IJRESM
International Journal of Research in Engineering, Science and Management
Volume-1, Issue-10, October-2018
www.ijresm.com | ISSN (Online): 2581-5792

# A Survey on Secure Weight Based Cell Segmentation Algorithm for Multiple Scan Chains BIST

E. Sankari[1], K. Rama Moorthy[2]
[1]ME Student, Department of Electronics and Communication Engineering, PSNA CET, Dindigul, India
[2]Associate Professor, Department of Electronics and Communication Engineering, PSNA CET, Dindigul, India

***Abstract*—This Paper present a new BIST outline method for-testability and security method that places the testing capacities physically with the circuit under test (CUT) since it experiences difficulty free plan and low cost. Linear Feedback Shift Registers (LFSR) are the most broadly utilized pseudorandom Test Pattern Generators (PRTPG) in Built in Self-Test (BIST) frameworks. The vital processes of scan-based BIST that can shrink switching activity in and also attain maximum fault coverage with reasonable test length .The proposed system depends on secure weighted based cell division for various scan chains utilizing BIST by choosing the best gathering of cell to be associated in a similar output chain with same or extremely shut weight. Which will empowers all output chains all the while and guarantee finish blame inclusion finally the cell was secure sweep by encryption circuit from information spillage. Experimental results on Benchmark IPS circuits and test generator has been coded in Verilog HDL and Simulated using Xilinx.**

***Index Terms*—Built-In Self-Test (BIST), Circuit under Teat (CUT), Encryption, Linear Feedback Shift Register (LFSR)**

## I. Introduction

Advances in VLSI innovation have prompted the manufacture of chips that contain extensive number of transistors. The undertaking of testing such a chip to check amend usefulness is to a great degree complex and frequently extremely tedious. The issue of testing the chips themselves the fuse of these into framework has made the expense of test age develop exponentially. The outline and test improvement

exertion BIST gives an approach to progressively the deteriorate the electronic framework under test so this permits sub congregations to be initially gone through a BIST cycle and if there are no blame at that point sheets in the framework is are gone through a BIST cycle at long last there are no board blames then the whole framework can go through the BIST cycle. Built In Logic Block Observer (BILBO) is a ban of circuit flip tumble with included testing equipment which can be configured to influence the flip flounder to carry on like a sweep chain, Linear Feedback Shift Register (LFSR) design generator. A based reaction minimal or just as D flip flop. Deficiencies might be because of an assortment of elements, including equipment disappointment, programming bugs, administrator mistake and system issues. Sweep chain strategy is an all the more intense procedure since it has high observability and controllability of plan.

Several techniques have been proposed to address this problem. The Test Pattern Generation is flexible to both the test-per-clock and the test-per-scan schemes it has a number of cells to change the test pattern with single input changes (SIC). In multiple cell as multiple SIC that applied to scan chain to reduce the transition state [1]. To compare memory with single cycle of synchronous write and asynchronous read function that values can be read and written within one single cycle. The structure needs less test cycles to reach full coverage and power consumption during tests range. But it is not applicable for multimillion gate designs [2]. In the test pattern generation that insert a random bit in continuous test pattern transition between corresponding bits of pattern pairs. In Bipartite LFSR one half of each continuous insert in test pattern but it has a degradation of delay and performance [3]. During scan shift operation the scan input change from one state to another state. So it takes more switching activity in Circuit under Test. It was reduced by Low Transition Random Test Pattern Generation (LT-RTPG) which is easy to detect faults and another method is 3Weight weighted Random BIST(3W-WRBIST) detect the undetected fault in LT-RTPG [4].The output of one cell feeds input of the second cell directly. It said that the bit swapping is applied to LFSR as an output value thus it combine with 2x1 multiplexer for reduce transitions scan-chain overall switching activity in the circuit under test during test applications [5].

The main thing is to attain a maximum cell test so the low power scan based BIST scheme is applied with weights for the test enable signals Which mean inject a primitive polynomial and extra variables into the linear feedback shift register (LFSR). Such that the one scheme is activated and the one is rest at the time [6]. MISR is generally used in output response but it has ‘n’ bit programmable MISR that could be change into a single signature. that the reconfigurable LFSR can be used as the test pattern generator as well as a response compactor inside Logic BIST to improve the fault coverage of IC testing[7].To scan cell stitching on logic cluster controllability (LoCCo).Flip-Fops which would require more test combinations to test the logic. Place flip flops at the beginning of scan chains while with lower required combinations or lower controllability are positioned toward the end. When ATPG tools generate test patterns for Logic Cluster Controllability (LoCCo) based scan chains, don’t care bits get clustered toward the end of chains, which in turn reduce the shift-in transition count of the Flip-Flops [8].

Scan chain attack is more difficult to implement since hackers must either use the test controller as a test engineer or directly activate the scan chain by probing the scan chain signals directly. Most of present crypto chips include an embedded hardware random number generator used for generating secret keys. This generator can be reused for providing true random numbers to the scrambler block. The three stages are scan partitioning, scan-based X-filling, and statistic-based scan stitching. First one is  reliving the routing overhead Second thing  is executed for making a lot of same bit streams at last  the performed for the reduction of the energy consumption under low routing overhead[9]. To balance trustworthiness and testability a new Design for Security (DFS) methodology is proposed through the modification of scan chain structure. Achieve high security without compromising the testability of the inserted scan structure. To support reshuffling Using an AES core as the testing platform, to elaborate the security assessment and testability of cryptographic circuits [10].

The process based on scan based on test pattern. the user create a one security key then it load for time to stimuli in test vector then the secured key unload form the secret key or in encryption mode [11]. Key Generation module and a Round module are implemented in  Data Encryption Standard (DES) and Advanced Encryption Standard(AES) Signature analysis is Set signal as 0 it load either  plaintext or seed for  generator for first round  then set1 for next rounds[12]. To protect the information from data hacker so it used in both safe and test mode In the safe mode it not directly access so it use security key that key was opened by passing a scan authentication pattern then it reset the then and it access to scan chain In the test mode reconfigurable LFSR is applied to automatic test pattern generation that granted to scan chain these al are occur with the help of PLL [13]. This approach consists in replacing original registers by serial scan registers, and connecting these scan registers into one or several scan chains. Extra control signals allow shifting IN and OUT test data through the scan chain(s), providing full control and observation of the circuit internal states. Scan design greatly reduces the complexity of the test pattern generation and the overall test application time [14]. A new hardware chaos-based pseudorandom number generator which is mainly based on the deletion of a Hamilton cycle the mid-term effects of a slight modification of the seed or of the inputted generator cannot be predicted [15].

In the proposed system an inputs are generate by scan chain thus it pass through to segmentation before going to circuit under test (CUT) an encryption was held. Main thing to attain a maximum fault coverage in a minimum test length. The process is held with the help of Benchmark circuit and it simulated with Xilinx.

## II. Architecture of Built in Self-Test (BIST)

Built in Self-Test (BIST) is the strategy of planning extra equipment and programming highlights into coordinated circuits to enable them to perform self-testing then the testing of their own activity utilizing their own circuits, in this manner lessening reliance on an Automatic Test Equipment. Design for-Testability system since it makes the electrical testing of a chip simpler, quicker, more proficient, and less exorbitant.

BIST are named Logic BIST (LBIST) and Memory BIST (MBIST). LBIST which is intended for testing arbitrary rationale ordinarily utilizes a Pseudo Random Test Pattern Generator (PRPG) or Linear Feedback Shift Register (LFSR) to produce input designs that are connected to the implement interior output chain and a Multiple Input Signature Register (MISR) for getting the reaction of the implement to these test input designs.

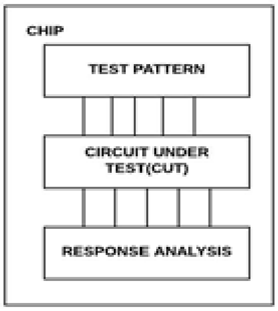

Fig. 1. Basic idea of BIST

An off base MISR yield shows an imperfection in the implementation. The essential BIST engineering requires the expansion of three equipment squares to an advanced circuit: a Test Pattern, Circuit under test and Output reaction.

### A. *Test Pattern Generator (TPG)*

The Test Pattern Generator produces the test designs for the CUT. Precedents of example generators are a ROM with put away examples, a counter, and a Linear Feedback Shift Register (LFSR). A run of the mill reaction analyzer is a comparator with put away reactions or a LFSR utilized as a mark analyzer. BIST Test Pattern Generation Techniques are named stored designs, Exhaustive examples, Pseudo thorough examples, Pseudo-Random Pattern Generation, Weighted Pseudo-arbitrary Pattern Generation, and Cellular Automata (CA) for Pattern Generation.

A LFSR is a move enlist that when timed advances the flag through the enlist starting with one piece then onto the next most-noteworthy piece some of the yields are joined in selective OR design to shape an input component. Execution of an Exclusive-OR door on the yields of at least two of the flip-slumps together and encouraging those yields once more into the contribution of one of the flip-flops.

Direct criticism move registers make to a great degree great pseudorandom design generators. At the point when the yields of the flip-flops are stacked with a seed esteem (anything aside from every one of the 0s which would make the LFSR deliver each of the 0 designs) and at the point when the LFSR is timed, it will produce a pseudorandom example of 0s. The most extreme number of PRPG designs conceivable and has an example check equivalent to 2n – 1 where n is the quantity of enroll components in the LFSR.

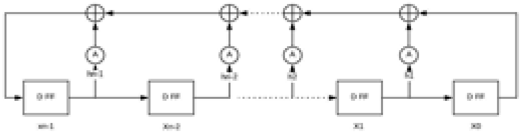

Fig. 2. Linear Feedback Shift Register (LFSR)

### B. *Circuit under Test (CUT)*

Compacts and investigates the test reactions to decide rightness of the CUT. A test control square is important to enact the test and investigate the reactions. Essential contributions to MUX and circuit yield from essential yields can't be tried by BIST. In ordinary activity, the CUT gets its contributions from different modules and plays out the capacity for which it was planned. Amid test mode, a test design generator circuit applies an arrangement of test examples to the CUT and the test reactions are assessed by a yield reaction compactor.

### C. *Output Response Analysis*

In the most widely recognized sort of BIST, test reactions are compacted in yield reaction compactor to shape marks. The reaction marks are contrasted and reference brilliant marks produced or put away On-chip, and the mistake flag shows whether chip is great or broken.

## III. Scan Chains

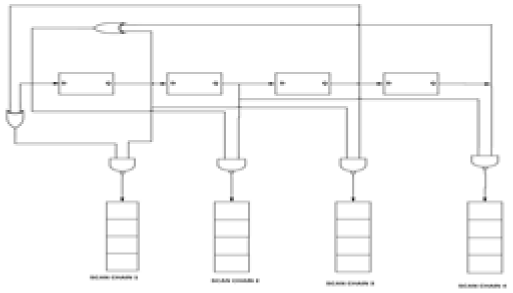

Fig. 3. Multiple scan chain

Scan chain is a technique used in design for testing. The objective is to make testing easier by providing a simple way to set and observe every flip-flop in an Integrated Circuit. Scan in and scan out said as the input and output of a scan chain .A scan enable pin is a special signal that asserted every flip-flop Clock signal for controlling all the Flip Flop during shift phase and the capture phase. One method for loading a seed value is to use registers with reset or set inputs. The LFSR will load with a hard-wired seed value. In certain applications, however, it is desirable to be able to vary the seed value. One technique for achieving this is to include a multiplexer at the input to the LFSR.

## IV. Weighted Based Segmentation

Weighted pseudorandom design BIST is viable for managing hard-to-recognize issues. In a pseudorandom test, each info bit has a likelihood of one portion of being either a 0 or a 1. In a weighted pseudorandom test, the probabilities, or information weights, can vary. The efficient of weighted pseudorandom testing is to inclination the probabilities of the information bits so the tests required for difficult to-recognize deficiencies will probably happen. One methodology utilizes programming that decides a solitary or various weight set dependent on a probabilistic examination of the difficult to distinguish deficiencies.

## V. Encryption

Encryption is the process of transforming data into an unintelligible form. Data that is encrypted is referred to as cipher text. If Data is not encrypted is referred to as plaintext. The data that is encrypted into cipher text is considered secret from everyone.

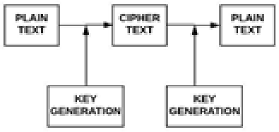

Fig. 4. Basic idea of encryption

There are two basic methods of encryption Symmetric and Asymmetric. Both use a key or keys to encrypt and decrypt information. A key is simply a known piece of external information used in the conversion process.

## VI. Proposed Design

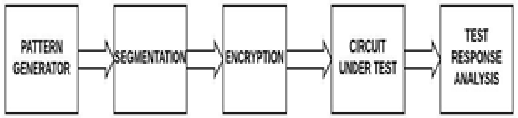

Fig. 5. Block diagram of proposed system

In this paper the proposed system is based on secure based cell division in Built in Self-Test with the technique of weight based segmentation. The important thing is to attain a maximum fault coverage in a minimum test length. The basic idea of BIST is test pattern generator at initial part it flow to circuit under test and then final part is test response. In test pattern, inputs are initially given by seed through Ex-Or by scan chain process. The cell from the Pseudorandom Test Pattern Generation are connected to the same scan chain which will separated into multiple scan chains. After that segmentation part has multiple scan chain with multiple of cell that segment cell based on weight it compare the multiple cell with a fixed weighted value that would match with a weight mean forward to circuit under test via secure system of encryption before the encryption process, cells are mismatch with the weight value. It deny at the present stage. In Encryption the data was secure from data leakage .Finally the cells are reached in safe manner it goes to circuit under test and the test response was attain with the help of Benchmark circuit .

## VII. Math

The work conclude that cell was divide with the help of segment methodology in a Built in Self-Test with secure the data from hacker and also protect from data leakage or data mismatching from other cells. Finally in this section having maximum fault coverage in minimum test length. This paper focus on data security and fault coverage. In future work it may extend for sequential circuit.

## References

[1] Feng Liang, Luwen Zhang, Shaochong Lei, Guohe Zhang, Kaile Gao, and Bin Liang , "Test Patterns Of Multiple SIC Vectors: Theory And Application In BIST Schemes," *IEEE Transactions On Very Large Scale Integration (VLSI) Systems*, Vol. 21, No. 4, April 2013 .

[2] Tobias Strauch," Single Cycle Access Structure for Logic Test ", *IEEE Transactions On Very Large Scale Integration (VLSI) Systems*, Vol. 20, No. 5, May 2012.

[3] Mehrdad Nourani, Mohammad Tehranipoorand Nisar Ahmed ," Low-Transition Test Pattern Generation For BIST-Based Applications*",IEEE Transactions On Computers*, Vol. 57, No. 3, March 2008

[4] Seongmoon Wang," A BIST TPG For Low Power Dissipation And High Fault Coverage*", IEEE Transactions On Very Large Scale Integration (VLSI) Systems*, Vol. 15, No. 7, July 2007.

[5] Abdallatif S. Abu-Issa and Steven F. Quigley," Bit-swapping LFSR and scan-chain ordering: a novel technique for peak- and average-power reduction in scan-based BIST", *IEEE Transactions On Computer-Aided Design Of Integrated Circuits And Systems*, Vol. 28, No. 5, May 2009.

[6] Dong Xiang, Xiaoqing Wen, Laung-Terng Wang," 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* 2016.

[7] Devika K N and Ramesh Bhakthavatchalu," Programmable MISR Modules For Logic BIST Based VLSI Testing", IEEE International Conference on Control, Instrumentation, Communication and Computational Technologies 2016

[8] Shalini Pathak, Anuj Grover, Mausumi Pohit, and Nitin Bansal;" LoCCo-Based Scan Chain Stitching for Low-Power DFT *", IEEE Transactions On Very Large Scale Integration (Vlsi) Systems* 2017

[9] Sungyoul Seo, Keewon Cho, Young-woo Lee, and Sungho Kang," A Statistic-based Scan Chain Reordering for Energy-Quality Scalable Scan Test *", IEEE Journal on Emerging and Selected Topics in Circuits and Systems* 2018.

[10] Yier Jin," Design-For-Security vs. Design-For-Testability: A Case Study on DFT Chain in Cryptographic Circuits", *IEEE Computer Society Annual Symposium on VLSI* 2014.

[11] Darshit Vaghani, Satyadev Ahlawat, Jaynarayan Tudu, Masahiro Fujita†, and Virendra Singh," On Securing Scan Design Through Test Vector Encryption", *IEEE International Symposium On Circuit And System 2018*

[12] Giorgio Di Natale, Marion Doulcier, Marie-Lise Flottes, and Bruno Rouzeyre," Self-Test Techniques for Crypto–Device", *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, Vol. 18, No. 2, February 2010.

[13] Yahia Ouahab, Rashid Rashidzadeh, Roberto Muscedere," A Secure Scan Chain Using A Phase Locking System And A Reconfigurable LFSR", *IEEE 30th Canadian Conference On Electrical And Computer Engineering* 2017

[14] Mathieu Da Silva, Marie-Lise Flottes, Giorgio Di Natale, Bruno Rouzeyre," Preventing Scan Attacks On Secure Circuits Through Scan Chain Encryption *", IEEE Transaction On Computer-Aided Design Of Integrated Circuits And Systems 2018.*

[15] Mohammed Bakiri, Christophe Guyeux, Jean-Franc¸ois Couchot, Luigi Marangio, and Stefano Galatolo," A Hardware and Secure Pseudorandom Generator for Constrained Devices*", IEEE Transaction on Industrial Informatics* 2018.