. Linear feedback shift register (LFSR) reseeding forms the basis for many test-compression solutions. A seed can be computed for each test cube by solving a system of linear equations based on the feedback polynomial of the LFSR.

II. LINEAR FEEDBACK SHIFT REGISTER

LFSR is a circuit consists of flip-flop in series. LFSR is a shift register where output bit is an XOR function of some input bits. The initial value of LFSR is called seed value. LFSR's seed value has a significant effect on energy consumption. The output that influence the input are called tap. A LFSR is represented by as polynomial, which is also known as characteristic polynomial used to determine the feedback taps, which determine the length of random pattern generation. The output of LFSR is combination of 1's and 0's. A common clock signal is applied to all flip-flops, which enable the propagation of logical values from input to output of flip-flop. In computing, a linear-feedback shift register (LFSR) is a shift register whose input bit is a linear function of its previous state. The most commonly used linear function of single bits is XOR. Thus, an LFSR is most often 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 called the seed. The stream of

values produced by the register is completely determined by its current (or previous) state. Likewise, because the register has a finite number of possible states, it must eventually enter a repeating cycle. However, an LFSR with a well-chosen feedback function can produce a sequence of bits which appears random and which has a very long cycle. There are various method are pseudo number are known as linear configuration equation in contrast the use of feedback shift register permits very fast binary sequences.

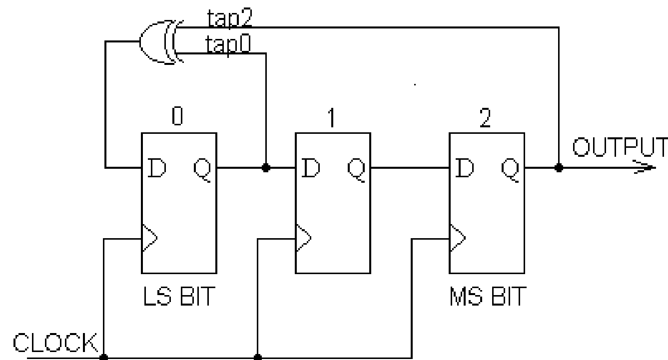


Figure 1. Typical Linear feedback shift Configuration

The bits in the LFSR state which influence the input are called Taps. A maximum length LFSR produce an m sequence. The period of the sequence is $2^n - 1$, where n is the number of shift register used in design. For 32 bit the period is large enough for design practical purpose. The arrange of taps for feedback in LFSR can be expressed in finite field expressed Arithmetic polynomial modulo 2. For example, if the Tap is the 32nd, 30th, 11th and 5th bits then the feedback polynomial is maximum length polynomial is used for memory utilization and power requirement. We have comparison of performance result of simulation and synthesis of different bit-length LFSR. The target device we have used Xilinx 3S Xc3s500e-4ft256 and performed operation Xilinx ISE 10.1.Application of LFSR is Generation of Pseudo-random sequences, uses in Circuit Testing, Test Pattern Generation, Signature Analysis, uses in Cryptography, used to increase the accuracy of received time and the robustness of the data stream in the presence of noise, High Speed Address Generator for Image Watermarking and for Image Size Scaling etc.

III. 32 bit Generic Linear Feedback Register

It is most commonly used topology for pseudo random bit sequence no generating technology it is obtained with an array of FFs with a Linear Feedback performed by several XOR gates .A 32 bit LFSR is characterized by its feedback polynomial given by

$$P(x) = x^{32} + x^{22} + x^{2} + x^{1} + 1 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

However they can be efficient describe through the N order polynomial where the binary coefficient define the well known polynomial characteristic of its [9].

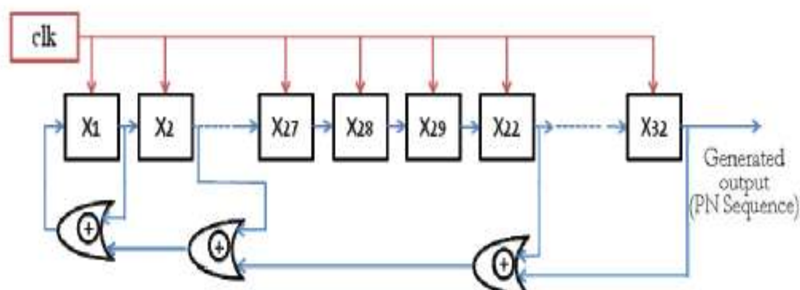


Figure 2. 32 bit linear feedback Shift Register

The circuit diagram for 32-bit LFSR with maximum length polynomial shown in Figure 2 and we can observe that randomness behavior for 32 bit LFSR from 30225 to30500ns for using Xilinx 10.1 simulator.

(A) LFSR Architecture

It is very important to choose the proper LFSR architecture for achieving the appropriate fault coverage. Every architecture consumes different power even for same polynomial. Another problem associated with choosing LFSR is LFSR design issue, which includes LFSR partitioning, in this the LFSR are differentiated on the basis of hardware cost and testing time cost . A typical architecture consists of a test pattern generator (TPG), usually implemented as a linear feedback shift register (LFSR), a test response analyzer(TRA), implemented as a multiple input shift register(MISR), and BIST control unit(BCU), all implemented on the chip(Fig.3).

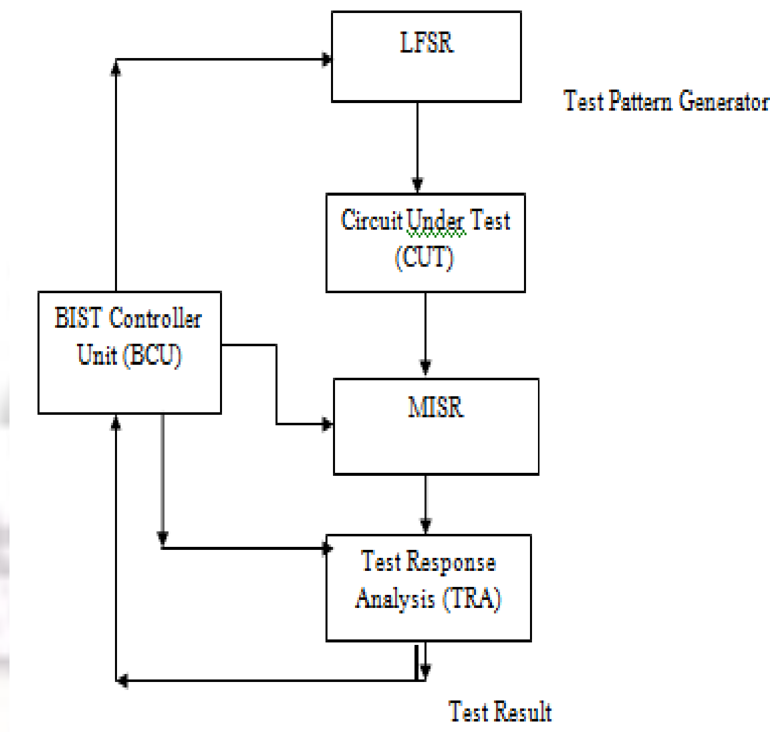


Figure 3. LFSR Architecture

This approach allows applying at speed test and eliminates the need of an external tester. The BIST architecture components are given below:

1- Circuit Under Test (CUT)- It is the portion of the circuit tested in BIST mode. It can be sequential , combinational or a memory. Their Primary Input (PI) and Primary Output (PO) delimit it.

2- Test Pattern Generator (TPG)- It generates the test pattern for CUT. It is a dedicated circuit or a microprocessor. The patterns may be generated in pseudorandom or deterministically.

3- Multiple input signatures registers (MISR)- It is designed for signature analysis , which is a technique for data commpression. MISR efficiently map different input streams to different signstures with every small probability of alias. MISR are frequently implemented in built-in-self-test (BIST) design, in which output responses are compressed by MISR.

4- Test Response Analysis (TRA)- It analyses the value sequence on PO and compare s it with the expected output.

5- BIST Controller Unit(BCU)- It controls the test execution ; it manages the TPG , TRA and reconfigures the CUT and the multiplexer. It is activated by the Normal/Test signal and generates a Go/No go.

International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 3 Issue 7, July-2014, pp: (217-222), Impact Factor: 1.252, Available online at: www.erpublications.com

(B) Algorithm of Linear feedback shift Register:

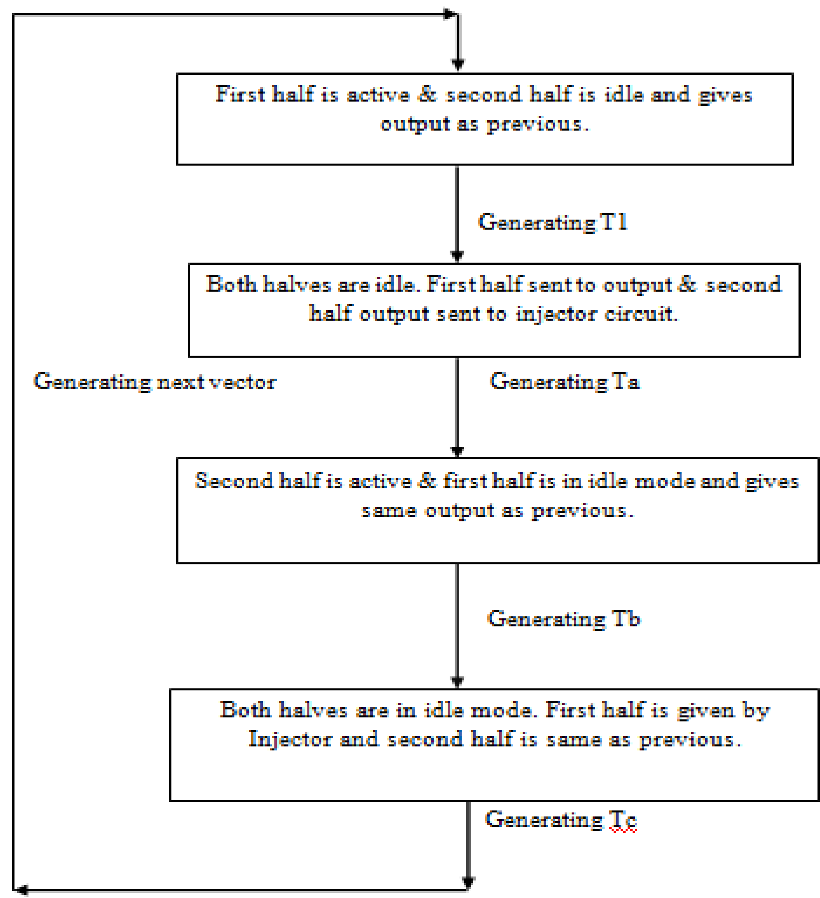
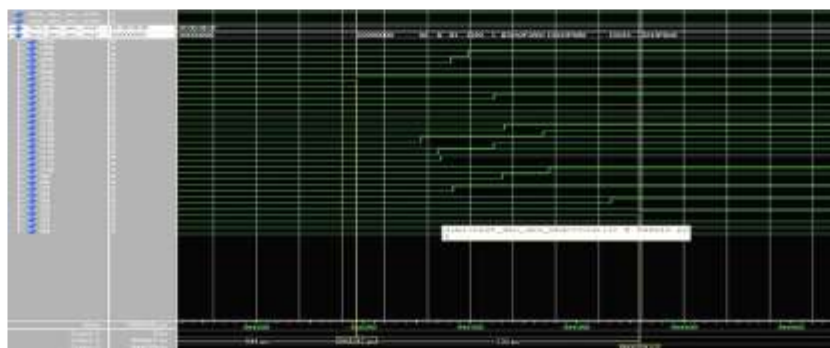


Figure 4. Algorithm for LFSR

The initial value of LFSR is called seed value. LFSR's seed value has a significant effect on energy consumption. Increasing the correlation between bits reduces the power dissipation. This can be achieved by adding more number of test vectors, which decreases the switching activity. LFSR is characterized by the polynomial by its characteristics polynomial and inverse of characteristics polynomial is generated polynomial. In this approach the 3 intermediate test vectors are generated between every two successive vectors (say T1, T2) .The total number of signal transition occurs between these 5 vectors are equivalent to the number of transition occurs between the 2 vectors. Hence the power consumption is reduced [6]. Additional circuit is used for few logic gates in order to generate 3 intermediate vectors. The 3 intermediate vectors (Ta, Tb, Tc) are achieved by modifying conventional flip-flops outputs and low power outputs [6]. The first level of hierarchy from top to down includes logic circuit design for propagation either the present or next state of flip-flop to second level of hierarchy. Second level of hierarchy is implementing Multiplexed (MUX) function.

IV. (A) Syntheses result



(B) Comparison of performance of parameter of 8-bit, 16-bit and 32-bit LFSR.

Performance	8bit	16bit	32bit
Time to complete	40ns to5140ns =5100ns	20 ns to 1310720 ns =310.7us	20 ns to 85899345920= 85.9sec
Total no of Random State generating	255	65535	429,49,67,295
Clock	12.800	12.800	12.800
Shift Resister	08	16	32
No of slice	04	09	18
No of flip flop	08	16	32
Total memory used	185904kb	185904 kb	185904 kb
G clk	01	01	01
Gate +net delay	7.21ns	7.27ns	7.27 ns
Total pin	40	18	34

It is clearly found from above table that 8 bit 16 bit and 32 bit LFSR with maximum feedback polynomial can generate maximum random output [9]. The 32 bit LFSR takes a lot of simulation time 85.9 sec with 12.800 ns clock period for generating $2^{32} - 1$= 429,49,67,295 random output. Also we can find the memory utilization is same for all three LFSR. Definitely 32 bit LFSR with maximum length feedback polynomial will generate large sequence which is more secure than other but because of simulation difficulties modification in long bit LFSR is needed. In the practical use 8-bit and 16-bit LFSR is sufficient for different cryptographic applications.

V. Conclusion

(A) Power analyzer report:

Name	Power(W)	Used	Total Available	Utilization (%)
Clock	0.006	2	-	-
Logic	0.000	45	12288	0.4
Signals	0.000	55	-	-
IOs	0.000	22	240	9.2
DCMs	0.000	0	4	0.0
Total Quiescent Power	0.253			
Total Dynamic Power	0.006			
Total Power	0.259			

In case of EDA tool we have used LFSR is coded in VHDL and seeded value of 32- bit, the generated code is synthesized in Xilinx for the Spartan 3e devices. The hardware summary is obtained by log file of Xilinx. It is observed that the total power consumed in modified LFSR is 25.9% less than the power consumed by normal LFSR. It is concluded that low power LFSR is very useful for the BIST implementation in which the circuit under test (CUT) may be Combinational , Sequential and Memory Circuit.

VI. Future Scope:

It has observed that in case of the higher no. of bits so that there are problems of longer time and more power consuming during circuit under test (CUT) when used FPGA implementation. Further extend this work reduced power consumption using low power LFSR using various low power VLSI technique. We can further decrease the power consumption during testing in VLSI implementation.

References

[1]. Zhanglei Wang, Hongxia Fang, Krishnan Chakraarty, Fellow, IEEE, and Michael Bienek "Deviation-Based LFSR Reseeding for Test-Data Compression". IEEE Transactions On Computer-Aided Design of Integrated Circuits and Systems Vol.-28 No.-2, Feb.2009.

[2]. E. Atoofian, S. Hatami, Z. Navabi, M. Alisaface and A. Afzali-Kusha," A New Low-Power Scan-Path Architecture," IEEE International Symposium, Vol.5, pp.5278 - 5281, 23-26 May 2005.

[3]. Balwinder Singh, run Khosla, Sukhleen Bindra "Power Optimization of Linear Feedback Shift Register (LFSR) for Low Power BIST". 2009 IEEE International Advance Computing Conference (IACC 2009) Patiala, India, 6-7 March 2009.

[4]. S.Sivanantham, Ganga Gopakumar, Asmita Pandey, Malu J Paikada, "Adaptive Test Clock Scheme for Low Transition LFSR and External Scan based Testing". International Conference on Computer Communication and Informatics (*ICCCI* -2013), Coimbatore, India, Jan. 09 – 11, 2013.

[5]. S. Gerstendorfer and H.Wunderlich. "Minimized power consumption for scan-based BIST". In Proc. IEEE International Test Conference, pp 77–84, 1999.

[6]. C. Giri, B. Kumar, and S. Chattopadhyay, "Scan flip-flop ordering with delay and power minimization during testing," in Proc. Annu. IEEE INDICON, pp. 467–471, Dec. 2005.

[7]. S. Wang, "A BIST TPG for low power dissipation and high fault coverage," IEEE Trans. Very Large Scale Integrated System (VLSI) , Vol. 15, No. 7, pp. 777–789, Jul. 2007.

[8]. A. Hertwig and H. J. Wunderlich, "Low power serial built-in self-test," in Proc. IEEE Eur. Test Workshop, pp. 49–53,May 1998.

[9]. Amit Kumar Panda*, Praveena Rajput, Bhawna Shukla, "FPGA Implementation of 8, 16 and 32 Bit LFSR with Maximum Length Feedback Polynomial using VHDL" International Conference on Communication Systems and Network Technologies, pp-770-773, 2012.