Contemporary Design of Logic BIST using non Linear S-Box Function as PPRG

Puppala Mounika, Damarla Paradhasaradhi

Abstract**: *Built-In Self-Test is a design for testability (DFT) method used for testing integrated circuits. It provides to test both logic circuits and memory cores in a system. For testing a logic circuit we need test vectors. This paper describes about Pseudo pattern random number generator used in BIST scheme to generate test patterns. In some applications requirement of test patterns will be more in that case a simple LFSR based LBIST is unsatisfactory. In this paper an alternative method is used for the generation of more test patterns. This can be achieved by a non linear function that is Substitution Box in combination with LFSR known as S-box based random number source. This feature empowers it for utilizing in Logic BIST and Memory BIST architecture. Functionality of LFSR, S-box based random number generator and LBIST structures are verified using Xilinx Vivado 18.2 tool.***

Index Terms**: *Logic Built-In Self-Test (LBIST), Memory BIST, Substitution Box, Random Number Generator (RNG).***

I. INTRODUCTION

For any framework, testing plays an important role to distinguish the defects that sink the quality of the system which sometimes leads to failure. With the advancement in sub-micron technology a large number of cores are coordinates on a single chip. Since the input/output pins are limited, testing of external cores becomes a difficult task. To resolve this issue BIST [11][4] schemes are widely used in which circuit analysis in the chip turns into a simple task as the time and cost prerequisites are low. BIST is a technique that allows a machine to test itself which reduces the complexity, subsequently decline the cost and reduce the dependence up on the external test equipment unlike Automatic test equipment (ATE). It has been proposed for many applications in the fields for testing such as medical devices, communication systems, automotive electronics, all types of complex machinery and integrated chips [2][4][7][10][14]. However BIST has the downside of area overhead because of additional circuitry the cost of the chip increases. The important factors to be considered while designing a test setup are time and complexity of testing circuits.

BIST techniques can be characterized in various ways, however two common characterization of BIST are Logic BIST (LBIST) and Memory BIST (MBIST). LBIST which intended for testing random logic, commonly utilizes a pseudo pattern random generator to produce input patterns which are applied to the next block i.e., scan chain and MISR for getting the response to the input test patterns. The MISR output shows the fault in a device. LBIST has its advantages it has the ability to test internal circuits without any association of external pins and also it can trigger an IC while running a individual test of a final product. LBIST can handle the data sizes up to 256 bits, which provides more security it has been using because of its numerous applications such as automotive, defense, aviation, telecom etc. LBIST is mandatory for IC's like ASIC, ASSP and for complex commercial IC's. Whereas MBIST [2] is called as Memory BIST used for testing of memories in the circuits. It typically comprises of test circuits that apply, compare and study the test patterns which exposes the defects in the memory device through a variety of standard algorithms. Another type of BIST technique is ABIST which is used to test the array of memories or for testing analog circuits.

In a conventional BIST architecture consists of a Test controller, pattern generator, UUT and response analyzer as shown in figure 1, TPG, synchronizer [3] and response analyzer are controlled by test controller which controls the test execution. For generating test patterns mostly LFSRs are used which generates random numbers, the generated test patterns are input to UUT which comprises of both combinational and sequential circuits, But using conventional LFSR has cons it produces less number of test patterns. PPRG can be implemented in different ways such as reversible linear feedback shift register [12], cellular automata PPRG [10], CLFSR [2], LTLFSR [13] so in this paper a modified LFSR has been proposed called as S-Box[1][7] number generator which is a combination LFSR and a substitution box is a non linear function used in most of the cryptographic applications because of its high security and capability to generate more number of test patterns. In this work, first designed the LFSR based BIST architecture and compare it with the s-Box based BIST. It is important to note that it increases the test patterns which is used to test the UUT and improves the accuracy.

Manuscript published on 30 April 2019.
***** Correspondence Author (s)

Puppala Mounika, Department of ECE, Koneru Lakshmaiah Educational Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India

Damarla Paradhasaradhi, Department of ECE, Koneru Lakshmaiah Educational Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India

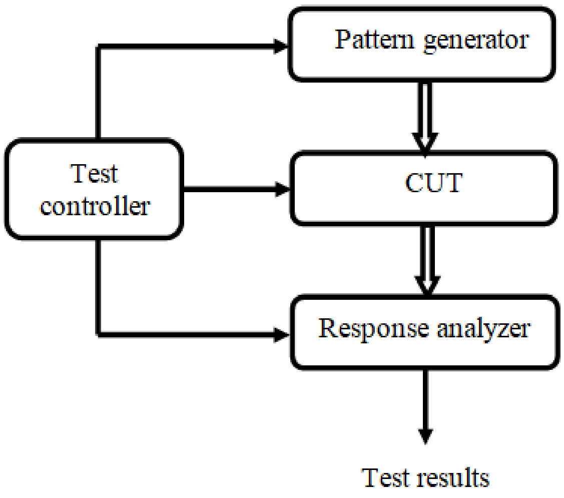

Fig.1: Basic BIST architecture (STUMPS)

The paper is organized as follows: Section II explains the existing LBIST architecture and its functional blocks. Section III, explains proposed S-box based LBIST architecture. In section IV, Simulation results are discussed and section V concludes the paper.

II. EXISTING MODEL

In this section the existing LBIST scheme is considered which exploits the proposed LBIST to generate mode test vectors, an appropriately structured BIST benefits in terms of cost and reliability, the existing LBIST module is shown in below figure. The contentable blocks in conventional design are PPRG, reaction analyzer, test selector synchronizer, space comparator and a phase shifter. In which the logical test can operate in two modes i.e. test mode and typical mode, in typical mode, BIST functions in a normal way it selects a single test pattern which is given independently and continues in a system where as in test mode it allows random test patterns to the scan chain for testing.
The existing scan based LBIST design is shown in figure 2, the test system states with the control signal from controller.

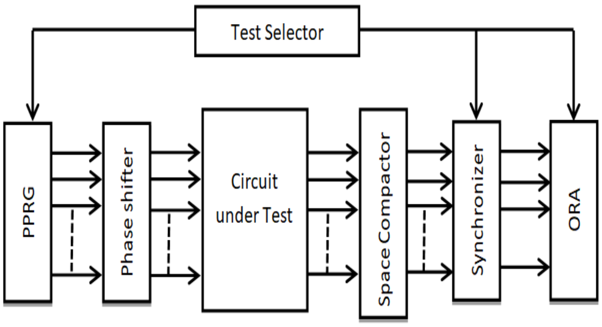

Fig.2: Scan based LBIST architecture

A. Pseudo pattern random generator

In LBIST, to generate test pattern that is used to test the circuit can be done in many ways. Those are stored patterns, exhaustive/complete patterns, pseudo exhaustive patterns, pseudo random generation, pattern generator by counter, cellular automata for pattern generator etc.

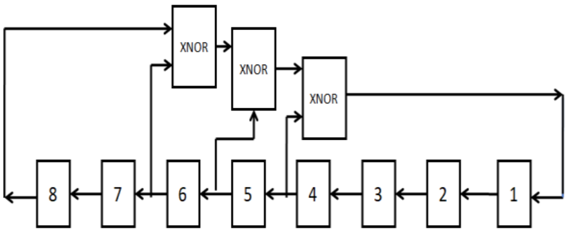

Fig.3: 8-bit LFSR structure

A series of 0's and 1's are repeated in the pattern generated in which mostly LFSR'S are utilized for pseudo random pattern generation sequence. In the conventional method polynomial [15][8] based LFSRS are used as shown in figure 3. The length of test pattern corresponds to the number of flip flops in the scan chain architecture. These can be designed using EX-NOR or EX-OR gates as per designer requirements depending upon the seed value. It loads and generates all the possible test patterns that are generated and are loaded in to the phase shifter, which can be further applied to UUT.

B. Phase shifter

Although BIST has many advantages still suffers from dependency problems. In stumps architecture shown in figure 1, LFSR which generates test patterns, are fed into the scan chain to the UUT, however due to the shift feature of LFSR, the bits of the diagonal lines are identical because of this feature. Some faults become un testable. To solve this problem, a phase shifter is placed in between PPRG and UUT. A phase shifter[16] is a serial to parallel converter which shifts the phase so that each scan chain is shifted by 'S' cycles. It removes the structural dependency problem and is implemented by using simple XOR test parity checker tree. We can also implement phase shifter using clock divided by two circuits.

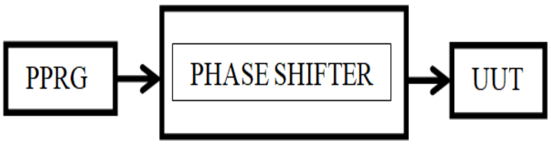

Fig.4: Block diagram of phase shifter

If we consider an N- deque LFSR, T is the positive polynomial; B is the selection vector the phase shift output shifted by S cycles with reference scan chain.Using phaseshifter structural dependency decreases and increases the randomness.

$$\text{Phase shifter} = BT^{S}$$

C. Unit under test

Unit under test mainly consists of both combinational and feedback circuits. In this the circuit that should be tested is considered and the inputs are taken from the phaseshifter.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

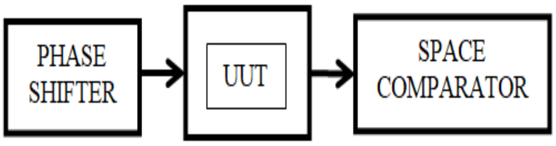

Fig.5: Block diagram of unit under test

D. Space Compactor

Programmability empowers highly powerful space compactors to be intended for the UUT. Depending upon the UUT, the design of space compactor varies. In our design a simple counter is considered as unit under test. So in this a reference counter will be considered.

E. Synchronizer

MISR (multiple input signature register) is used to generate the signature [3]. It receives outputs from the scan chain in response to different test patterns as shown in the figure 6.

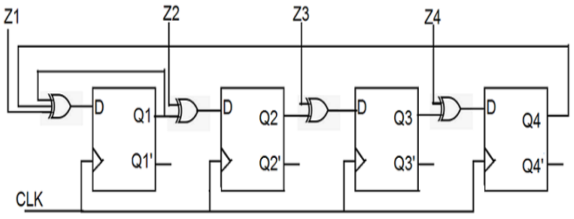

Fig.6: 4-bit Synchronizer

It performs both time and space compaction simultaneously. It is used to compress the multi bit stream so it is also known as parallel signal analyzer. It synchronizes both the signals that are received from unit under test and space comparator.

F. Output response analyzer

Output response analyzer, it analyses the sequence of given inputs and compares the executed test result with the expected output. The expected output is either ‘1’ or ‘0’ depending upon the input and output.

G. Test selector

The controller administrates over all tests executed and manages PPRG, MISR and ORA; there are two working modes for the LBIST. Test mode and a typical mode the BIST testing scheme starts with a control signal depending upon the control signal it could be within test mode or typical mode. It takes the test patterns and tests the LFSR where as in typical mode a specific input is provided. Finally it provides the test result once the test strategies are finished.

III. PROPOSED MODEL

In LBIST scheme pseudo pattern random generator plays a major role in generating test patterns so, selection of PPRG is important. The proposed random number source called as substitution box (S-box) random number generator is shown in figure 7. The proposed PPRG is a combination of 4-bit substitution box with LFSR. These are mostly used in cryptography applications [7], which are used to recognize non linear functions. Implementing these can be done through combinational circuits because of this the LBIST structure have smaller area overhead but the generated test patterns will be more while using s-box than compared with LFSR based PPRG are discussed in section IV. The above specified 4-bit substitution box is in hexadecimal format with inputs A = a_3, a_2, a_1, a_0 and outputs B = b_3, b_2, b_1, b_0. Logical functions for the above table.1 is

0	6	B	5	4	2	E	7	A	9	D	F	C	3	1	0	8

Table-1: 4-bit Substitution Box with input A and output B

$$b_3 = \bar{a}_2 a_3 + a_0 \bar{a}_1 \bar{a}_3 + a_0 a_1 a_2$$
$$b_2 = a_0 \bar{a}_1 a_2 \bar{a}_3 + a_1 \bar{a}_2 + \bar{a}_0 \bar{a}_2 \bar{a}_3 + a_0 \bar{a}_2 a_3 + \bar{a}_0 a_1 \bar{a}_3$$
$$b_1 = \bar{a}_0 a_1 \bar{a}_2 a_3 + \bar{a}_1 \bar{a}_3 + a_0 \bar{a}_1 a_2$$
$$b_0 = a_0 \bar{a}_1 \bar{a}_2 + \bar{a}_0 a_1 \bar{a}_3 + \bar{a}_1 a_3 + \bar{a}_0 \bar{a}_2 a_3$$

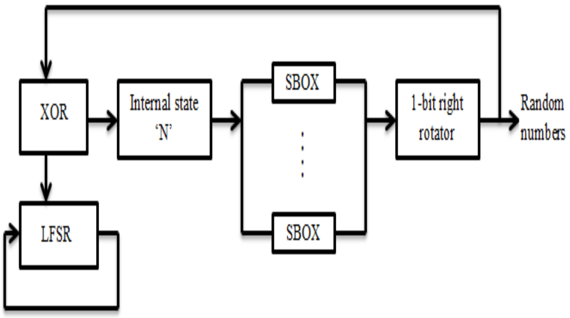

Fig.7: Block Diagram of S-Box RNG

The Substitution box was created in Xilinx vivado software for those above functions. The figure 7 shows the SbRNG has an internal state ‘N’, which must be the multiple of 4 also the length of LFSR should be same as that of ‘N’. The internal state N is XORed with LFSR then N will split into multiple of 4-bits. Then each 4 bit is given to an s-box circuit. finally the obtained result is rotated by 1-bit which gives the random numbers. For next cycle the state is once again XORed with ‘N’.

Designing of these causes a large area overhead but the key advantage of this is it can generate more test patterns than the simple LFSR. Depending upon the application requirement we can choose a simple LFSR or SbRNG as a random number source in LBIST. There are some other random sources such as Algebraic box [7], rand functions, Meressene Twister for generating random numbers.

IV. EXPERIMENTAL RESULTS AND DISCUSSIONS

This section represents the simulated results of the existing and the proposed model. For the synthesis and simulation of the complete LBIST structure, Xilinx Vivado 18.2 tool has been utilized. The designed SbRNG and LFSR are used as PPRG in LBIST scheme. The simulation result for LFSR based random number source is shown in figure 9.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

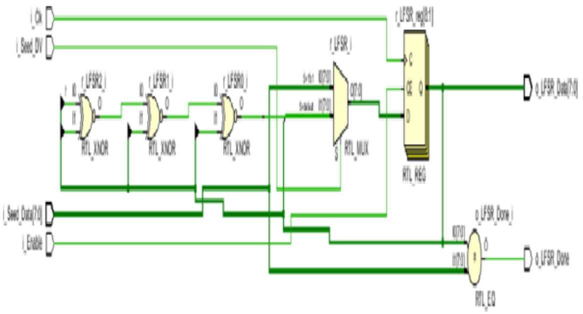

Fig.8: Schematic of 8-bit LFSR

For an 8-bit LFSR, there will be a total of 2^8 = 256 test patterns can be generated and the RTL schematic is shown in figure 8.

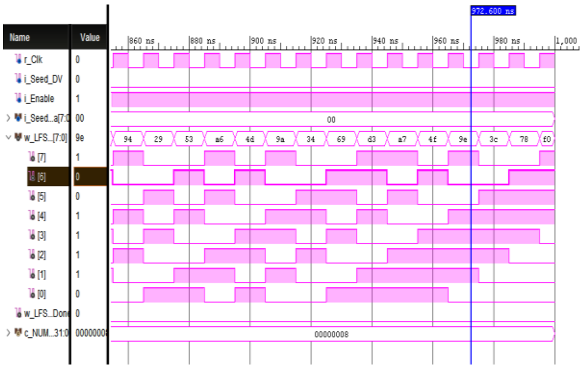

Fig.9: Simulated result of 8-bit LFSR

The rtl schematic for non linear 4-bit S-box is shown in figure 10.

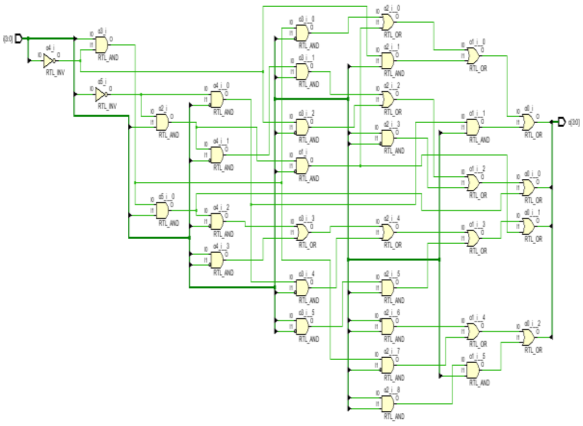

Fig.10: Schematic of 4-bit Substitution Box

Whereas using 8-bit SbRNG it allows the generation of test patterns doubles than the LFSR as shown in figure 11&12.

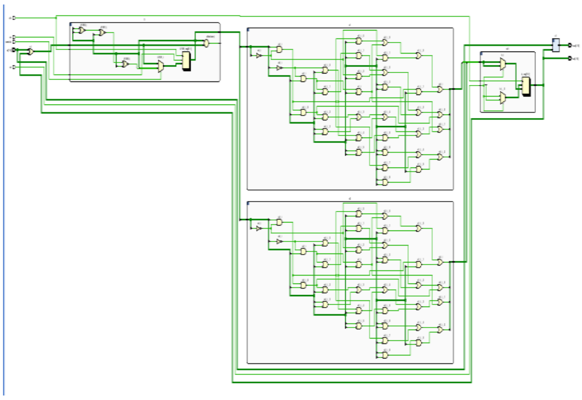

Fig.11: Schematic of S-Box RNG

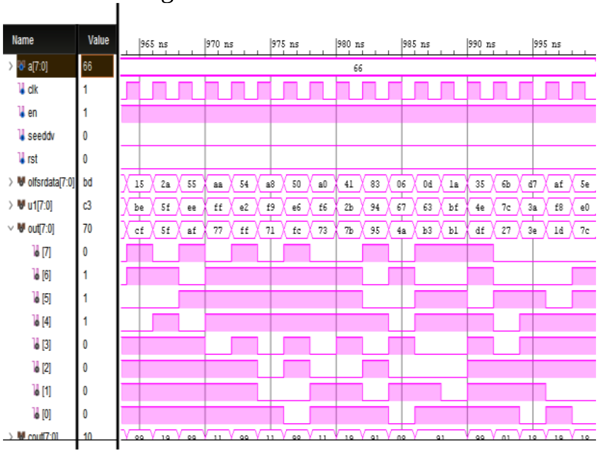

Fig.12: Simulated result of S-Box RNG

Final output results of the existed is shown in figure 13,14, it consists of all the blocks that are discussed in section II.

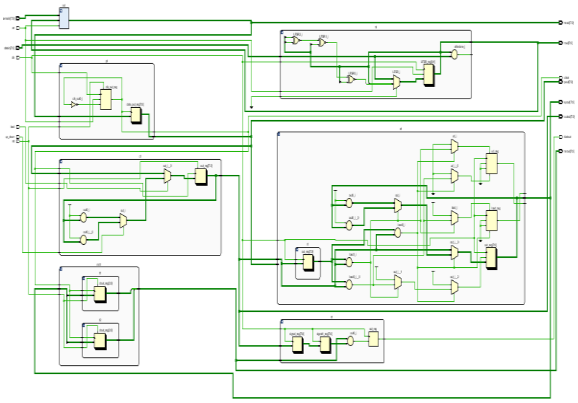

Fig.13: Schematic of LFSR based LBIST

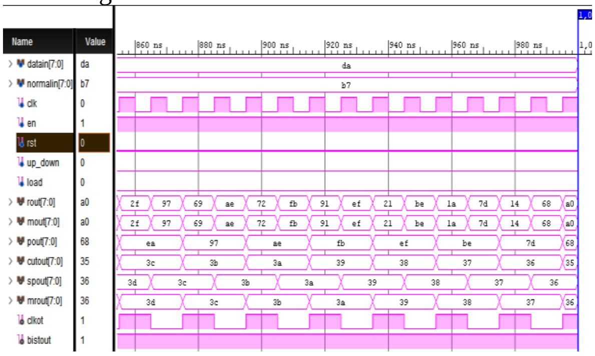

Fig.14: Simulated result of LFSR based LBIST

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

The proposed model is similar to existed model only the LFSR PPRG is replaced by a non linear function i.e.., S-Box because of this the test patterns generated by random source increases. The simulated result and schematic of S-box based LBIST is shown in figure 15,16.

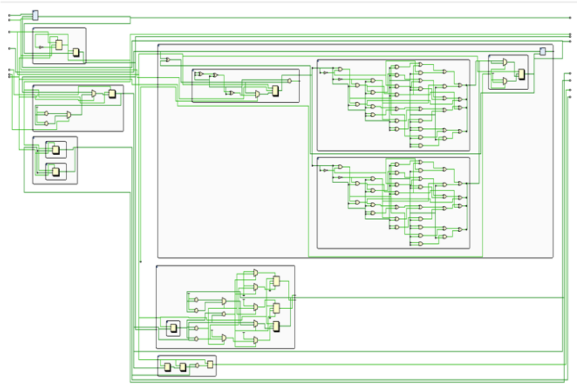

Fig.15: Schematic of Sb-RNG based LBIST

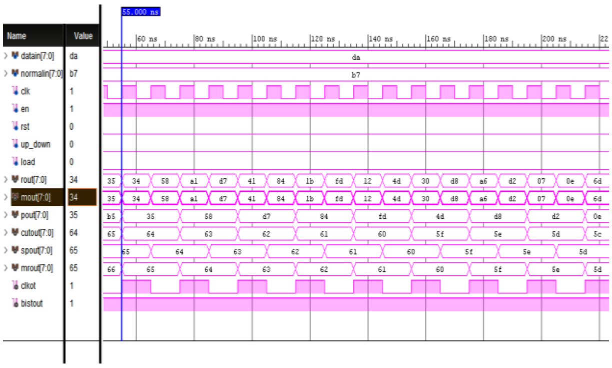

Fig.16 Simulated result of SbRNG based LBIST

The gate count of existing and proposed model is shown in below table 2

Circuit	Look Up tables	Flip flops	Inputs/outputs
LFSR based LBIST	44	58	63
S-Box random number generator based LBIST	50	66	63

Table-2: Gate count comparison between circuits with LFSR based LBIST and S-box RNG based LBIST

From table 2 it is clear that using S-box random number generator based LBIST there will be small area overhead compared to previous method but the key advantage of s-box based LBIST is it increases the test pattern coverage as discussed in section III. The Comparison graph for gate count is shown in figure 17.

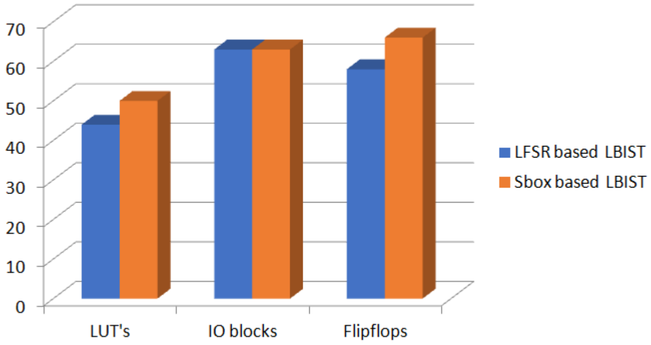

Fig.17: Graphical Representation of Gate Count between LFSR LBIST and S-Box LBIST

The randomness will be more using S-box than compared to lfsr based design but the area approximation will be more for s-box design. For the applications where area is not the first requirement then it's better to choose a non linear s-box based design.

V. CONCLUSION

The proposed substitution box random number source replaces the traditional LFSR in PPRG for LBIST circuits, the random numbers generated by the S-box RNG shows the better test pattern coverage than by the traditional method because of the non linear function used in proposed method. The LBIST UUT is implemented using a simple counter circuit. Finally the results of LFSR based LBIST and S-Box based LBIST are compared. The results are implemented using Xilinx vivado 18.2 tool. The designed s-box mostly suited for the cryptographic applications with smaller area overhead.

REFERENCES

1. Florian Neugebauer, Ilia Polian and John P. Hayes "S-Box-Based RandomNumber Generation for Stochastic Computing," *MICPRO, ELSEVEIR*, 10.1016/j.micpro.2018.06.009, 1-14, 14 june 2018.
2. Preethy K John and Rony Antony P, "BIST Architecture for Multiple RAMs in SoC", 7th International Conference on Advances in Computing & Communications, ICACC, pp 159–165, August 2017.
3. K N Devika and Ramesh Bhakthavatchalu, "Programmable MISR modules for logic BIST based VLSI testing," International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 16-17 December 2016.
4. NPTEL course "Built in self test for Embedded systems," Chapter-40.
5. Dong Xiang, Laung-Terng Wang and Xiaoqing Wen, "Low-Power Scan-Based Built-In Self-Test Based on Weighted Pseudorandom Test Pattern Generation and Reseeding," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 3, pp. 942-953, 19 September 2016.
6. Martin Omana, Daniele Rossi, Filippo Fuzzi, Cecilia Metra, Chandrashekaran Tirupathi and Rajesh Galivanche, "Scalable Approach for Power Droop Reduction During Scan-Based Logic BIST," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 1, pp. 238-246, 14 June 2016.
7. M. Gay, Jan Burchard and Ilia Polian . "Small scale AES toolbox: Algebraic and propositional formulas, circuit-implementations and fault equations," *TRUEDEVICE 2016.*
8. R.C. Ravi shankar Reddy and V. Sumalatha, "Implementation of Area and Power Efficient Built in Self-test Pattern Generator", IEEE WISPNET conference, pp.106-113, 15 September 2016.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

9. Maike Tech and K. Arun, “Design of Low Power Test Pattern Generator for Built In Self Test (BIST) Circuits”, *International Journal of Technical Research and Applications*, Volume 4, pp.210-214, June 2016.
10. M Dalui and Biplab K.Sikdar, “A cellular automata based highly accurate memory test hardware realizing March C^-, *Microelectronics Journal* vol. 52, pp 91- 103, June 2016.
11. https://en.wikipedia.org/wiki/Built-in_self-test.
12. J. Rajski , Jerzy Tyszer, G.Mrugalski and Benoit Nadeau Dosite, “Test generator with preselected toggling for low power built-in self-test,” in Proc. IEEE VLSI Test Symp., pp. 1–6, Apr. 2012.
13. M. Nourani, M. Tehranipoor and Nisar Ahmed, “Low-transition test pattern generation for BIST-based applications,” *IEEE Trans. Comput*., vol. 57, no. 3, pp. 303–315, Mar. 2008.
14. S. Banerjee, D.R. Chowdhury and B.B. Bhatacharya, “A programmable built-in self-test for embedded DRAMs,” IEEE International Workshop on Memory Technology, Design, and Testing, pp. 58-63, 2005.
15. N. Z. Basturkmen, S.M. Reddy and I. Pomeranz, “A low power pseudorandom BIST technique,” in Proc. 8th IEEE Int. On-Line Test. Workshop, pp. 140–144, Jul. 2002.
16. J Rajski and J. Tyszer, “Design of Phase Shifters for BIST Applications,” IEEE VLSI Test Symposium, 30 April 1998.

AUTHORS PROFILE

Puppala Mounika is pursuing M.Tech (VLSI), Department of Electronics and Communication Engineering from Koneru Lakshmaiah Educational Foundation (Deemed to be University), Guntur, Andhra Pradesh, India. Her research interests are CMOS VLSI.

Damarla Paradhasaradhi, currently working as Assistant Professor in Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur. He did M. Tech from Pondicherry University in 2014. He worked as an ASIC Design and Verification Engineer for 2 Years. His research interests are CMOS VLSI, QCA, MEMS.