University of Windsor
Scholarship at UWindsor

Electronic Theses and Dissertations | Theses, Dissertations, and Major Papers

2016

A Hardware Security Solution against Scan-Based Attacks

Ankit Mehta
University of Windsor

Follow this and additional works at: https://scholar.uwindsor.ca/etd

Recommended Citation

Mehta, Ankit, "A Hardware Security Solution against Scan-Based Attacks" (2016). *Electronic Theses and Dissertations*. 8002.
https://scholar.uwindsor.ca/etd/8002

This online database contains the full-text of PhD dissertations and Masters' theses of University of Windsor students from 1954 forward. These documents are made available for personal study and research purposes only, in accordance with the Canadian Copyright Act and the Creative Commons license—CC BY-NC-ND (Attribution, Non-Commercial, No Derivative Works). Under this license, works must always be attributed to the copyright holder (original author), cannot be used for any commercial purposes, and may not be altered. Any other use would require the permission of the copyright holder. Students may inquire about withdrawing their dissertation and/or thesis from this database. For additional inquiries, please contact the repository administrator via email (scholarship@uwindsor.ca) or by telephone at 519-253-3000ext. 3208.

A Hardware Security Solution against Scan-Based Attacks

By

Ankit Mehta

A Thesis

Submitted to the Faculty of Graduate Studies
through the Department of **Electrical and Computer Engineering**
in Partial Fulfillment of the Requirements for
the Degree of **Master of Applied Science**
at the University of Windsor

Windsor, Ontario, Canada

2016

© 2016 Ankit Mehta

ProQuest Number: 10182906

All rights reserved

INFORMATION TO ALL USERS
The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript
and there are missing pages, these will be noted. Also, if material had to be removed,
a note will indicate the deletion.

ProQuest 10182906

Published by ProQuest LLC (2016). Copyright of the Dissertation is held by the Author.

All rights reserved.
This work is protected against unauthorized copying under Title 17, United States Code
Microform Edition © ProQuest LLC.

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346

A Hardware Security Solution against Scan-Based Attacks

by

Ankit Mehta

APPROVED BY:

_____

Dr. Ahmed Azab
Mechanical, Automotive & Materials Engineering

_____

Dr. Huapeng Wu
Electrical and Computer Engineering

_____

Dr. Rashid Rashidzadeh, Supervisor
Electrical and Computer Engineering

_____

Dr. Majid Ahmadi, Supervisor
Electrical and Computer Engineering

September 19, 2016

DECLARATION OF CO-AUTHORSHIP/PREVIOUS PUBLICATION

I. Co-Authorship Declaration

I hereby certify that this thesis incorporates the outcome of joint research in collaboration with, and under the esteemed supervision of Dr. Rashid Rashidzadeh and Dr. Majid Ahmadi.

I am aware of the University of Windsor Senate Policy on Authorship and I certify that I have properly acknowledged the contribution of other researchers to my thesis, and have obtained written permission from each co-author(s) to include the above material(s) in my thesis. I certify that, with the above qualification, this thesis, and the research to which it refers is the product of my own original work.

II. Declaration of Previous Publication

This thesis includes 3 original papers that have been previously published /submitted for publication in peer reviewed journals as follows:

Thesis Chapter	Publication Title/ full citation	Publication Status
All Chapters	Title: " A Hardware Security Solution against Scan based attacks", 2016, IEEE Int'l Symposium on Circuits and Systems	Accepted
All Chapters	Title: " A Secure Test solution for Sensor Nodes containing crypto cores"	Submitted

All Chapters	Title: "A hardware secure solution for scan enabled circuits using access control"	Submitted

I certify that, to the best of my knowledge, my thesis does not infringe upon anyone's copyright, nor violate any proprietary rights. Any ideas, techniques, quotations, and material appertaining to other people included in my thesis, published or otherwise, are fully acknowledged in accordance with standard referencing practices. Furthermore, to the extent that I have included copyrighted material that surpasses the bounds of fair dealing within the meaning of the Canada Copyright Act, I certify that I have obtained a written permission from the copyright owner(s) to include such material(s) in my thesis and have included copies of such copyright clearances in my appendix.

I certify that I have obtained written permission from the copyright owner(s) to include the above published materials in my thesis. I certify that the above material describes work completed during my registration as graduate student at the University of Windsor.

I declare that this is a true copy of my thesis, including any final revisions, as approved by my thesis committee and the Graduate Studies office, and that this thesis has not been submitted for a higher degree to any other University or Institution.

ABSTRACT

Scan based Design for Test (DfT) schemes have been widely used to achieve high fault coverage for integrated circuits. The scan technique provides full access to the internal nodes of the device-under-test to control them or observe their response to input test vectors. While such comprehensive access is highly desirable for testing, it is not acceptable for secure chips as it is subject to exploitation by various attacks. In this work, new methods are presented to protect the security of critical information against scan-based attacks. In the proposed methods, access to the circuit containing secret information via the scan chain has been severely limited in order to reduce the risk of a security breach. To ensure the testability of the circuit, a built-in self-test which utilizes an LFSR as the test pattern generator (TPG) is proposed. The proposed schemes can be used as a countermeasure against side channel attacks with a low area overhead as compared to the existing solutions in literature.

DEDICATION

I would like to dedicate this thesis to my family my late grandfather Ainshi Lal Mehta and late grandmother Lajwanti Mehta. Your blessings and the values you taught me made this possible. I miss you a lot and still remember the good old days. In addition to this, I would like to dedicate my work to my parents and my cousin brother. Special thanks to my parents, Mr. Sanjay Mehta and Mrs. Sonia Mehta, for always supporting me to pursue my master's degree and my loving, sweet younger sister, Manya Mehta, who is very good and her constant motivation helped me to achieve my master's degree. No matter how far I go in my life, this would not have been possible without all of you.

I would also like to thank my cousin brother, Dr. Bhuvanender Vashist (Sonu Bhaiya), for always motivating me to continue my studies and making me realize the importance of a degree from abroad. This would never have been possible had you not given me your emotional support. You have always stood as my shield against all problems I have faced and provided the best and the right guidance. I thank God for having you in my life and will love you forever. Last but not the least, I would like to thank God for the person that I am today and making this master's degree possible.

ACKNOWLEDGEMENTS

I would like to thank my supervisor, Dr. Rashid Rashidzadeh, and advisor, Dr. Majid Ahmadi, their unbounded support, motivation, constructive comments, and motivation throughout my master's degree helped address even the most basic of questions. Without their support, I could not have completed this degree. The constructive feedback which they provided helped polish my work. I would also like to thank my other committee members, Dr. Ahmed Azab and Dr. Huapeng Wu, for all their comments and valuable suggestions for the improvement of this work.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

Abbreviations/Symbols	Description
IC	Integrated Circuit
SSI	Small Scale Integration
MSI	Medium Scale Integration
LSI	Large Scale Integration
VLSI	Very Large Scale Integration
DfT	Design for Test
SoC	System on Chip
ATE	Automatic Test Equipment
DC	Direct Current
AC	Alternating Current
ppm	Parts per million
BIST	Built-in self-test
TPG	Test Pattern Generator
CUT	Circuit Under Test

Abbreviation/Symbol	Description
LFSR	Linear Feedback Shift Register
GF	Galois Field
EPG	Exhaustive Pattern Generator
CFSR	Complete LFSR
PRPG	Pseudo Random Pattern Generator
RP	Pattern Resistant
CRC	Cyclic Redundancy Check
SISR	Single Input shift register
MISR	Multiple input shift register
JTAG	Joint Test Action Group
IPs	Intellectual Property
TAPC	Test Access Port Controller
TAP	Test Access Port

Abbreviations/Symbols	Description
TDI	Test Data Input
TDO	Test Data Output
TMS	Test Mode Select
TCK	Test Clock
TRST	Test Reset
IR	Instruction Register
BSC	Boundary Scan Cell
TAM	Test Access Mechanism
CTL	Core Test Language
WSP	Wrapper Serial Port
WSI	Wrapper serial Input
WSO	Wrapper Serial Output
WSC	Wrapper serial control

Abbreviations/Symbols	Description
WIR	Wrapper Instruction Register
WPC	Wrapper Parallel control
WPI	Wrapper Port Input
WPO	Wrapper Port output
WPP	Wrapper Parallel port
WBY	Wrapper Bypass Register
WBR	Wrapper Boundary Register
CFI	Cell Functional input
CFO	Cell Functional Output
CTI	Cell Test Input
CTO	Cell Test output
RC4	Riveset Cipher 4
PUF	Physically Unclonable Function

Chapter 1

Introduction and Background

1.1 Motivation and Problem Statement

The need to increase the processing power and speed of processors, on the other hand reducing the price and power consumption of processors has led to decrease in the feature size of the transistors, This, in turn, has directly affected the operating clock frequency of microprocessors. For example, the operating frequency of current microprocessors is in the gigahertz range as compared to a few 100 KHz in the 1970s. The reductions in feature sizes and the increased number of transistors per chip raises the probability that an IC may have manufacturing or functional defects. With feature sizes at the nanometer scale, it is not unusual that some of the transistors in the microchip may not work properly, and thus, causing the entire chip to malfunction [1].

Defects created at the manufacturing stage are unavoidable even if the utmost care is taken in state of the art fabrication facilities. A popular rule of ten, which is followed in industry which states that the cost of testing goes up as we move from wafer to chip and from chip to board level and before it can be adopted for the system level use as shown in figure 1. Due to impossibility of infallible design and fabrication processes involved, it is imperative to screen out faulty ICs and defective parts so as to prevent the shipping of defective parts to customers. Testing techniques have been developed without considering the fact that the circuit added to increase testability can also be used to access security sensitive information. Many systems have been attacked using the test interfaces currently available.

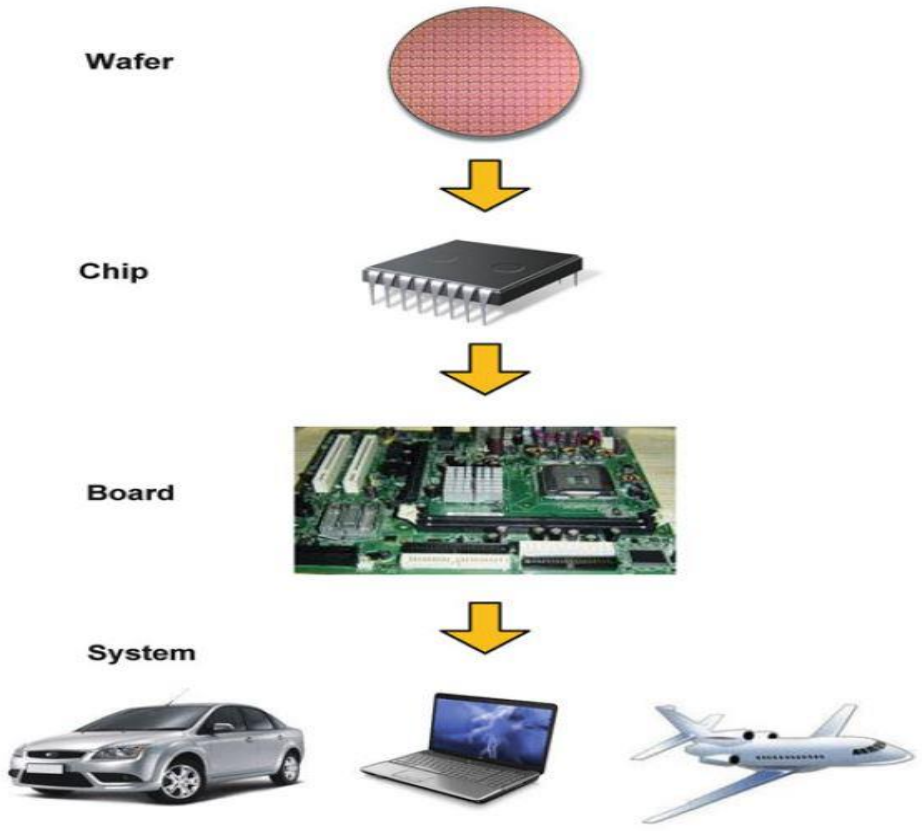


Figure 1: Various stages of Testing [90]

In this thesis, we have proposed a secure design for test techniques to counter the scan based attacks.

1. In the first technique, two modes for testing have been proposed, namely, the secure mode of testing and the insecure mode of testing. A controller is designed to control the transition from the secure mode to the insecure mode of testing and vice versa.
2. In the second technique, a secure self-test technique has been proposed keeping in view the various stages of testing once the integrated circuit has been launched to the market.

1.2 Testing of Digital Circuits

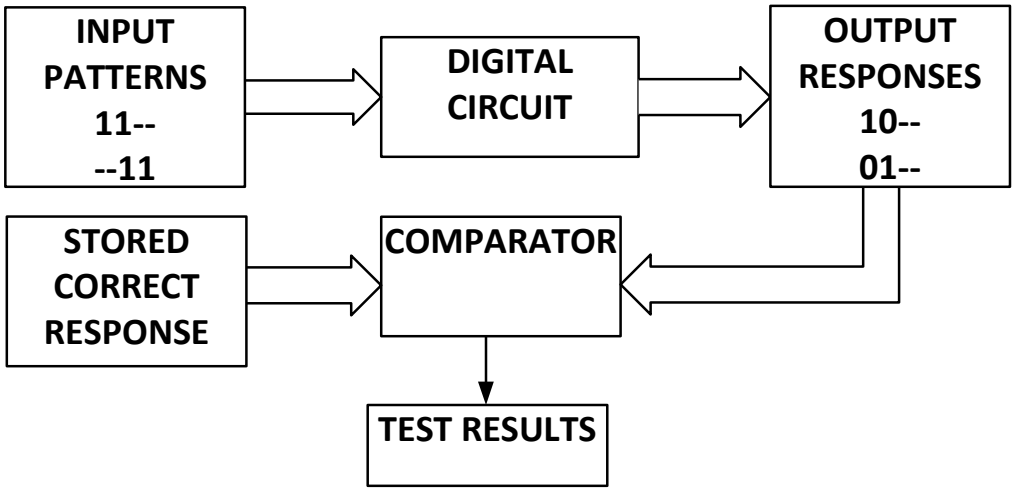


Figure 2: Flow for testing of Digital Circuits

Figure 2 shows the flow of testing for the digital circuits. For a given device under test, the binary test patterns are applied as the input to the circuit. The respective output responses are then obtained. These output responses are then compared with the correct stored responses in a response analyzer. If the responses match, then the circuit is considered to be acceptable, else the circuit is faulty. Most of the input test vectors are applied by an apparatus called ATE (Automatic Test Equipment) [2].The test responses are written and stored in the memory of the test equipment.

1.3 VLSI Testing Challenges

The manufacturing of VLSI devices is a complex and cumbersome process. Figure 3 shows the image of a manufactured IC in which the channel length is 120 nm and there are six levels of interconnections and wirings. There are many stages in the IC manufacturing process. In this particular process, some random manufacturing imperfections can cause variations in the process,

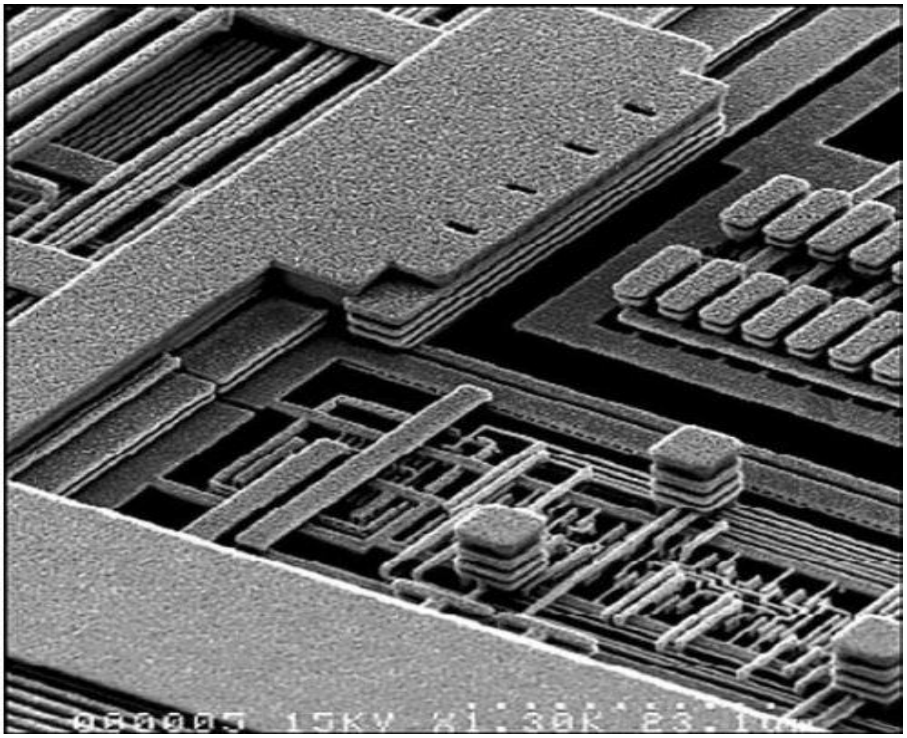


Figure 3: CMOS chip by IBM incorporating 6 levels of interconnections [7]

voltage and temperature in the final manufactured IC. Variations affecting transistor channel length, the metal interconnect width and thickness, and dielectric thickness can be grouped under process variations [11-13].

1.4 Types of Testing

Testing methodology changes depending on the production stage at which an IC being tested. In the initial stage of production, for instance, after the wafers have been manufactured, *wafer sort testing* is performed. The motive to test at this stage is to sort out the faulty wafers [3, 4]. The remaining wafers which are deemed to be satisfactory are then processed to the next stage for packaging. While the sorting of wafers is performed, the *characterization test* is also conducted. Broadly, the test can be classified as follows:

1. *Functional Tests*: In these type of tests, the input test vectors are applied and then the responses are compared. The motive is to check the correct functionality of the device under test. Many manufacturing faults (stuck at faults) are covered by this technique of testing.
2. *Parametric Tests*: This type of testing can be categorized as a DC parametric test and an AC parametric test. The former consists of an open test, a short test, a leakage test and a threshold test whereas the latter entails refresh and pause time tests, rise and fall time tests, a speed test, and setup and hold tests. The test standards which have been designed do not depend upon the technology node being tested and hence, are independent of the technology being tested.
3. *Structural Tests*: In this approach, the circuit under test is mainly tested by fault models based on the knowledge of the structural information of the device under test. Adopting structural testing can save time and increase the test efficiency significantly. Any specific fault model adopted in the structural testing does not guarantee the detection of all the possible faults in the circuits but can be quantified by the term fault coverage.

At this point, it is important to highlight the notable differences involved in the testing of ICs and memory. The test methodology for memories fall in the paradigm of *functional* testing, which is designed to cover attributes such as address decoder speed, cell coupling, data sensitivity, write operation, and address uniqueness. To achieve extensive fault coverage, it demands long test vector sequences.

Chip level testing and board level testing have many differences. In board level testing, the components are previously tested and embedded. One of the aims in board level testing is to check the contacts and wires used in the routing [5-6].

1.5 Test Dynamics and Fault models

A ***fault*** in a manufactured IC can be defined as a defect which results due to a physical condition which prevents the circuit from performing in the desired manner. A ***Failure*** can be termed as a deviation from the expected performance of an IC; it expresses a need for repair so as to obtain the intended device output. A ***circuit error*** can be defined as the wrong output signal from the defective circuit. Fault models are used to generate and compare the test vectors for the device under test. When modeling a fault model, it is important to consider the following points:

1. The fault model should be efficient in terms of the number of test patterns and test vector generation.
2. The fault model must be capable of predicting the behavior of the circuit under test.

The fault model can be divided into two categories, namely, the single fault model and the multiple fault model. The single fault model can be described as

$$\text{Number of single faults} = k \times n \tag{1}$$

where k signifies the type of faults and n signifies the possible fault sites which can be present in the digital circuit. However, in the practical scenario, there are commonly multiple faults in the device-under-test and is given by

$$\text{Number of multiple faults}=(k+1)^n - 1 \tag{2}$$

As shown in the equation 2 the circuit can have the k possible faults. The "-1" term represents the fault free circuit. In the single fault model two or more faults can result in the same faulty behaviors for all the patterns .However, these faults can be termed as ***equivalent faults***. Under this assumption the total number of vectors to be actually considered for the given circuit are much less than $k \times n$. This reduction in which the redundant faults are removed by the overlapping test

vectors is termed as ***fault-collapsing.*** By following the fault collapsing algorithms, fault simulation times and the test time for circuits with large value of n are reduced [8-10].

1.6 Hardware Attacks and Problem Statement

Over many years, test interfaces have been built to test digital circuits. It was not known that the interfaces for testing could pose a security threat to the device under test. Many systems have been attacked using the controllability and observability provided by the advanced test techniques developed over past decades. To some level, the designer can prevent the system from being hacked by these DfT techniques and thus, can eventually reduce the system exploitation by applying various defenses. There is a strong need for the protection of crypto chips and the prevention of misuse of intellectual property without the inventor's knowledge. This thesis focuses upon the protection of hardware from scan based attacks and three solutions have been proposed for different scenarios of testing.

1.7 Thesis Contribution

The contributions of this thesis can be summarized as follows:

- novel secure design for test techniques have been proposed for digital circuits;
- the area overhead for the proposed secure test techniques are negligible ; and
- the proposed secure techniques do not compromise the fault coverage which many existing techniques do.

1.8 Thesis Organization

The thesis contains a total of 7 chapters. In chapter 1, the introduction motivation and testing challenges is discussed and hardware security is discussed. In Chapter 2 various test techniques are discussed. Chapter 3 discusses about IEEE 1149.1 and P1500 standard. In chapters 4 to 6 secure hardware methods are discussed. Chapter7 concludes with the summary, conclusion and future work.

Chapter 2

Testing of VLSI Circuits and Design for Testability

2.1 Introduction

Design for test techniques are used in integrated circuits to make the design testable while reducing the cost of testing. To physically realize the design for test techniques, extra hardware is usually required; this extra hardware is realized in the form of logic gates which are directly connected to the internal logic or the core logic to be tested. The advantages of using the DfT techniques include:

(a) increased fault coverage; (b) making the circuit easier to control and observe; (c) reduced testing time; and (d) supporting the hierarchical testing for logic.

The product quality of integrated circuits is quantified by various terms such as **Defect**, **Yield** and **Defect Level**. A defect can be defined as a fabrication problem caused by the manufacturing process. The defect on the wafer can be caused by process variation the impurities in wafer material and chemicals, dust particles in the projection system, or mask misalignment. Yield is defined as the fraction or the percentage of good chips produced in the system out of the total chips produced in a batch of manufacturing chips. Defect level is the metric which is used to characterize the effectiveness of the test type and the manufactured product quality achieved. It is the ratio of the faulty chips to the chips which have passed the tests. The unit used to measure the defect level is ***parts per million (ppm)***.

2.2 Built in Self-Test

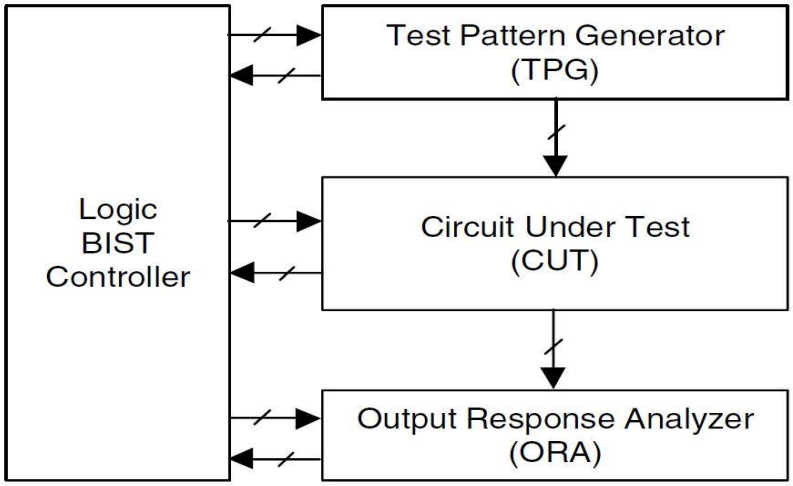


Figure 4: Flow demonstrating BIST Testing [10]

Figure 4 shows a typical setup for built in self-test (BIST), which consists of a test pattern generator (TPG) for generating the test patterns, circuit under test (CUT) which needs to be tested, and a response analyzer which analyzes the response obtained from the circuit under test and compares it with the golden signature. For controlling all the operations of BIST, there is a BIST controller which is responsible for switching between the various states. Using BIST is advantageous as; it eliminates the need for the external tester, supports at speed testing which helps to detect delay faults, and it also helps to reduce test time and tester memory requirements. One of the problems associated with built-in self-test as a method of testing is that the BIST should be able to deal with the unknown values X [8-9].

2.3 Test Pattern Generation

The most commonly used test pattern generators for BIST applications are linear feedback shift registers (LFSRs) which are also used for exhaustive testing, pseudo exhaustive testing, and pseudo random testing. To achieve full fault coverage and have the multiple stuck at fault

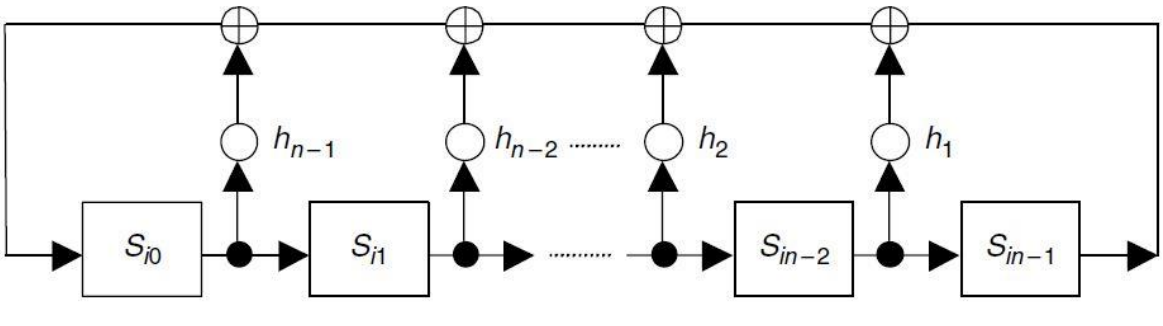


Figure 5: The n-stage conventional LFSR [10]

coverage, exhaustive testing is used. The various possible configurations of LFSR are discussed in the proceeding sections. [15].

2.3.1 Standard LFSR

Figure 5 shows the configuration of the conventional LFSR. It is made up of n D-flip flops and exclusive-OR (XOR) gates. When the XOR gates are placed on the external feedback path, it is called **external-XOR** LFSR [14].

2.3.2 Modular LFSR

Figure 6 shows the modular type n stage internal feedback type LFSR with the feedback connections in the internal type. The speed of the modular LFSR is faster as compared to the conventional LFSR. This is due to the fact that in the conventional type configuration, each XOR gate introduces a gate delay [14].

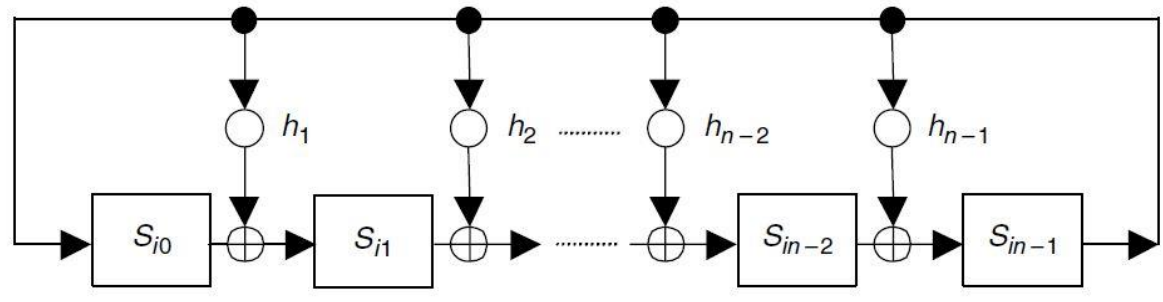
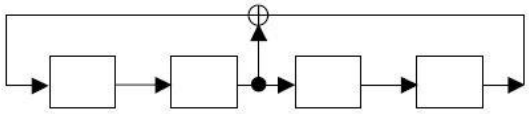
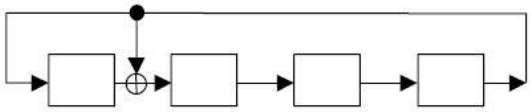


Figure 6: The n stage modular LFSR [10]

2.4 LFSR Characteristics



(a)



(b)

(a)	(b)
0 0 0 1	**0 0 0 1**
1 0 0 0	1 1 0 0
0 1 0 0	0 1 1 0
1 0 1 0	0 0 1 1
0 1 0 1	1 1 0 1
0 0 1 0	1 0 1 0
0 0 0 1	0 1 0 1
1 0 0 0	1 1 1 0
0 1 0 0	0 1 1 1
1 0 1 0	1 1 1 1
0 1 0 1	1 0 1 1
0 0 1 0	1 0 0 1
0 0 0 1	1 0 0 0
1 0 0 0	0 1 0 0
0 1 0 0	0 0 1 0
1 0 1 0	**0 0 0 1**

Figure 7: Test pattern generated by different LFSR [10]

Figure 7 shows the difference in the sequence of the test patterns which is generated by the different types of LFSR as discussed above; it is assumed that the initial contents of both types of LFSR are set to {0001}. It is clear from the figure that for the type "a" LFSR, the sequence repeats after 6 cycles whereas for the type "b" LFSR, the sequence repeats after 10 clock cycles [16]. The polynomials which describe the above sequences can be described by $1+x^2+x^4$ and $1+x+x^4$, respectively. Many solutions exploiting the use of LFSR have been proposed using the advanced design for test techniques such as broadcast scan method, variable linear decompressors, and Illinois scan architecture [10].

2.5 Mathematical Modelling of LFSRs

The various possible forms of LFSRs are shown in Figure 5 and Figure 6;each has S_n flip flops, n feedback paths, and is defined by the feedback coefficient h_n. The feedback coefficient defines whether the feedback path is active or not.

- If $h_i = 1$, the feedback path is closed or active.
- If $h_i = 0$, the feedback path is open or inactive ,

The value of the output of the flip-flop is multiplied by its coefficient p_i; the result of the multiplication depends upon whether the value of h_i is 1 or 0.To begin, we can assume that the initial value stored in the flip flops is s_{i0}, s_{i1},…..s_{in-1} and the feedback connections can be defined as h_1, h_2,…… h_{n-1}.The output can be defined as s_m.

$$s_m \equiv s_{i0}h_{n-1} + \cdots + s_{i-2}h_2 + s_{i-1}h_0 \; mod \; 2$$

Following this, the next stage of the LFSR is defined as

$$s_{m+1} \equiv s_{i1}h_{n-1} + \cdots + s_{i-1}h_2 + s_i h_0 \; mod \; 2$$

The general equation expressing the output of the LFSR can be defined as follows

$$s_{i+m} \equiv \sum_{j=0}^{m-1} s_i \cdot h_{i+j} \; mod \; 2 \quad ; s_i \; , h_j \in \{0,1\} \; , i = 0,1,2\ldots \tag{3}$$

2.5.1 Attacks against the LFSR

The inputs and the outputs from the LFSR are governed by a linear relationship. The advantage of this linear relationship is used in communication systems. On the other hand, as a cryptosystem, this opens opportunities for attackers. In this section, the linear relationship of the LFSR is studied and possible attacks are also discussed. To attack an LFSR, it is assumed that the position of feedback switches is the secret key of the system (h_{m-1},…., h1, h_0). It is also assumed that the

attacker knows some bits of the plaintext and the cipher-text, as well as the knowledge of the degree of the polynomial form the periodicity of the LFSR polynomial. The bits of the plaintext can be described as p_0, p_1….. p_{2m-1} and the cipher-text bits can be written as c_0, c_1,…..c_{2m-1}.With the known cipher-text and plain-text bits, the attacker can construct the 2m bits

$$s_i = p_i + c_i \; mod \; 2; \quad i = 0,1,2 \ldots .2m - 1 \tag{4}$$

To attack the LFSR, it is imperative to know the feedback coefficients h_i and the stream of the input bits as defined by Equation 3.With the above knowledge, the attacker can generate the "m" equations for "m" values with different values of "i" as shown by the set of equations below.

$$\begin{aligned} i = 0, \quad & s_m \equiv s_{i0}h_{n-1} + \cdots + s_{i-2}h_2 + s_{i-1}h_0 \quad mod\ 2 \\ i = 1, \quad & s_{m+1} \equiv s_{i1}h_{n-1} + \cdots + s_{i-1}h_2 + s_i h_0 \quad mod\ 2 \\ & \vdots \qquad\qquad \vdots \qquad\qquad \vdots \\ & \vdots \qquad\qquad \vdots \qquad\qquad \vdots \end{aligned}$$

$$i = m - 1, \quad s_{2m-1} \equiv s_{i0}h_{n-1} + \cdots + s_{i-2}h_2 + s_{i-1}h_0 \quad mod\ 2$$

Thus by solving above linear equations with "m" unknowns the attacker can easily find out the feedback coefficients h_0, h_1,……, h_{m-1} by applying matrix inversion technique and Gaussian elimination algorithm, once the feedback coefficients are found the attacker can build the LFSR and obtain the output sequence

2.6 Cyclic LFSRs

To reduce the length of the test data, cyclic LFSRs can also be used for test generation. For cyclic LFSR, first, the (n, k) have to be defined for n-stage LFSR, and with periodicity of 2^k-1. The cyclic

LFSRs are generated from the cyclic codes over the GF (2) which contains the 2^k different code-words and the n-bit tuple is realized by rotating the code-word bits to the right. The minimum code-word or weight of cyclic LFSR is defined by "*d*" in cyclic LFSR [17-18].

n'	k'	d	$g(x)$
7	4	3	$1+x+x^3$
7	3	4	$(1+x)(1+x+x^3)$
7	1	6	$(1+x^7)/(1+x)$
15	11	3	$1+x+x^4$
15	10	4	$(1+x)(1+x+x^4)$
15	7	5	$(1+x+x^4)(1+x+x^2+x^3+x^4)$
15	6	6	$(1+x)(1+x+x^4)(1+x+x^2+x^3+x^4)$
15	5	7	$(1+x+x^4)(1+x+x^2+x^3+x^4)(1+x+x^2)$
15	4	8	$(1+x)(1+x+x^4)(1+x+x^2+x^3+x^4)(1+x+x^2)$
15	2	10	$(1+x)(1+x+x^4)(1+x+x^2+x^3+x^4)(1+x^3+x^4)$
15	1	14	$(1+x^{15})/(1+x)$

Table 1: Table showing the generator polynomial for cyclic LFSR [10]

To generate the test patterns from the cyclic LFSR, the following steps have to be followed [18]:

1. The generator polynomial *g(x)* has to be of greatest degree k' (or the smallest degree k) for generating (n', k')=(n', n'-k) cyclic code that divides the $1+x^n$ and has the distance (design) of $d \geq w+1$ [10]; and
2. The equation h(x) = $(1+x^n)/g(x)$ can be used to generate the (n', k) cyclic code which is the dual code of (n', n'-k) and is generated from *g(x)*.To construct the (n', k) cyclic LFSR, the following equation can be used:

$$f(x) = h(x)p(x) = \frac{(1+x^n)p(x)}{g(x)}$$

where *h(x)* is the parity check polynomial of *g(x)* which satisfies the equation $g(x)*h(x) = 1+x^{n'}$.

Shortening of the equation (n', k) cyclic LFSR to (n, k) cyclic LFSR can be achieved by deleting the rightmost, middle or the leftmost $n'-n$ stages from the (n', k) cyclic LFSR which also yields the lowest area overhead [19].

2.7 Exhaustive Testing

In exhaustive testing, the total number of 2^n test patterns are applied to the circuit under test. Generally, exhaustive testing is not preferred for combinational circuits with a large number of inputs "n" as it takes a long time to cover all the states. A binary counter can even be used as the exhaustive pattern generator (EPG), but the maximal length LFSRs are more efficient as compared to the binary counters; hence, they are generally used to cover all the 2^n-1 states. A right seeding is necessary for the LFSR to generate the right test patterns [20]. A right seeding is necessary to cover all the zero states in the test patterns of LFSR. The LFSR containing these zero states is called the complete LFSR (CFSRs) [21]. The techniques which can be used as the pattern generator satisfying the criteria of exhaustive testing are discussed in the proceeding sections.

2.7.1 Complete LFSR

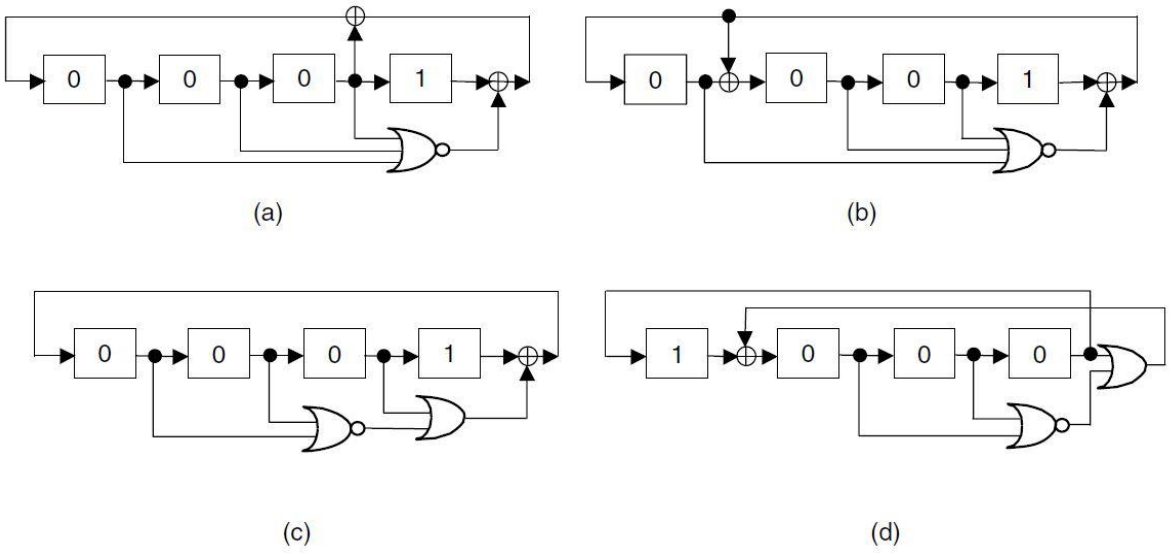


Figure 8: Complete LFSRs (a) four-stage standard LFSR (b) four stage modular LFSR (c) Minimized version of (a) (d) Minimized version of (b) [10]

Figure 8 (a) and 8 (b) show the application of complete LFSRs for testing a 4-input circuit under test. The 4-stage LFSR has a period of 16 cycles. At the last stage of the complete LFSR, an XOR gate and a NOR gate take the input from (n-1 stages) and act as a **zero-detector**. Using this scheme is advantageous as it can achieve the zero state for each bit after the state of {0001}. The LFSR presented in (a) and (b) can be minimized as shown in Figure 8 (c) and (d). The realizations shown in (c) and (d) have the zero state after the sequence of {1000}. The advantage of using exhaustive testing is that the detectable faults in the combinational logic will be detected. Furthermore, when the number of inputs are small, exhaustive testing is useful, otherwise it is time consuming and not feasible for circuits with a large number of inputs [10].

2.7.2 Binary Counter

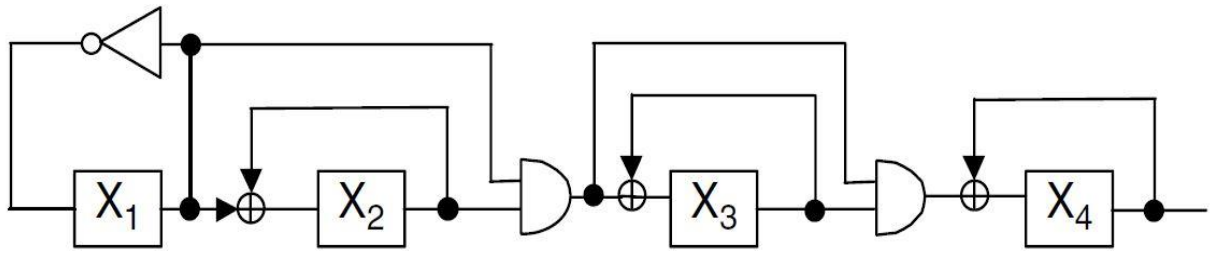


Figure 9: Binary counter used as Exhaustive Pattern Generation [10]

Figure 9 shows the example of a binary counter used as the test pattern generator for a 4 input combinational logic. The area overhead required by the binary counters is much larger as compared to the conventional LFSR used as a test pattern generator [22].

2.8 Pseudo Exhaustive Testing

This type of testing requires a fewer number of test patterns as opposed to 2^n test pattern required by the exhaustive test technique for a combinational logic with "n" inputs. All the stuck at faults can be covered by this method of testing.

2.9 Pseudo Random Testing

In this type of testing, a pseudo-random test pattern generator is used (PRPG) for generating the pseudo random test sequences [9, 10, 15]. This type of testing can be used for combinational as well as sequential circuits but does not give a clear idea of the fault coverage and the length of test sequence to be used for testing. However, many schemes have been proposed to resolve this shortcoming in [23, 24].

2.9.1 Maximum-Length LFSR

Maximal Length LFSR can be used as the pseudo random test pattern generator. The sequences produced by a maximal length LFSR has 0.5 probability of generating 1's and 0.5 probability of

generating 0's at the output. The shortcoming of using this technique is that the circuit under test may be resistant to the random pattern which means that the probability of certain nodes receiving the 0 or 1 value is low assuming the probability of having 0 or 1 in the input sequence is equal [25].

2.9.2 Weighted LFSR

To solve the problem of pattern resistant faults and increase the fault coverage in RP-resistant circuits, this method of testing is used. It uses an LFSR and a combinational circuit known as the weighted pattern generation technique which is described in [26]. The motivation to fit the combinational circuit between the output of the combinational circuit and the LFSR is to increase the frequency of some patterns and decrease the frequency of certain test patterns; hence, this technique increases the probability of detecting those faults which cannot be detected by using simple LFSR as the test pattern generation. The method to implement this technique is discussed in [27].This technique changes the equal distribution of maximal length LFSR so as to produce the equal distribution weighted input sequence containing 0s and 1s which are fed to the combinational logic under test. It adjusts the probability distribution to 0.25 or 0.75 instead of 0.5which helps in increasing the fault coverage not covered by the 0.5 distribution model. In [28-30], good fault coverage was obtained by assuming a probability distribution fault model.

2.10 Segmentation Testing

In the circuits where the length of the test pattern is too large or the number of inputs n is too large, a segmentation technique or partitioning technique is followed to reduce the test time [31]. By dividing the circuit under test into segments or partitions, this technique uses the idea of exhaustive testing. The partitioning can be achieved in one of two ways: hardware partitioning or sensitized partitioning [31-32]. In hardware partitioning, multiplexers are inserted and the embedded inputs

and outputs of the sub circuits are connected to unused primary inputs and outputs of the sub circuit under test. In sensitized partitioning, the circuit partitioning and the sub circuit isolation are achieved by applying the input test patterns to the input lines. The process of partitioning the circuit and testing it simplifies the overall testing process. Although the multiplexers reduce the operating speed, the overall functionality is not altered and hence, this method is still used as an accepted technique [33-35].

2.10.1 Signature Analysis

Signature analysis is one of the most widely used compaction techniques which is based upon the idea of cyclic redundancy checking (CRC) [16]. This technique can be divided into two categories: (1) **serial signature analysis,** which is used for compacting the output responses obtained from the circuit under test having a single output and (2) **parallel signature analysis,** which is used for compacting the responses obtained from the logic under test having multiple outputs [36-39].

1. **Serial Signature Analysis Technique**

In this type of technique, LFSR is used for the signature analysis and XOR gates are used for compacting the L-bit output sequence obtained from the logic under test. Figure 10 shows an "L" bit modular LFSR used to generate the output signature [10, 16, 43].

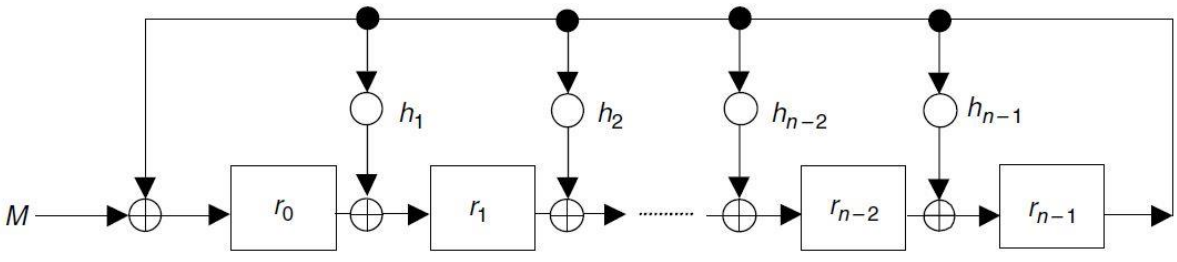


Figure 10: N-stage single input shift register [10]

Let the L-bit message be defined as M= {$m_0 m_1 m_2 \ldots . m_{L-1}$} and can be written as

$$M(x) = m_0 + m_1 x + m_2 x^2 + \cdots + m_{L-1} x^{L-1}$$

As the L-bit sequence is shifted into the modular LFSR, the remainder of the serial shift register R is given by {$r_0 r_1 r_2 \ldots . r_{n-1} x^{n-1}$} expressed below as

$$r(x) = r_0 + r_1 x + r_2 x^2 + \cdots + r_{n-1} x^{n-1}$$

The above response analyzer works as the CRC code generator [39]. Assuming that the LFSR is defined by the characteristic polynomial *f(x)* then the polynomial division can be defined as

$$M(x) = q(x) f(x) + r(x)$$

The final signature obtained from the SISR is the remainder *r(x)* of the polynomial division.

2. **Parallel Signature Analysis Technique**

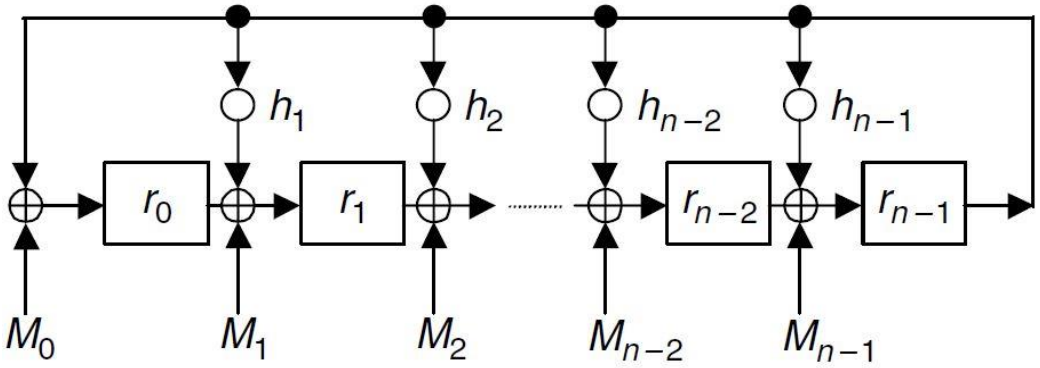


Figure 11: N stage multiple input shift register [10]

Other response analysis techniques such as transition count testing, ones counting, and the serial signature technique require a significant area overhead for testing an output with n-bit combinational logic. Figure 11 shows the n stage multiple input signature registers. In the multiple

input signature analysis technique, n-XOR gates are used in combination with the modular LFSR so as to compact the n L-bit output sequences from M_0 to M_{n-1}. In [40-42], it is shown that the MISR with n-inputs can be modeled as the n-input SISR if the input sequence is $M(x)$ and the error polynomial is $E(x)$ as written below [41].

$$M(x) = M_0(x) + xM_1(x) + \cdots .. + x^{n-2}M_{n-2}(x) + x^{n-1}M_{n-1}(x)$$

and

$$E(x) = E_0(x) + xE_1(x) + \cdots + x^{n-2}E_{n-2}(x) + x^{n-1}E_{n-1}(x)$$

Chapter 3

Boundary Scan and Core Based Testing

3.1 Introduction

The standard for the Boundary scan based testing is IEEE 1149.1 standard, also known as the JTAG standard. The standard was developed for testing of digital circuits on the board level and the standard is also used for testing integrated circuits. The standard has also an extension by the name of IEEE 1149.6 standard and is used for the prototyping of input/output high speed networks [44].

To address the problems related to testing the core based ICs where the *intellectual properties* (IPs) act as the building blocks, a different standard is developed which is analogous to the IEEE 1149.1 standard. The standard for core based testing is known as P1500 standard approved by IEEE in 2005.Most of the features in this standard are similar to that of the IEEE 1149.1 standard. Various features are supported by this core based testing standard such as design reusability, plug and play features, and hierarchical test features [10].

In this chapter, both standards are discussed in detail and a comparison is also made between the two widely known industry standards. The attacker can take the advantage of the full controllability and observability provided by these standards and attack the device under test while the device has been adopted for the infield use or even at the manufacturing stage.

3.2 IEEE 1149.1 Boundary Scan Standard

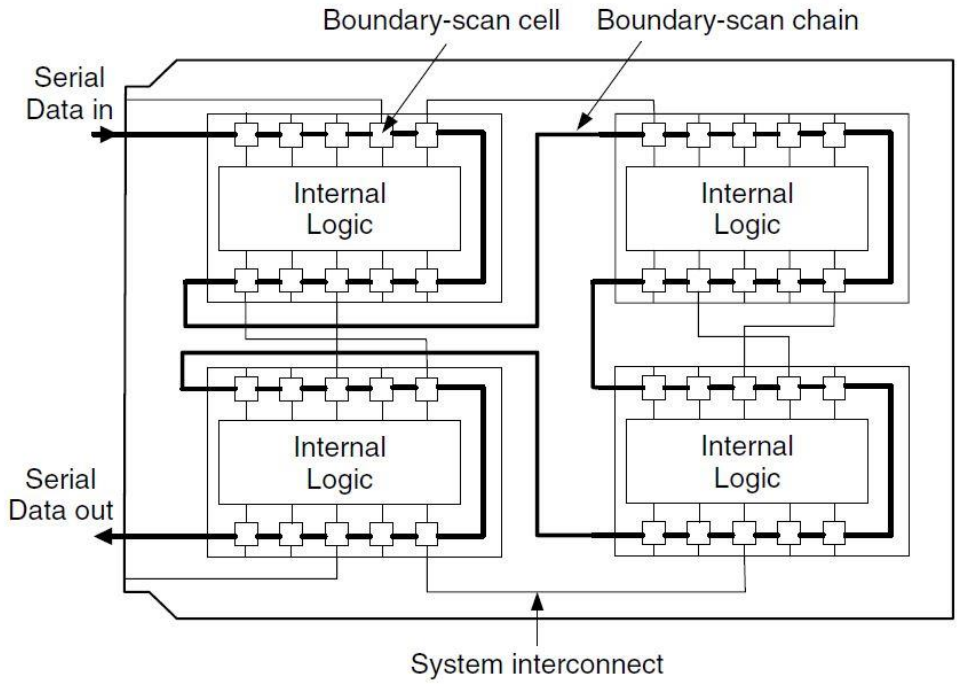


Figure 12: Board level testing in daisy chain architecture [10]

As shown in figure 12, the boards are connected serially as defined by IEEE 1149.1 standard to support boundary scan based testing at the board level. The motivation to call it boundary scan structure comes from the fact that the circuit under test is surrounded by the boundary scan cells serially so as to have good controllability and observability for the circuit under test. Those chips which support the IEEE 1149.1 architecture can be fitted in the board level architecture through the boundary scan registers. This protocol also supports the normal chip operations and thus, enhances the design debugging and testing capabilities [9]. The standard also supports the interconnect testing between the different circuits under test connected in a daisy chain architecture [45].

3.3 IEEE 1149.1 Test Architecture and Working

Extra circuitry and memory is included in the IEEE 1149.1 architecture in addition to the boundary scan cells so as to support the working of the whole IEEE standard. The internal logic, as shown in the figure 13, is the actual circuit under test which is compliant for various designs for test techniques such as scan based tests, built in self-test (BIST), and the boundary scan test technique. The standard is known to consist of various modules such as

- **a test Access port** (TAP) which is made of 5 terminals called t**est data input** (TDI), **test data output** (TDO), **test mode select** (TMS), **test clock** (TCK), and **test reset** (TRST);
- a TAP controller (TAPC);
- **an associated decoder** and **instruction register** (IR);
- many registers such as ***bypass registers, boundary scan registers, device ID registers*** **and** specific data registers which are used to control the signal flow; and
- the ***TAP controller***, which is a 16-bit state machines that controls the working of the state machines [9-10].

In addition to the test access port which is defined above, the IEEE 1149.1 architecture also consists of a 16-bit finite state machine which controls each step of the boundary scan architecture. The instruction which needs to be executed is serially loaded onto the instruction register through the external available TDI pin to the external user. The test signals which configure the boundary scan test for the instruction to be executed is provided by the dedicated decoder [45].

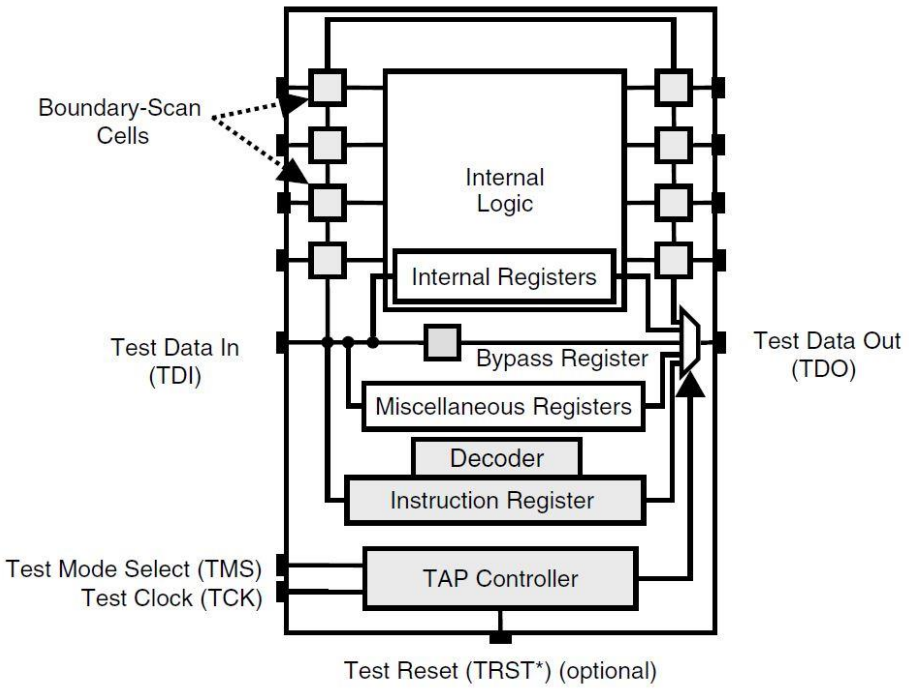


Figure 13: IEEE 1149.1 architecture [45]

Figure 13 shows the detailed structure of the serially connected board as shown in figure 12 above. The TAP port defines the standard for the boundary scan as well as additional input/output pins. The instructions in the boundary scan architecture are loaded through the ***test data input*** (TDI) pin. The associated decoder controls the test instructions so as to perform boundary related scan based tests. Additionally, there are ***test data registers*** which load the system-specific related information (namely company name, device ID instruction). Some of the mandatory test instructions such as SAMPLE, BYPASS, PRELOAD and EXTEST and several other instruction sets such as RUNBIST, CLAMP, USERCODE, IDCODE, HIGHZ are also included in this standard [45].

3.4 Boundary Scan Cell, Test Circuitry and Bus protocols

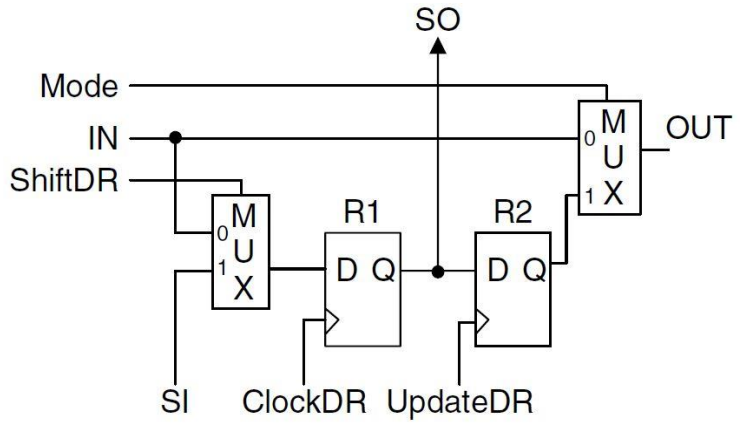


Figure 14: A Boundary Scan Cell [45]

Figure 14 shows the detailed boundary scan cell which forms part of the long boundary scan chain. The cell can be configured to acts as an input or output cell. For BSC as an input cell, the IN signal is used for the chip input pad whereas for BSC as an output cell, the OUT signal is connected to the output signal pad. The Mode signal controls the data driven on the OUT signal line. When Mode signal is disabled the boundary scan cell is in the **normal mode** of operation, data passes from IN to OUT directly like a short signal. Conversely, when Mode signal is enabled the boundary scan cell is in **test mode** of operation, data stored in the R2 flip flop is shifted from the multiplexer through the OUT signal port. The operations which a boundary scan cell can support are clockDR, shiftDR and updateDR. When the shiftDR signal is disabled and clockDR signal is enabled, the data which is present at IN is captured by the capture flip flop. Similarly, when the shiftDR is enabled and the clock pulse is applied to clockDR, the data is shifted from scan input SI to scan output SO to feed into the next boundary scan cell [45].

3.4.1 TAP State diagram

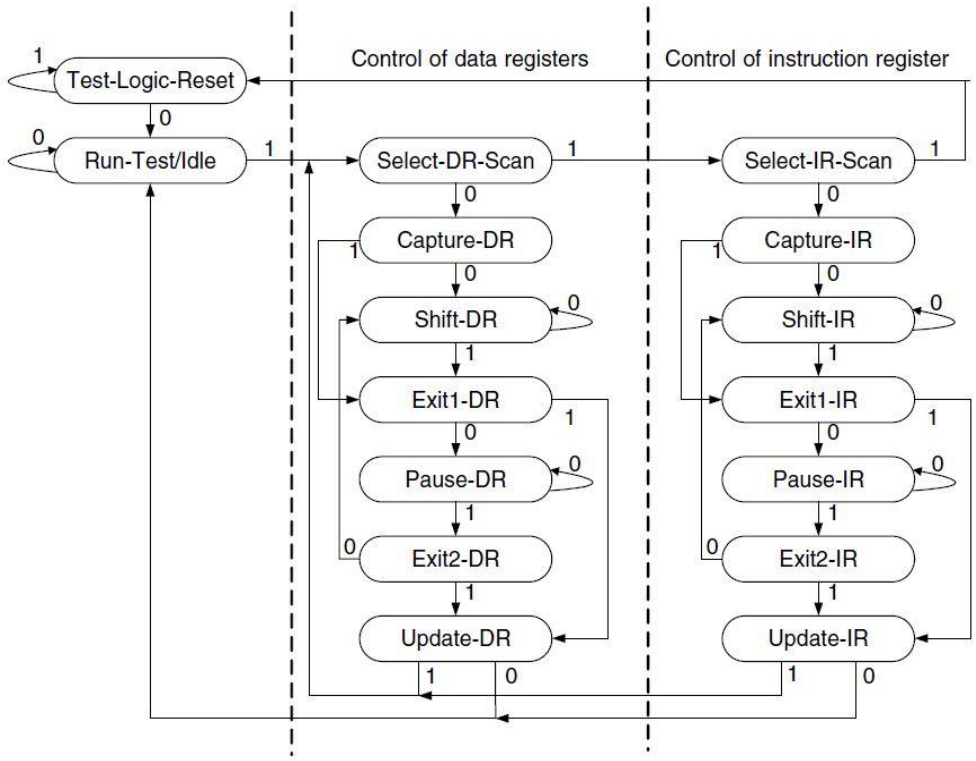


Figure 15:16-state finite state machine to support Boundary Scan Architecture [45]

Figure 15 shows all the state transition of the TAP controller in accordance with the state diagram. The states are controlled by the rising edge of the TCLK; on the other hand, the next state is being determined by the logic level of TMS. There are nine control signals being solely controlled by the TAP controller, namely, clockDR, shiftDR, updateDR, clockIR, shiftIR, updateIR, selectTCK, and enable signals. All 16-states are divided into three categories. The leftmost states consist of two states, namely, rest and the "Run-Test Idle" state. This is followed by the middle part which has 7 states and lastly, the rightmost part which also has 7 states. The functions of the rightmost part are analogous to middle part; however, there is a difference between the set of registers being used to perform these operations [45].

The important states can be described as follows [45-47]:

- **Test-Logic-rest:** The boundary scan circuitry is disabled so that the system can perform in the normal mode of operation. If the Logic 0 is applied to the TRST port, then the TAPC enters this state. The TAPC can be synchronously reset to logic 1 if the TMS is applied for 5 clock cycles. If a glitch occurs at the TMS, then the TAP controller is forced into the Run/test idle state. In order to return to the normal state, the TAP controller has to be kept at 1 for the next 3 clock cycles.
- **Run-Test Idle**: In this state, the boundary scan circuitry waits for some test operations to be synchronized with the TCK.
- **Select DR Scan-** This is one of the temporary states aimed at initializing the data register to enter into the manipulation column.
- **Capture-DR:** In this state, the data is loaded in parallel to the specified data registers. This state is used to capture the current test results and the normal operation status.
- **Shift-DR:** The stored test data is scanned out from the data registers by the current instruction. As long as the TMS is 0, the TAP controller will remain in this state.
- **Exit-DR:** In this state, all parallel loaded or shifted data held in the data registers are preparing for the update or pause instruction.
- **Pause-DR:** This is used to pause the normal operation so as to perform some external operation. This command is useful if the test operation is to be paused so that the tester can shift the data serially from the input pin .This can also be used to bring latency into the test procedure.

- **EXIT2-DR:** This instruction is used to indicate the completion of the test procedure. In addition, it allows the TAPC to enter into the update state or to indicate the end of the Pause-DR command such that the Shift-DR can be activated so as to shift more data.
- **Update-DR:** In this command, the data is latched so as to obtain the parallel output from the selected data registers on the falling edge of the TCLK. The data stored in one data register is shifted to another data register in the boundary scan cell discussed above so as to perform the operation of a serial shift register.

3.5 IEEE 1500 Architecture

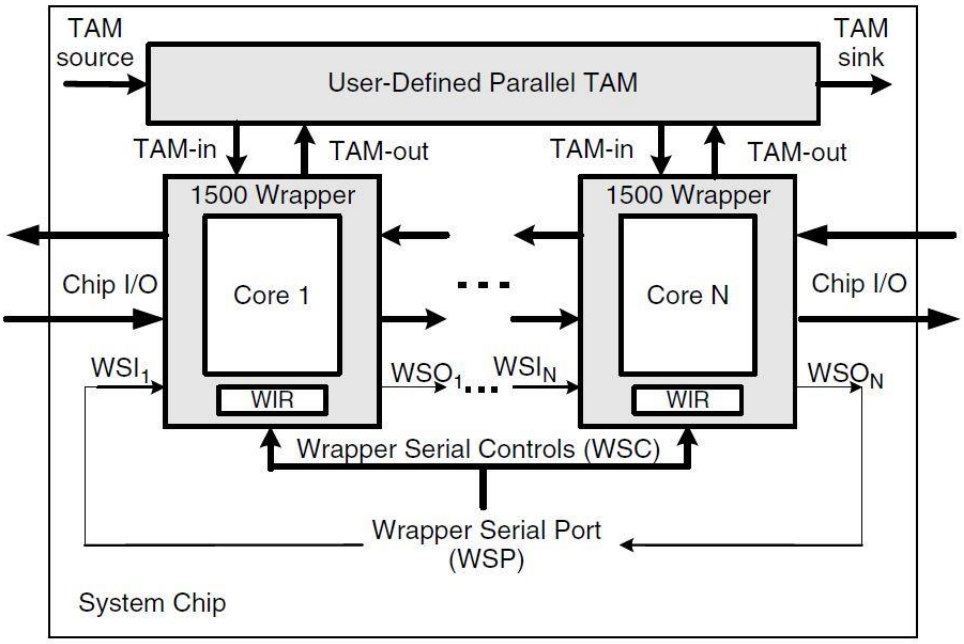


Figure 16: IEEE P1500 illustrating wrapper on different cores and TAM [48]

The IEEE 1500 standard defines the use of wrapper architecture on the boundary of input/output terminals of different cores which allows the testing of different types of cores in a standardized manner. Figure 16 shows the scenario where the N cores are wrapped by the IEEE 1500 standard defined wrapper. The wrapper serial port (WSP) comprises of the wrapper serial instructions which

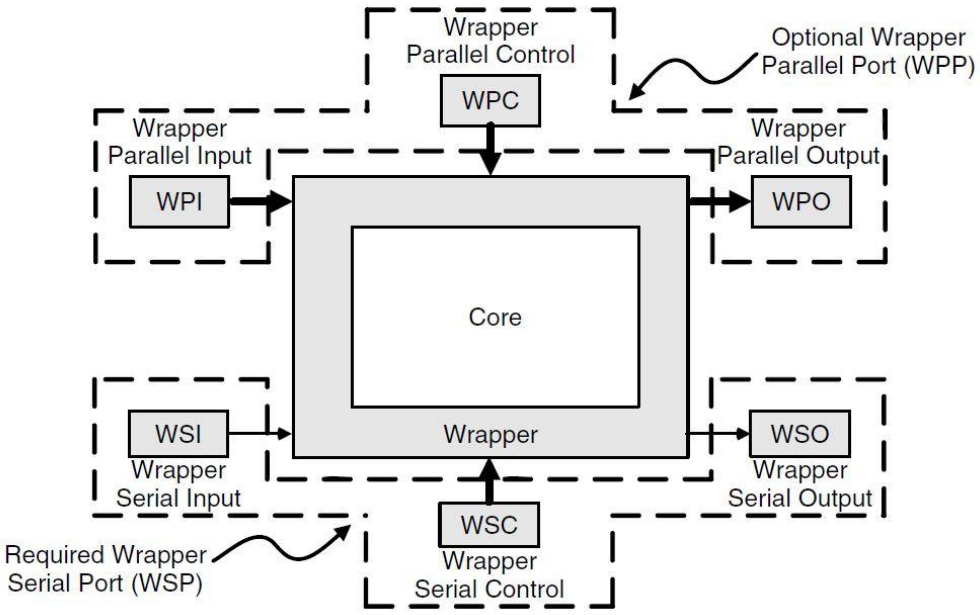


Figure 17: IEEE P1500 Test interface illustrating parallel and serial wrappers [48]

consist of ***wrapper serial input*** (WSI), ***the wrapper serial output*** (WSO), and several ***wrapper serial control*** (WSC) terminals. The individual wrapper has an instruction register called the ***wrapper instruction register*** (WIR) whose function is to store the instruction to be executed for the individual cores [48-50]. The wrapper serial port supports serial test instructions much like the boundary test architecture of the IEEE 1149.1 architecture. Moreover, the IEEE 1500 standard also supports parallel ***test access mechanisms***. Individual cores can have their own TAM-in and TAM-out ports consisting of different control lines to support the parallel test access instructions for the cores. Figure 17 shows the both the core interface and the serial and parallel data control as being highlighted. Also reflected in figure 17 are the ***wrapper parallel control*** (WPC), ***wrapper port input*** (WPI), maps to the TAM input port and the ***wrapper parallel output*** (WPO) which corresponds to the wrapper output port. In the IEEE 1500 standard, serial ports are defined to be mandatory; on the other hand, the parallel ports are defined to be optional. The parallel interface defined in the IEEE 1500 standard leads to significant test time reductions for the SoC based testing

as compared to the IEEE 1149.1 standard. In the IEEE 1500 standard, the use of core test language is also proposed which supports the usage of different kinds of cores from different vendors on the same system on chip. The language defined can capture and express the test related information by complying with the defined IEEE 1500 standard [48].

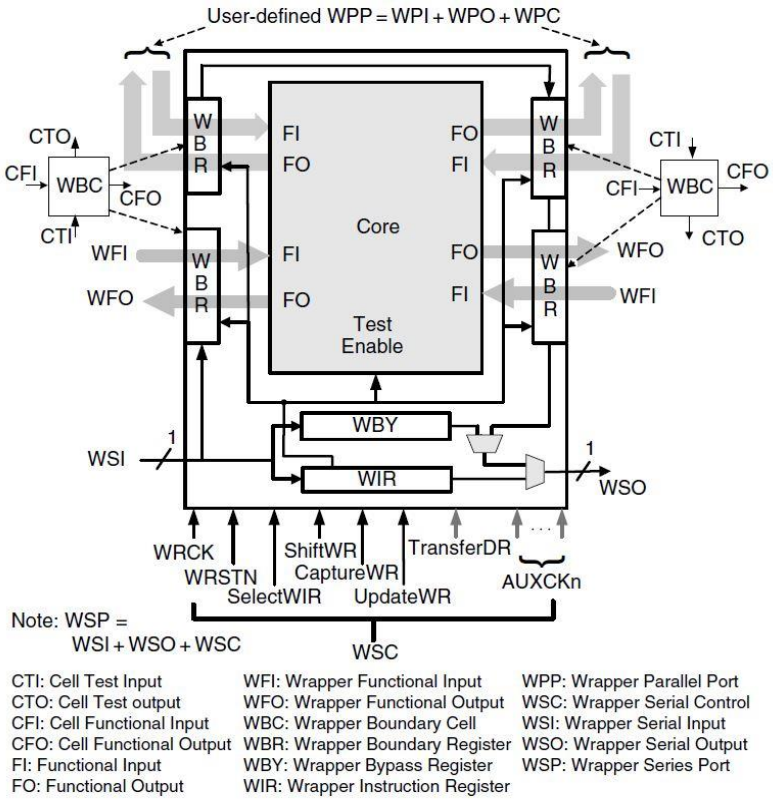


Figure 18: Test circuitry supporting IEEE P1500 architecture [48]

Figure 18 shows the detailed architecture of the IEEE 1500 standard and the standard core architecture which compromises of the following parts, as described below [48]:

1. ***Wrapper serial port*** (WSP) which consists of *wrapper serial input* (WSI), *wrapper serial output port* (WSO), and several wrapper terminals. Analogous to TDI and TDO of the IEEE 1149.1 standard, WSP uses WSI and WSO to scan in and out the wrapper instructions in the IEEE 1500 standard. The mandatory instructions which are included are WRSTN,

WRCK, SelectWIR, CaptureWR, ShiftWR, and UpdateWR with optional instructions called TransferDR which are briefly defined below.

- **WRCK-** This instruction is dedicated to the operation of the IEEE 1500 standard.
- **AUXCKn-** This instruction is used for the auxiliary 1500 clocks and can be used for the implementation of wrapper boundary registers. The n signifies the number of auxiliary clocks which signifies the number of clock being used. These clocks can be shared by the system clocks as well.
- **WRSTN-**This instruction resets the wrapper circuitry and takes the system into the normal mode of operation, as required. The wrapper bypass instruction is analogous to the wrapper instruction defined in the IEEE 1149.1 standard.
- **SelectWIR-** This instruction is used to determine an instruction or the data type of operation to be performed. If the selectWIR =1, then it signifies the connection between WSI and WSO, else only some data registers are connected between WSI and WSO.
- **CaptureWR**-This instruction is used to enable capture operation for the selected data registers.
- **ShiftWR-** This instruction enables the shift operation for the selected registers.
- **UpdateWR-** As the name suggests, it is used for the update operation of the data registers.
- **TransferDR**-This is used for the transfer operation for of the selected registers implementing the transfer function.

2. ***Wrapper Parallel Port*** (WPP) comprises of the user defined *wrapper parallel input* (WPI), *wrapper parallel output* (WPO), and *wrapper parallel control* (WPC) signals. All of these terminals are optional and a WPP may include clock terminals of the WSC.
3. ***Wrapper Instruction Register*** (WIR) is used to store the information which needs to be executed in the IEEE 1149.1 standard. When the WSC is set to 1, the WIR is selected unconditionally. It is implemented using a two stage design which supports the loading and shifting of the instruction in the data registers. The broad differences between the IEEE 1149.1 and IEEE 1500 standard can be outlined as follows:
    - There is no state machine used in the IEEE 1500 standard and the control signals used are provided by the WIR, which get the instruction form the WSC terminals. Figure 28 shows the image of the wrapper instruction register which consists of shift stage and decode/update stage as well; and
    - IEEE 1500 optionally provides a parallel load mode as shown in figure 24, which allows the WIR to capture the control information directly or to capture data that can be used to test WIR or other IEEE 1500 circuitry.
4. ***Wrapper Bypass Register (***WBY) - is used similarly to the bypass register used in the IEEE 1149.1 architecture. The WBY register is selected and connected between the WSI and WSO if the current instruction of the wrapper bypass register is being executed. It can also act as the default register between the WSI and WSO.
5. ***Wrapper Boundary Register*** (WBR) - It consists of wrapper boundary cells analogous to the boundary scan registers of the IEEE 1149.1 standard. There are 4 terminals in each Wrapper boundary register (WBR), namely, ***cell functional input*** (CFI), ***cell functional***

output (CFO), ***cell test input*** (CTI), and ***cell test output*** (CTO) which is shown in figure 18.The functional modes are further classified as follows :

- *Normal Mode:* The WBR is transparent to the system and core executes the normal function of operation.
- *Inward Facing Mode:* The test access is for the core and the functional inputs of the core are controlled by WBR and also observed by the WBR.
- *Outward Facing Mode:* The test access is used for the external test circuitry where the wrapper functional outputs and wrapper functional inputs are controlled and captured by the Wrapper boundary register (WBR).
- *Nonhazardous (safe) mode*- The functional inputs and outputs of the core are controlled by the wrapper boundary register (WBR) to a safe state.

Chapter 4

A Hardware Security Solution against Scan-based Attacks utilizing LFSR

4.1 Introduction to Hardware attacks

In this chapter, the possible hardware attacks on the IEEE 1149.1 standard and a secure method of testing resilient to hardware attacks are presented and discussed. Scan based designs for test techniques have been widely adopted and used for many years. Though such access is desirable for testing the circuit under test, it is not acceptable for secure chips as it can lead to their exploitation. In the proposed method, a secure way of testing the circuit under test is presented and the access to the circuit under test is severely limited so as to reduce the risk of scan based attacks. To address the testability issue, a built in self-test is proposed so as to thwart off against scan based and side channel analysis attacks.

4.2 Literature Survey and Existing solutions in Literature

Scan based testing provides a good control over the controllability and observability of the circuit under test. Such access is not desired for the secure circuit under test. Scan chain based testing can also be exploited for cryptanalysis attacks as they give direct access to the circuit under test [51-52]. Also, various other attacks such as differential power analysis attacks [52], timing analysis attacks [53], and fault injection attacks [54-55] may present themselves when using scan chain based testing. Many well-known encryption algorithms such as the RC4 stream cipher and the AES encryption algorithm have been attacked by the use of scan based testing techniques [56]. Thus, a tradeoff needs to be maintained between the security and testability of the chip under test. In [57], authors have discussed how the scan chains can be used to retrieve the secret key from the chip under test even when the critical registers containing the secret key are not included in the chip. In [58], authors have used scan based design for the test method from the perspective of

physically unclonable functions (PUF).The variations present in terms of process, voltage and temperature in addition to the intrinsic characteristics of PUFs have all been studied and discussed by the authors. Yu Zheng et.al. [59-60], have discussed how scan chains can be used from the perspective of PUF and how unique signatures can be obtained from scan chains. To counter scan based attacks various solutions have been proposed such as using built-in-self-test for testing, hybrid designs which are combination of BIST and scan chains [61]. Yang et.al. [57, 62] have discussed attacks against the Advanced Encryption Standard hardware implementation by using scan chains as the tool for information leakage and for the recovery of the crypto key of the Advanced Encryption Standard. To mitigate the problem of scan based attacks, authors have also introduced a solution which uses the mirror key registers for the insecure mode of testing and a different set of registers for the secure mode of testing. Authors have also concluded that even if the key register are not directly scannable, the attackers can still build the key and hence, attack the system. In [63], authors have proposed a scan chain scrambling technique which, provided that the right key is given, the assignment of key registers is static, else the semi-random values are assigned to the key registers. Lock and key technique is proposed in [64] to mitigate the problem of scan based attacks. Here, they have used a linear feedback shift register so as to input the right test vectors in the circuit under test. A right test key is needed to switch from the insecure mode to the secure mode of testing. If the test key entered by the user is not authentic, the LFSR assumes the semi random values which can mislead the attacker. Low cost secure scan (LCCS) has been proposed as a solution for the protection of intellectual property information in [65]. In this solution, dummy flip flops are used in addition to the normal D flip flops in the scan based testing technique. At the time of testing, the right test key needs to be entered in the right sequence with the dummy D flip flops. If the right test key is not integrated in accordance with the position of the

dummy flip flops, then random values are assigned in the scan based testing technique and random responses are shifted out from the flip flops. In [66], authors have proposed a scan based architecture in which the subsequent values are changed dynamically at each stage of scan flip flops and hence, creates a secure way of testing the circuit under test.

4.3 Scan Based Attacks

Scan chains provide full access to the circuit under test (CUT) through the test access port of the CUT in the test phase. The test responses obtained from the circuit under test are used for the evaluation. The scan based testing operation can be described in the following four steps.

a) **Scan In:** In this step, the test vectors are serially loaded into the scan flip flops which are directly connected to the circuit under test. The known test values can even be fed to the critical registers in the scan based test technique.
b) **Response Capture:** The response of the applied test vectors to the circuit under test is captured at the output by the scan flip flops.
c) **Scan Out:** The response captured by the scan flip flops are shifted out and are available at the output pin TDO.
d) **Response Evaluation:** The responses obtained for the circuit under test are analyzed by the attacker to unfold the test circuitry and hence, decode the position of the critical registers.

To counter this type of scan based attack and make the data obtained from scan based testing less prone to attacks, a solution has been proposed in [56] to introduce random invertors in the scan chain path. For a total number of m flip flops, the proposed solution can have 2^m various possible configurations and the probability of attack would then be $1/2^m$.The shortcoming of this technique is that after fabrication, the positon of invertors cannot be changed and it remains fixed forever. A

spy flip flop scheme has been proposed in [67] which prevents the switching from one mode to another mode of testing. This scheme requires the use of a secure test controller and the overhead area of the proposed scheme is also very significant. The architecture discussed above is not prone to fault injection or side channel power analysis attacks which are different types of attacks to leak out critical information from scan based testing.

4.4 Proposed Method

In the proposed method of testing, the secret code is generated by an array of flip flops which can be used for the purpose of encryption or identification as shown in figure 19. The flip flops are hard wired to generate the secret key at the power-on state of the array of flip flops. To protect the secret key created by the array of flip fops against scan based attacks, direct access to the flip flops is not given in the proposed technique. Instead, a built in self-test is used as the design for test method to test the circuit under test. There are two modes of operation in the proposed method: (a) the secure mode or the safe mode of operation and (b) the test mode or the insecure mode of testing. In the test mode of operation of scan based testing, the first three flip flops are configured to work as the test pattern generator (TPG) which generates the code for the testing of the circuit under test and is shifted through the array of flip flops. The proposed scheme does not allow switching from insecure mode to secure mode; on the other hand, if the system switches from secure mode to

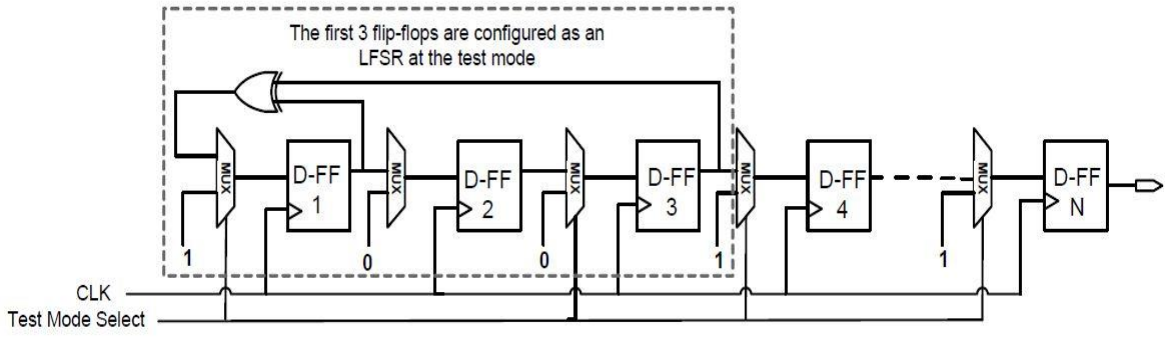


Figure 19: First 3 flip flops configured as test pattern generator [68]

insecure mode, then the following steps are sequentially taken [68]:

- a reset signal is applied to the array of flip flops containing the secret key to clear the content of all flip flops;
- the first three flip flops are converted to a 3 bit-LFSR to act as an Automatic Test pattern generator (ATPG) for the array of flip flops configured as the shift register in this mode of testing;
- the access to the output of the shift register is granted to the scan chain which will allow the scan chain to capture the data and perform the response evaluation operation; and lastly
- the data captured by the scan chain is compared against the response of a fault free circuit to determine whether or not the circuit generating the secret key is faulty..

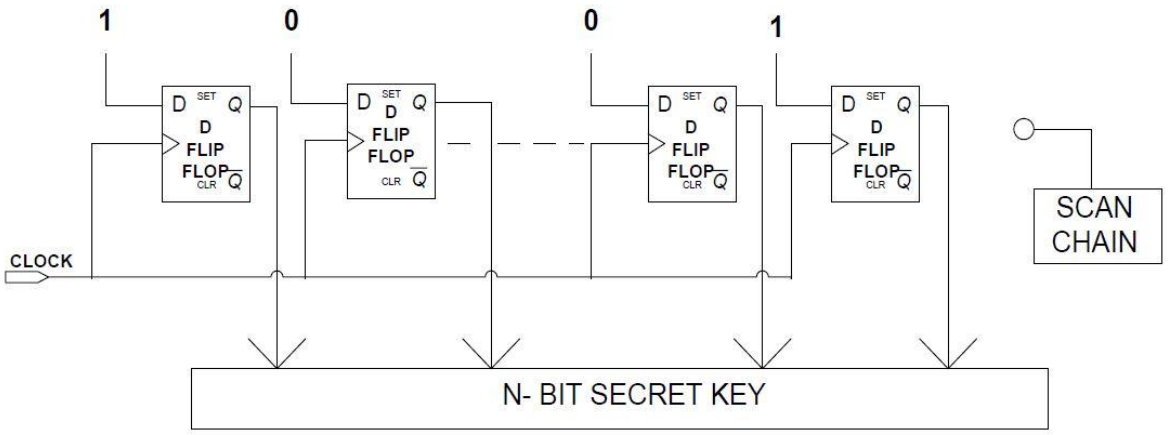


Figure 20: Stored hard wired key in array of D flip flops [68]

It is not necessary to power off the circuit while switching from the secure mode to the test mode as the reset signal is applied to the array of flip flops. The proposed architecture in the secure mode of testing is shown in the figure 20. The test patterns which are generated by the test pattern generator are shown in the figure 21 and are determined by the number of D flip flops required for the purpose of testing. As compared to the test techniques proposed in [65], no separate set of registers is needed for the different modes of testing and it reduces the area overhead by a large amount. A fault in the circuit generating the secret code changes the output data captured by the scan chain. The transition from the secure mode to insecure mode sends a reset signal through the chain of flip flops as shown in the figure 22.The control circuit prevents the attackers from access to the key through the shifting of the data right after changing the mode of operation. To address the testability issue of the key generating circuit a built in self-test (BIST) is developed in the figure 19 [68].

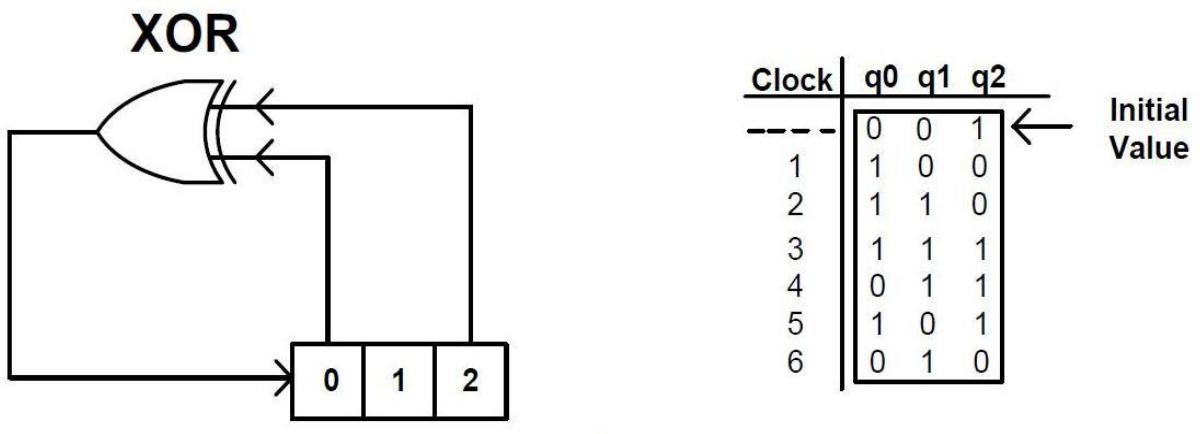


Figure 21: 3-bit LFSR configured to act as test pattern generator [68]

The first three flip flops are configured to form the shift register which generates the test patterns represented by the equation [68]

$$F_{LFSR} = x^3 + x + 1$$

The pattern generated by the LFSR is applied to the rest of the flip flops and the response by the last flip flop is captured by the scan chain for the evaluation. The test patterns generated by the LFSR is shown in the figure 21. It can cover all the stuck at faults since the output of each flip flop has to switch from the high to low and low to high. It can also be used cover the delay faults due to the successive number of transitions between the adjacent test patterns. A fault in the circuit generating the secret code changes the output data captured by the scan chain. To support the proposed architecture, one state can be added to the IEEE 1149.1 boundary scan architecture as shown in figure 23. The states of the TAP controller has to accommodate one extra state to support the secure mode of testing.

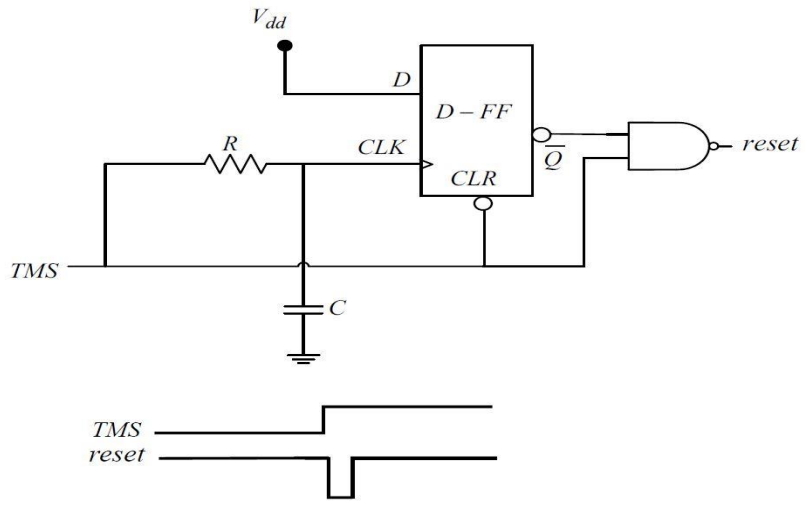


Figure 22: Test Controller for switching between various modes of testing [68]

As the Test Mode select (TMS) switches to the high level, it enters the safe mode and remains in this mode as long as the TMS is high. In this state, the N bit secret key loads while the access to the main scan chain is disabled. As soon as the TMS switches to low, it will change state and enters the scan mode. Before switching to the scan mode, the control circuit generates a pulse to reset the flip flops [68].

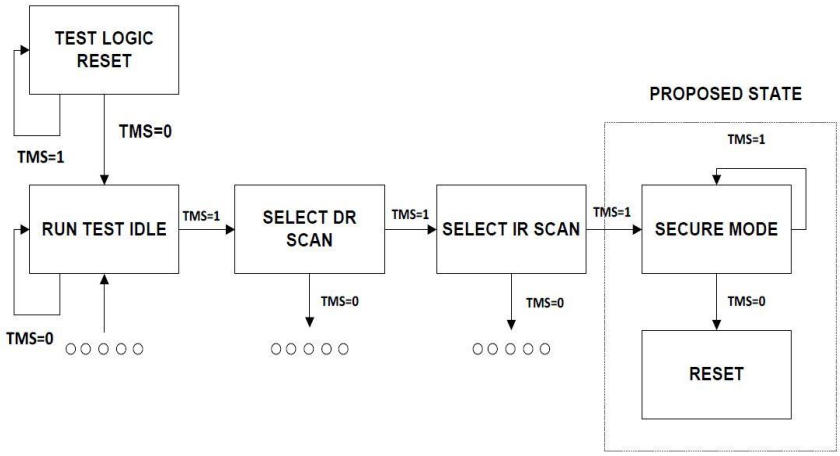


Figure 23: Modified 16-bit state machine supporting IEEE 1149.1 architecture [68]

4.5 Simulation Results

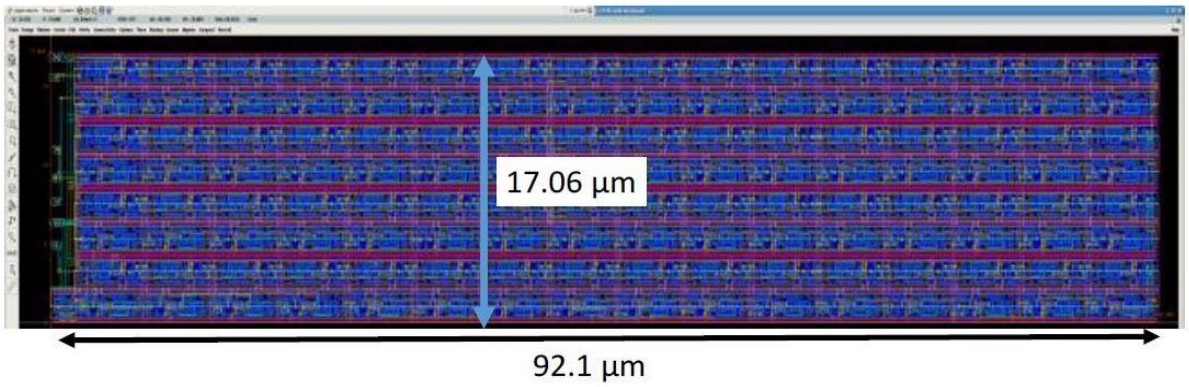


Figure 24: The implemented design on cadence 65nm suite [68]

The proposed architecture in [68] was implemented in the Cadence environment with 65nm technology. The results were also compared to the existing solutions in literature and are shown in the Table 2. The effect on increasing area overhead has also been studied. The layout of the proposed architecture is also shown figure 24. The proposed architecture consumes 1571 μm^2 of Silicon. The proposed architecture is almost linearly scaled with the use of 256 bit secret key, which is double of the 128 bit key [68].

TABLE I. GATE OVERHEAD OF EXISTING METHOS WITH PROPOSED METHODS ON ISCAS BENCHMARK 1989

Benchmark Name	#No of Gates	#No of Gates and Flip Flops	#LCCS Overhead on Bench(%)	Proposed Scheme-#No of Gates & Flip-Flops	Proposed Scheme Overhead
				#128 bit Secure Key	#128 bit Secure Key(%)
S13207	7951	8620	22.4	1796	20.83
S15850	9772	10369	19.2	1796	17.32
S35932	16065	17793	18.1	1796	10.09
S38584	19253	20705	15.6	1796	8.67
S38417	22179	23815	18.1	1796	7.54

Table 2: Comparison of proposed architecture with existing solutions [68]

Chapter 5

A Secure Test Solution using BIST for Crypto-Cores

5.1 Introduction to Core based attacks

A common system-on-chip (SoC) can have many embedded cores. Generally, the cores embedded on the system-on-chip can come from various chip vendors .The cores embedded on the chip can be in the form of soft cores or hard cores. Testing of system on chips by itself has become a problem the security related concerns add another dimension to the complexity of system on chip (SoC) testing. Scan based design for testability is one of the popular test techniques but this method compromises the security of the device under test. The system utilizing scan chains are prone to various types of attacks.

5.2 Scan based attacks and countermeasures

Many encryption algorithms such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Triple DES are key based algorithms and involve either the use of a private key or a public key in the encryption and decryption of the plaintext. Attackers can analyze and access the key involved in these algorithms and thus, attack the whole system [69]. The AES algorithm is a widely accepted standard by NIST [70]. AES can use a 192, 128 or 256 bit input to encrypt or decrypt the data. The plaintext data is processed and computed on two dimensional arrays. As the first round, also known as the initial round, is completed using the round function, the plaintext message is copied to an array. It is then XOR-ed with a secret key contained in the algorithm. The array is later transformed by implementing the round function and repeating it 10 times.

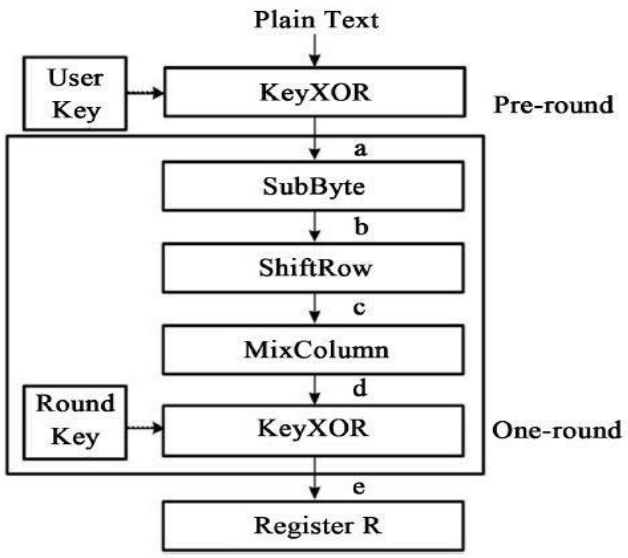


Figure 25: Steps involved in AES Encryption [70]

The final state is then copied as the output. The round function of AES can be parameterized by the key expansion and it is capable of generating a variation of the original secret key for another round. A single AES round consists of many operations such as SubBytes, ShiftRows, MixColumns, and the AddRoundkey operations. Once the first round is completed, the computed value of the round register is used in the second round. For testing the functionality of a chip, it is mandatory to include the round register. The attacker takes advantage of the chip using the scan chain embedded in the chip to retrieve the secret key used in the encryption algorithms. Figure 25 illustrates the steps involved in AES encryption operation, and figure 26 shows how an attacker can attack the round operation of AES using the internal scan chains. The round register also stores the intermediate cipher-text before and after the pre-round operation. The attacker switches the chip implementing the AES algorithm many times between the normal mode and the test mode to build the entire structure of the cryptosystem and control the system as required

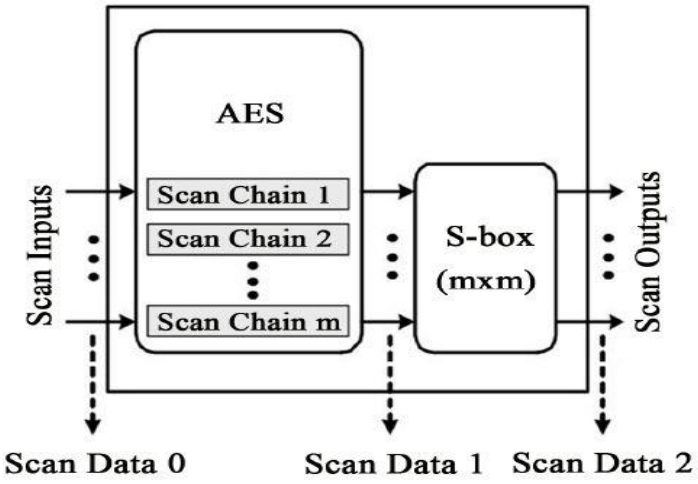


Figure 26: Scan based attack on AES round operation [72]

by an attacker [71]. An attacker may also resort to a side channel attack [69] or a signature attack [72] to obtain the secret key from the encryption algorithms. In [73], a fake key method is presented. In the system on chip environment, even though various protection measures are used, the critical information can still be obtained through the primary input or output pin. The scan based attacks can compromise the security of TV satellite boxes as well, which can lead to the shipping of many defective systems to customers. In [74-75], it is shown that the security of the crypto system can be compromised if the required steps are not taken to increase the level of system security. In [76], the authors have successfully attacked the trivium cipher and have generalized the attack to various other stream ciphers as well. Different attacks have been proposed against various stream ciphers using scan chain designs [74]. The authors implemented the trivium cipher scan chain design on the Spartan FPGA board and proposed the XOR- chain architecture as the countermeasure to prevent scan based attacks. In the proposed XOR scan chain

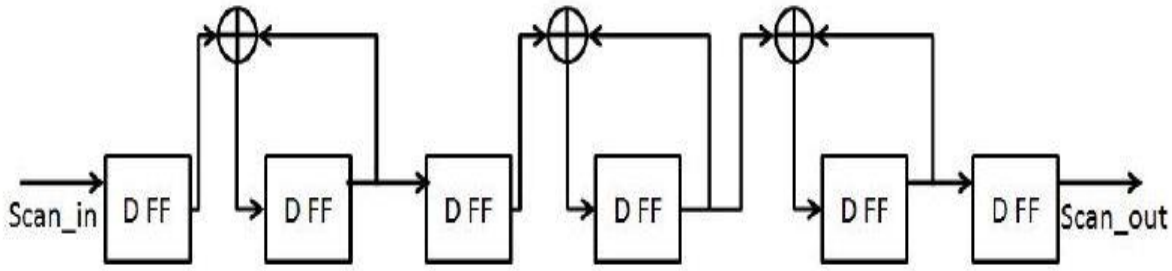


Figure 27: Architecture showing the XOR gate at random places [76]

architecture, random XOR gates are inserted in the normal scan chain. In the modified architecture, one of the inputs of the XOR gate is the input of the flip flops preceding the normal output of the scan chain as shown in figure 27. In the proposed scheme, the XOR gates serve as the invertor and invert the previous value of data fed in the scan chain. In Figure 27, the authors have discussed the placement of XOR gates at specific positions between the normal D flip flops and discuss the effect on the final output pattern obtained from the scan_out pin. In the end, the security and area overhead analyses of the proposed technique are also performed with respect to the previous published works in literature. By taking advantage of side channel information obtained from the scan based attack, many recent encryption algorithms such as RSA [77], ECC [78] can be attacked successfully using the scan chains. The proposed secure testability method does not deviate much from the normal scan based testing and does not compromise the fault coverage provided by the normal scan based test technique.

5.3 Proposed Method

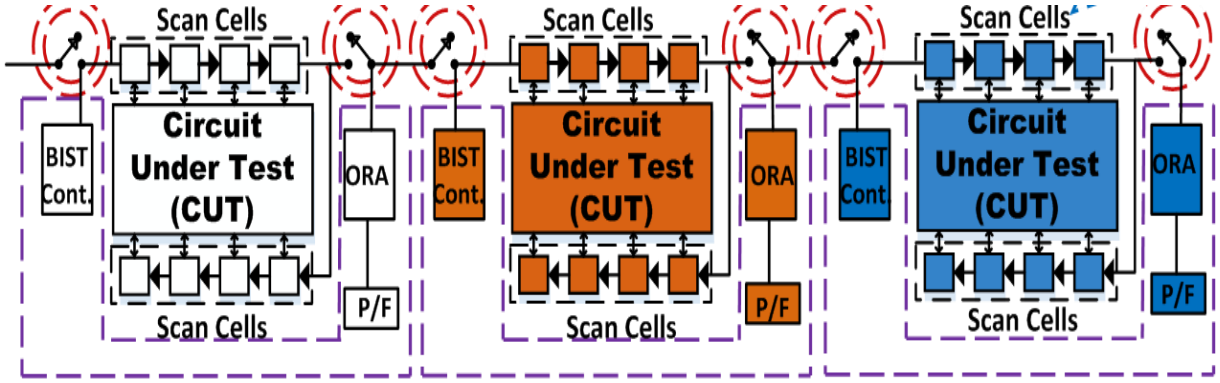


Figure 28: Proposed Architecture showing the signature analysis

In the proposed method, the access to the crypto-core containing security sensitive information is not provided through the scan chain in the operation mode as shown in Figure 28. A BIST is considered to perform tests on the crypto-core. As a result, the boundary scan cannot be used to access the critical information in the crypto-core. The BIST controller for the proposed method consists of test pattern generators, the circuit under test, and the response analyzers. The BIST controller test pattern generator is designed in such a manner that it achieves the required fault coverage. The test pattern generated by BIST is fed into the circuit under test and the responses obtained from the circuit under test are then compared by the output response analyzer, which compares the output with the stored "golden" test patterns. The obtained test responses determines whether the circuit under test is faulty or fault free. To shift the responses to the test access port, the switches needs to be closed. The proposed method only makes use of the offline BIST i.e. when the circuit under test is not in its normal mode of operation. The proposed BIST for testing the circuit under test generates the timing control signals and the scan enable signals. All clocks are generated by the proposed logic BIST controller to coordinate the BIST operation among the TPG, CUT, and ORA, as well. As the test operation is completed, the BIST then sends the final

done command to indicate the process is complete. The advantage of the proposed solution is summarized below.

- The proposed BIST method can effectively test and find the errors of the system. It can also provide the diagnostic information about the circuit under test without the need of an external tester.
- The proposed BIST supports the on-chip implementation and testing of the circuit under test which can support at-speed testing for the circuit under test.
- Using the proposed BIST effectively reduces the dependency on external testers, the test time, and test costs as BIST itself acts as the tester for the circuit under test.

While designing the proposed BIST, much care was taken to deal with the unknown blocking values used in the output response analyzer for signature analysis. Any unknown values (X), if fed to the output response analyzer, can corrupt the response analyzer and thus, the whole BIST can malfunction. In the fault injection attack, the attacker deliberately alters the correct functioning of the circuit under test by resorting to different methods such as analyzing the variations in the power traces, inducing faulty clocks in the circuit, overheating the device, and sometimes exposing the device to particular types of radiation. In one of the methods, an attacker lowers the chip power supply level and then injects transient faults by starting from a single bit error and increasing the number of faulty bits later. The above methodology is proven to be successful in the ARM 9 processors [79-80] and in the ASIC implementation of the stream ciphers [81-82].

5.4 Complexity Analysis

To successfully attack the proposed crypto system, the following assumptions need to be made by an attacker:

1. The attacker first needs to find the circuit under test as the different circuits under test may have their own specific built in self-test on the system on chip (SoC);
2. The attacker is aware of the P1500 standard and has the full control of the system on chip;
3. The attacker has control over the internal scan chain of the circuit under test on the system on chip and the pin to the internal scan chain of the circuit under test is not fused out; and
4. The attacker understands and comes to the fact that the proposed test technique can only be used for the offline testing of the circuit under test.

Chapter 6

A Hardware Secure Solution for Scan enabled Circuits using access Control

6.1 Introduction

As human society is progressing towards technological advancement and relying more and more on electronic devices, there has been an ever-increasing demand to constantly improve the technology available. Since integrated circuits form the heart of electronic devices, there has always been demand to have tiny ICs with millions of transistors embedded on them. Testing forms an important step which needs to occur before an IC can be released in the market for public use or before it can be used for board level applications [83-84]. Over past years, many techniques have been developed to test integrated circuit systems at various levels such as the board level or the system level.

6.2 Literature Survey and Existing Solutions

To test a circuit, an access mechanism has to be developed to control the internal nodes and observe their response to applied test vectors. Scan is a widely used technique which increases the testability of the device under test. An unrestricted access provided by the scan architecture raises a conflict between the security and testability of devices. Though scan based testing offers many advantages in controlling and observing the internal nodes of the circuit under test, it also suffers from disadvantages as listed below:

- conventional scan can be used to extract sensitive information such as private key from embedded crypto-cores;
- area overhead increases if the full circuit is to be tested using the scan based testing technique;

- the volume of the test patterns increases considerably as the design becomes more and more complex and hence, the test patterns have to be compressed before they can be applied to the circuit under test; and lastly
- in order to reduce complexity, test time and power consumption, partial scan design can be used at the cost of low fault coverage.

To have a secure test solution against scan based attacks, many methods have been proposed. In [85], authors have proposed a new secure solution to protect the secret data from scan based attacks. The authors in the proposed architecture have recommended a dedicated architecture to control the data fed to the Logic under Test (LUT). The dedicated architecture consists of security blocks called reset controllers and scan enable integrity controllers to control a state machine. The state machine satisfies two main principles i.e. robust encoding and redundancy. To prevent a physical attack on the scan chain, the proposed method also embeds the scan enable integrity block. To bypass this block, an attacker has to know the correct position of critical scan flip flops which is not an easy task. In [86], Ross et.al. have proposed different attacks against smart cards, TV systems, and security processors. It is shown how tamper resistant attacks can easily demean security systems. From a variety of available tamper resistant techniques, the designers settled with the four layer wrapping of 40 gauge (80 μm) nichrome wire which surrounded the processor, battery, memory, and even the sensory circuitry. The authors in [87] have proposed a secure design flow for securing ICs against the scan based side channel analysis attacks. To have a secure design, rather than using the full custom layout with the iterative design process, the authors have proposed a few modifications on the logic synthesis, the place and route step, and the stream out step to have a secure design flow. In [88], a secure design for test has been developed for the pipelined Advanced Encryption standard. The proposed method provides a good tradeoff between security

and testing of crypto ICs, it provides a high test quality, and good fault diagnosis while protecting the key of the implemented crypto hardware. In [89-90], various secure scan based designs for test are discussed and a secure design for a test technique is proposed by using a popular hash function called CRC-MAC (cyclic redundancy check-message authentication algorithm) which performs a stream oriented operation on the input stream data. The authors have implemented the CRC-MAC algorithm to have a secure design for a test solution. In [91], Chang et.al. have discussed the watermarking of ICs as a countermeasure against IP fraudulence by unauthorized foundries. A secure solution is proposed in the above paper which protects against the counterfeiting of ICs by foundries, the above watermarking scheme bridges the gap between IP protection and IP management. The increased area overhead by the proposed method has also been reduced by the nearest neighbor algorithm. The authors in [92] have proposed scan based side channel attacks against the symmetric stream ciphers, in which the attacker have inserted the scan chains in the Light Encryption Device (LED) stream cipher. The 64-bit key was recovered by just applying 73 different plaintext vectors.

6.3 Proposed Method

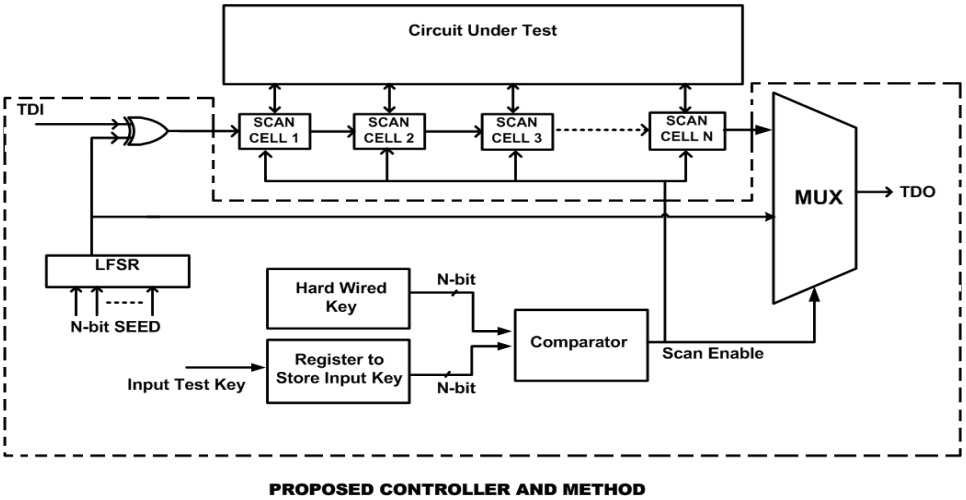


Figure 29: Proposed Architecture for controlled access

In the proposed method a secure controller is used to control the transitions from an insecure mode to a secure mode. The controller consists of a hardwired key comparator as shown in figure 29. To protect the internal circuit under test against attacks using the scan chain, direct access to the circuit under test is not provided in the insecure mode of testing. There are two modes of operation, one being the vulnerable or insecure mode in which the key is not provided. The scan chain in this mode shifts random data from randomly seeded LFSR as shown in figure 29. The input test vector from TDI is XOR-ed with the pattern from the LFSR and consequently, the input test vector at TDI needs to be modified accordingly based on the pattern generated by the LFSR. In the proposed method a different LFSR has been used if the user is not verified, the purpose of using the different LFSR is that attacker is not able to build LFSR from known patterns by Berlekamp Massey algorithm. When the device is switched from the vulnerable mode to the secure mode, the following operations which take place are summarized below.

a) A reset signal is applied to the LFSR to erase the contents of the flip flop.
b) The test key is compared with the hardwired key embedded in the controller at the time of manufacturing.
c) Once the test-key is verified, the scan chain is granted access to the circuit under test. The test patterns are XOR-ed with the output of LFSR and then applied to the circuit under test.
d) After the verification of the key, the user is asked to seed the LFSR; if the seeding of the LFSR is wrong, it produces the wrong test patterns

If the test key is not right, the randomly seeded LFSR delivers random patterns to mislead the attackers. The reset signal applied before switching to the secure mode from the vulnerable mode ensures that any previous patterns from the LFSR obtained are cleared.

6.4 Measurement Results

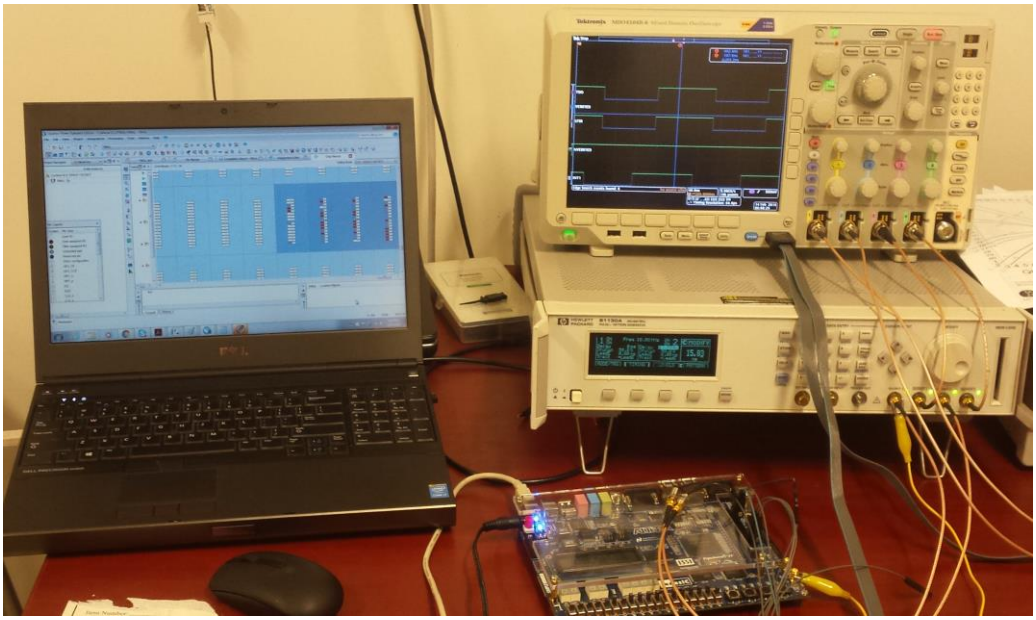


Figure 30: Measurement setup for the proposed architecture

The above proposed method was implemented on the Altera FPGA DE2 115 board as shown in figure 30. The system illustrates the area of the proposed method on the chip planner of the Altera Board and the measurement set-up. The hardwired key was implemented using switches on the FPGA board and the user key was provided through the input port. When the input key was right as compared to the hardwired key, a signal was generated which allowed the circuit to enter the secure mode of operation. In the secure mode, the input test patterns were XOR-ed with the LFSR data and then applied to the CUT. This is needed to reduce the probability of reverse engineering through input and output data analysis. As the input test pattern was applied, the coded output was seen at the output as shown in figure 31. However, as shown in figure 33, when the user is not verified, access to the main scan chain and the circuit-under test is disabled and the semi-random data from the randomly seeded LFSR is shifted out through the TDO pin. However, the variation is observed when the length of the implemented LFSR is increased for the purpose of high security.

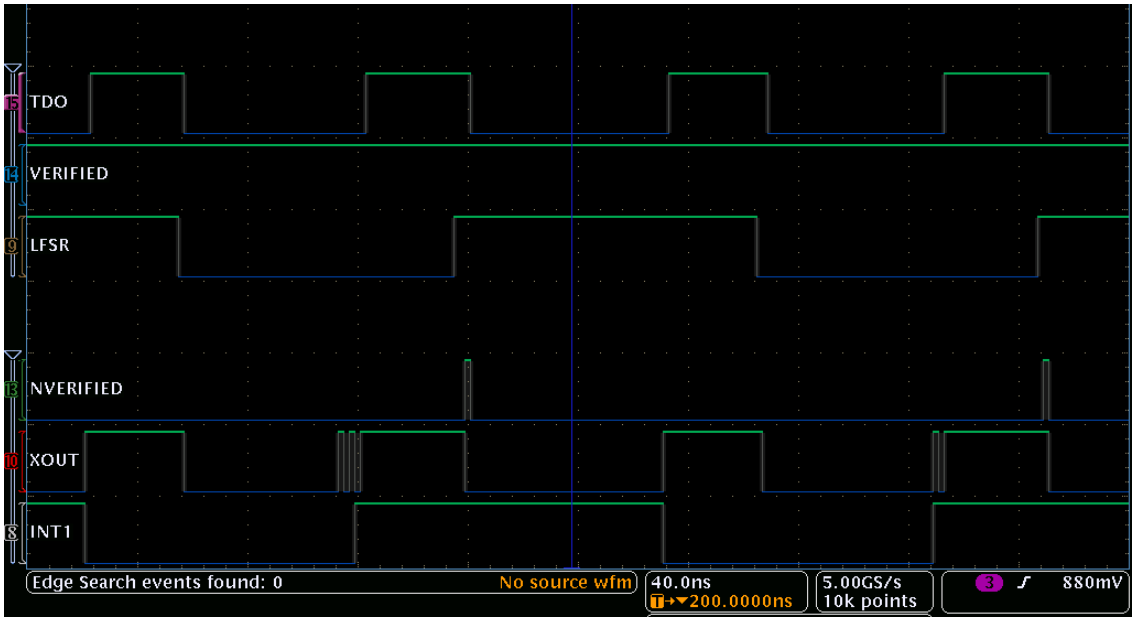


Figure 31: Waveform if user is granted access to scan chain

The proposed solution is compared with the existing solutions in literature in Table 3. To switch from the insecure mode to the secure mode and vice versa, a controller is proposed which is shown in Figure 32.

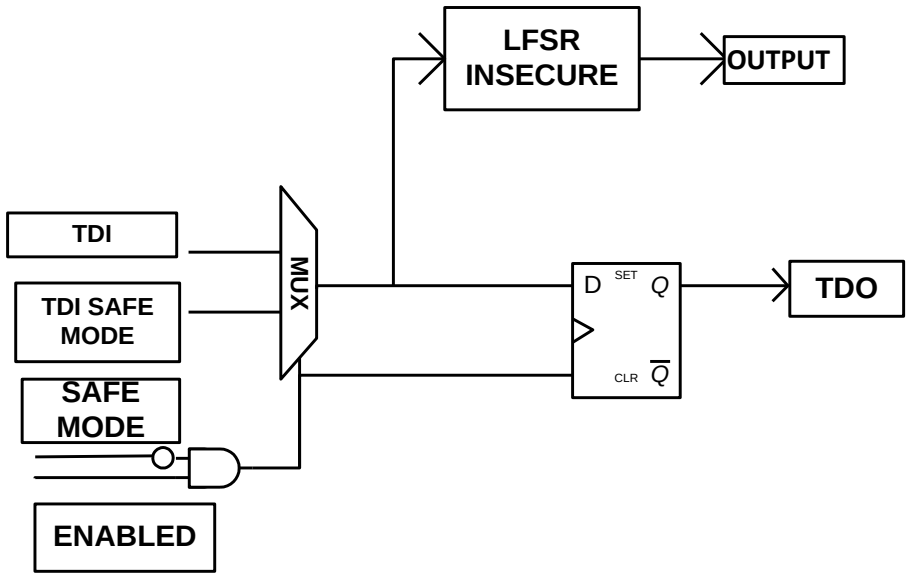


Figure 32: Proposed Secure controller to switch modes

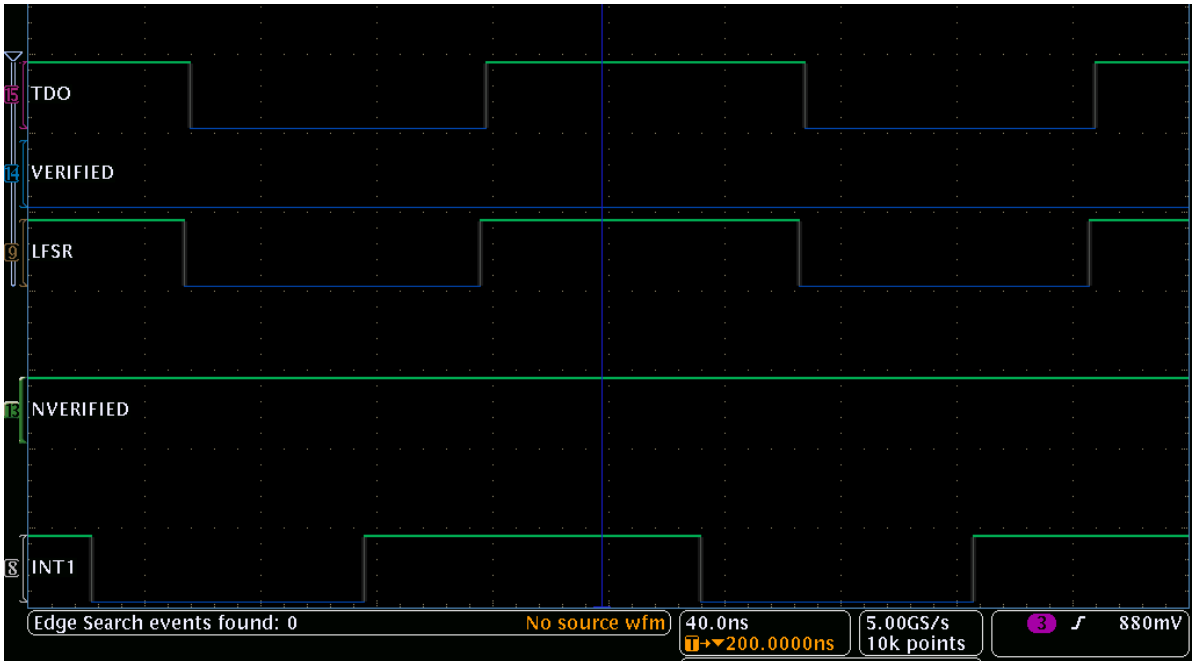


Figure 33: Waveform to support if the user is not granted access

#Normal Scan chain no of gates and flip flops	#LCSS overhead on normal scan chain (%) [Ref 65]	#State Dependent Architecture overhead (%) [Ref 66]	#Proposed Architecture area gates	#Proposed Architecture Area Overhead
23815	18.1	16	750	3.14
20705	15.6	8.1	750	3.62
17793	18.1	2.1	750	4.21
10369	19.2	1.5	750	7.23
8620	22.4	1.0	750	8.70

Table 3: Area overhead and comparison with existing solutions

6.5 Conclusions

The proposed solution in this section reduces the area overhead as compared to the existing solutions as shown in table 3. The proposed solution checks the authenticity of tester at two levels.

Chapter 7

Summary, Conclusions and Future Work

Scan based design as a test method is an effective technique that provides strong controllability and observability which, in turn, provides a high fault coverage for the circuit under test. Using scan chains for testing opens the opportunity for a scan-based attack. In this thesis, three solutions for different applications have been proposed to protect a circuit-under-test against scan-based attacks.

A fully testable circuit may not be secure as it grants the full controllability and observability of the circuit nodes to the tester. To address the trade-off between security and testability, an LFSR based solution was proposed. The proposed solution operates in two modes (a) the secure mode of testing and (b) the test mode or the insecure mode of testing. In the secure mode, the circuit under test is isolated from the scan chain and even an indirect access is not provided to the circuit under test. An embedded LFSR was used to generate the test patterns for the circuit under test. Denying access to enter any input pattern in the secure mode of testing wards off the opportunity to mount any successful attacks on the circuit under test. In the insecure mode of testing, access to the circuit under test is given but the access to the key is disabled in this mode of testing.

In the second method, a built-in self-test solution for the cores embedded in a system on chip (SoC) has been proposed. The proposed solution does not need an advanced external tester to perform the tests on the system-on-chip. If the circuit is tested at the manufacturing stage, full access to the device-under-test is granted. On the contrary, if the device is tested in-field, access to the CUT is disabled.

In the third method, a secure control test solution is presented. In this method, a test key is used to grant access to the CUT. If the test key is verified, then access to the main scan chain is given, else random data is shifted out from a random pattern generator to mislead the attacker.

With the emergence of new technologies, new test solutions have to be developed to ensure security and prevent security threats against hardware through the scan architecture. TSV based 3D stacked ICs are expected to present significant performance improvements compared to the conventional 2D ICs. The potential of this new technology will not be fully materialized if the security related issues are not properly addressed. A hardware security solution against side-channel attacks and scan-based attacks for 3D ICs is a great research topic for future work.

REFERENCES

[1] Gordon E. Moore, “Cramming more components onto integrated circuits”, Electronics, vol 38, no 8, pp 114-117, 1998.

[2] A.C. Stover, ATE: Automatic Test Equipment, New York, Mc Graw Hill, 1984.

[3] N.G. Einspruch, VLSI Handbook, Orlando, Florida: Academic Press, 1985.

[4] A.K. Stevens, Introduction to Computer Testing, Reading Massachusetts: Addison- Wesley, 1986.

[5] K.P. Parker, Integrated Design and Test: Using CAE Tools for ATE Programming, Los Alamitos, California: IEEE Computer Society Press, 1987.

[6] J. Bateson, In Circuit Testing, New York: Van Nostrand Reinhold Company, 1985.

[7] L. Geppert, Technology 1998 Analysis and forecast: IEEE Solid State Spectrum, vol 35, no 1, pp 23-28, 1998.

[8] M. Abramovici, M.A. Breuer, and A.D. Friedman, Digital System Testing and Testable Design, IEEE Press, Piscataway, New Jersey, 1994.

[9] M.L. Bushnell and Vishwani D Agrawal, Essentials of Electronic Testing for Digital Memory and Mixed Signal VLSI Circuits, Springer Science, New York 2000.

[10] Laung-Terng Wang, Cheng-Wen Wu and Xiaoqing Wen, VLSI Test Principles and Architecture, Morgan Kaufmann Series in System on Silicon, Elsevier, 2006.

[11] C.E. Stroud, A Designer’s Guide to Built in Self Test, Kluwer Academic, Norwell, MA, 2002.

[12] C Stroud, J.Emmert, and J.Batley, A new bridgning fault model for more accurate fault behavior, in Pro Automatic Test Conference (AUTOTESTCON), pp. 481-485, September 2000.

[13] A.J. Van de Goor, Testing Semiconductor Memories: Theory and Practise, John Wiley and Sons, Chichester, U.K. 1991.

[14] S.W. Golomb, Shift Register Sequence, Aegan Park Press, Laguna Hills, CA 1982.

[15] P.H. Bardell, W.H. Mc Anney, and J. Savir, Built in Test for VLSI: Pseudo-random Techniques, John Wiley and Sons, Somerset, New Jersey, 1987.

[16] W.W. Peterson and E.J. Weldon Jr. Error Correcting Codes, MIT Press, Cambridge, MA,1972

[17] C.L. Chen, Exhaustive test pattern generation using cyclic codes, IEEE Transactions on Computers, vol 37, no 3, pp. 329-338, 1987.

[18] L.T. Wang and E.J. Mc Cluskey, Circuits for pseudo-exhuastive test pattern generation, IEEE Transactions on Computer Aided Design, vol 7, no 10 pp. 1068-1080, 1988.

[19] L. T. Wang and E.J. Mc Cluskey, Linear feedback shift register design using cyclic codes, IEEE Transactions on Computers, vol.37, no 10, pp.1302-1306, 1987.

[20] E.J. Mc Cluskey, Built in Verification test, in Proc International Test Conference, pp.183-190, November 2000.

[21] E.J. Mc Cluskey, Logic Design Principles: With Emphasis on Testable Semiconductor Circuits, Prentice Hall, Englewood, Cliffs New Jersey, 1986.

[22] J. Wakerly, Digital Design Principles and Practices, 3ed Edition, Prentice Hall, Englewood Cliffs, New Jersey, 2000.

[23] TW Williams, W. Daehn, M. Gruetzner and C.W. Starke, Aliasing errors in signature analysis registers, IEEE Design Test Computers, vol 4, no 4, pp.34-35, 1987.

[24] CK Chin and E.J. Mc Cluskey, Test Length for pseudo random Testing, IEEE Transactions on Computers, vol 36, no 2, pp. 252-256, 1987.

[25] J. Savir, G.S. Ditlow, and P.H. Bardell, Random pattern Testability, IEEE Transactions on Computers, vol 33, no1, pp. 79-90, 1984.

[26] H.D. Schurmann, E. Lindbloom and R.G. Capenter, The weighted random test pattern generator, IEEE Transactions on Computers, vol 24, no 7, pp.695-700, 1975.

[27] J.A. Waicukauski, E. Lindbloom, E.B. Eichelberger, and O.P. Forenza, WRP: A method for generating weighted random test patterns, IBM J.Res. Dev, vol 33, no 2, pp. 149-161, 1989.

[28] R.Kapur, S. Patil, T.J. Snethen, and T.W. Williams, Design for an efficient weighted random pattern generation system, in Proc in International Test Conference, pp. 491-500, 1994.

[29] L. Lai, J.H. Patel, T. Rinderknecht, and W.T. Cheng, Hardware Efficient LBIST with complementary weights, in Proceedings International Test Conference on Computer Design, pp. 479-481, 2005.

[30] M. Bershteyn, Calculation of multiple sets of weights of weights for weighted random testing in Proceeding of International Test Conference, pp. 1031-1040, 1993.

[31] E.J. McCluskey and S. Bozorgui- Nesbat , Design for Autonomous Test, IEEE Transactions on Computers, vol 30, no 11, pp. 860-875, 1981.

[32] S. Bozorgui-Nesbat and E.J. Mc Cluskey, Structured design for testability to eliminate test pattern generation, in Digest of Papers, Fault Tolerant Computing Symposium, pp. 158-163, 1980.

[33] O. Patashnik, Circuit Segmentation for Pseudo Exhaustive Testing, Technical Report (CRC-TR) vol 83, no 14, Center for Reliable Computing, Stanford University, 1983.

[34] N.K. Jha and S.K. Gupta, Testing of Digital Systems, Cambridge University Press, Cambridge UK, 2003.

[35] K. Furuya and E.J. Mc Cluskey, Test Pattern test capabilities of autonomous TPG circuits, in Proceedings of International Test Conference, pp. 704-711, 1991.

[36] P. Girard, Survey of Low power testing of VLSI circuits, IEEE Design of Test Computers, 82-92, 2002.

[37] MA Breuer and NK Kanda, Simplified Delay Testing for LSI Circuit Faults, U.S. Patent No. 4, 672, 307, 1987.

[38] R.A. Frohwerk, Signature Analysis: A new digital field service method, Hewlett Packard, vol 28, pp. 2-8, 1977.

[39] N. Benowitz, D.F. Calhoun, G.E. Alderson J.E. Bauer, and C.T. Joeckel, An Advanced fault isolation system for digital logic, IEEE Transactions on Computers, vol 24, no 5, pp. 489-497, 1975.

[40] S.Z. Hassan and E.J. McCluskey, Increased fault coverage through multiple signatures, in Digest of Papers, Fault Tolerant Computing Symposium, pp. 354-359, 1984.

[41] L.T. Wang and E.J. Mc Cluskey, Concurrent built in logic block observer (CBILBO) in Proceedings of International Symposium of Circuits and Systems, vol 3 pp. 1054-1057, 1986.

[42] J.P. Hayes, Transition Count Testing of combinational logic circuits, IEEE Transactions on Computers, vol 25, no 6, pp 613-620, 1976.

[43] J. Savir and W.H. Mc Anney, On the masking probability with ones count and transition count, in Proceedings of International Test Conference, pp. 111-113, 1985.

[44] IEEE Std. 1149.6-2003, IEEE Standard for Boundary Scan Testing of Advance Digital Networks, IEEE Press, New York 2003.

[45] IEEE Std. 1149.1-2001 IEEE Standard Test Access Port and Boundary Scan Architecture, IEEE Press, New York, 2001.

[46] J.C. Chan, Boundary Walking Test: An accelerated scan method for greater system reliability, IEEE Transactions on Reliability, vol 41, no 4, 496-503, 1992.

[47] Y. Kim, H.D. Kim, and S. Kang, A new maximal diagnosis algorithm for interconnect test, IEEE Transactions on Very Large Scale Integration Systems, vol 12, no 5, pp. 532-537, 2004.

[48] IEEE Std. 1500-2005, IEEE Standard for Embedded Core Test, IEEE Press, New York, 2005.

[49] Y. Zorian, Test Requirements for embedded core based systems and IEEE P1500, in Proceedings IEEE International Test Conference, pp. 191-199, 1997.

[50] C.W. Wu, J.F. Li and C.T. Huang, Core based system on chip testing: Challenges and opportunities, Journal of Chinese Institution of Electronic Engineering, vol 8, no 4, pp 335-353, 2001.

[51] B. Yang, K. Wu, and R. Karri, Scan based side channel attack on dedicated hardware implementations of data encryption standard in Proceedings of the International Test Conference pp. 339–344, 2004.

[52] P. Kocher, J. Jaffe, and B. Jun, Differential power analysis, in 19th Annual International Cryptology Conference on Advances in Cryptology, pp. 388–397, 1999.

[53] P.C. Kocher, Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," in 16th Annual International Cryptology Conference on Advances in Cryptology, pp. 104–113, 2001.

[54] D. Boneh, R.A. Demillo, and R.J. Lipton, On the importance of checking cryptographic protocols for faults, in Eurocrypt, pp. 37–51, 1997.

[55] E. Biham, and A. Shamir, Differential fault analysis of secret key cryptosystems, in 17th Annual International Cryptology Conference on advances in Cryptology, pp. 513–527, 1997.

[56] G. Sengar, D. Mukhopadhyay, and D.R. Chowdhury, Secured Flipped Scan-Chain Model for Crypto Architecture, in IEEE Transactions on Computer-Aided design of Integrated Circuits and Systems, vol.26, no. 11, pp. 2080-2084, 2007.

[57] B. Yang, K. Wu and R. Karri, Secure scan: a design-for-test architecture for crypto chips, in 42nd Annual Conference on Design Automation, pp. 135–140, 2005.

[58] B. Niewenhuis, R.D. Blanton, M. Bhargava and K. Mai, Scan PUF A low overhead Physically Unclonable Function from Scan chain Power up states, in International Test Conference, pp. 1-8, 2013.

[59] Y. Zheng, A.R. Krishna, and S. Bhunia, Scan PUF: Robust Ultralow overhead PUF using scan chain, in 18 th Asia and South Pacific Design and Automation Conference, pp. 626-631, 2013.

[60] Y. Zheng, F. Zhang, and S. Bhunia, DScan PUF: A delay based Physically Unclonable Function built into scan chain, in IEEE Transactions on Very Large Scale Systems (VLSI) Systems, 2015, in press.

[61] K. Hafner, H.C. Ritter, T.M. Schwair, S. Wallstab, M. Deppermann, J. Gessner, S. Koesters, W.D. Moeller, and G. Sandweg, Design and test of an integrated cryptochip, in IEEE Design and Test of Computers, vol.8 , no.4 , pp. 6–17, 1991.

[62] B. Yang, K. Wu, and R. Karri, Secure scan: a design-for-test architecture for crypto chips, in IEEE Transactions on Computer Aided Design of Integrated Circuits and Systems, vol.25, no. 10, pp. 2287-2293, 2006.

[63] D. H'ely, M.L. Flottes, F. Bancel, B. Rouzeyre, N. B'erard, and M. Renovell, Scan design and secure chip, in 10th IEEE International On-Line Testing Symposium IOLTS, pp. 219-224, 2004.

[64] J. Lee, M Tehranipoor, C Patel, and J Plusquellic, Securing Scan Design using Lock and Key Technique, 20th international Symposium on Defect and Fault Tolerance in VLSI Systems, pp. 51-62, 2005.

[65] J. Lee, M. Tehranipoor, and J. Plusquellic, A low-cost solution for protecting IPs against scan-based side-channel attacks, in 24th IEEE VLSI Test Symposium, 2006.

[66] R Nara, H Atobe, Y. Shi, N Togawa, M. Yanagisawa, and T Ohtsuki, State Dependent changeable Scan Architecture against scan based side channel attacks, in Proceedings of the IEEE International Symposium on Circuits and Systems, pp. 1867-1870, 2010.

[67] D. Hely, F. Bancel, M. L. Flottes, B. Rouzeyre, A Secure Scan Design Methodology, in Proceedings of Design Automation and Test in Europe, pp. 1-2, 2006.

[68] Ankit Mehta, Darius Saif, and Rashid Rashidzadeh, A hardware Security Solution against Scan-based attacks, in IEEE Symposium on Circuits and Systems, pp. 1698-1701, 2016.

[69] R. Zimmermann, A. Curiger, H. Bonnenberg, H. Kaeslin, N. Felber , and W. Fichtner , A 177 Mbit/s VLSI implementation of the international data encryption algorithm, in IEEE Journal of Solid-State Circuits ,vol.29, no.4 , pp. 303-307, 1994.

[70] Advanced Encryption Standard (AES), Federal Information Processing Standard Publication, FIPS, PUB-197, U.S. National Institute of Standards and Technology.

[71] J.D. Goli, New methods for Digital generation and post processing of random data, in IEEE Transactions on Computers, vol 55, pp. 1217-1229, 2006.

[72] Cheng Xing, Sungju Park, and Ji Zhao, Analysis of recent secure scan test techniques, Journal of Software Engineering and Applications, vol 9, pp. 91-101, 2016.

[73] J.H. Song, T.J. Sung, J.H. Jung, and S.J. Park, An efficient Technique to protect AES Secret key from scan test channel attacks, in Journal of Semiconductor Technology, vol 12, pp. 286-292, 2012.

[74] D. Mukhopadhyay, S. Banerjee, D. RoyChowdhury, B.B. Bhattacharya, Cryptoscan:A secured scan chain architecture, in Proceedings of Asian Test Symposium, pp. 348-353, 2005.

[75] David Hely, F. Bancel, M. -L., B Rouzeyre , A secure scan design method , in Proceedings of Design Automation Conference, pp. 1177-1178, DATE 2006

[76] M Agrawal, S. Karmakar, D. Saha, and D. Mukhopadhyay, Scan based side channel attacks on stream ciphers and their counter measures, in INDOCRYPT LNCS, pp.226-238, 2008.

[77] R. Nara, K. Satoh, M. Yanagisawa, T. Ohtsuki, and N. Togawa, Scan based side channel attack against RSA Cryptosystems using scan signatures, in IEICE Transactions, vol 93, pp. 2481-2489, 2010.

[78] R. Nara, N. Togawa, M.Yanagisawa, T.Ohtsuki, Scan based attack against elliptic curve cryptosystems, in 15 th Asia and South Pacific Design Automation Conference, pp.407-412, 2010.

[79] A. Barenghi, G. Bertoni, E. Parrinello, and G. Peloski, Low voltage fault attacks on the RSA Cryptosystems, in Proceedings Workshop on Fault Diagnosis and Tolerance in Cryptography, pp.23-31, 2009.

[80] A. Barenghi, G.M. Bertoni, L. Breveglieri, M.Pellicioli, and G. Peloski, Low Voltage Fault attacks to AES, in Proceedings International Symposium on Hardware Oriented Security and Trust, pp.7-12, 2010.

[81] N. Selmane, S. Guilley, and J.L. Danger, Practical set up time Violation attacks on AES, in Proceedings European Dependable Computing Conference, pp.91-96, 2008.

[82] A. Barenghi, C. Hocquet, D. Bol, F.X. Standaert, F. Regazzoni, and I. Koren, Exploring the feasibility of subthreshold devices through an example of a 65nm AES Implementation, in Proceedings Workshop on RFID Security and Privacy, pp.48-60, 2011.

[83] Y.Zorian, E.J. Marinissen, and S. Dey, Testing Embeded-Core Based System Chips, *Proc. International Test Conference*, pp.130-143, 1998.

[84] Y. Zorian, S. Dey, and M. Redgers, Test of future System-on-chips, *Proc. International Test Conference*, pp.392-398, 2000.

[85] D. Hely, F. Bancel, M.L. Flottes, and B.Rouzeyre, Test control for secure scan, in European Test Symposium (ETS), pp.190-195, 2005.

[86] R. Anderson, M.Kuhn, Tamper Resistance- a cautionary note, in Proc. Of the second USENIX workshop on electronic commerce, vol 2, pp.1-11, 1996.

[87] K. Tiri, and I. Verbauwhede, A VLSI design flow for secure side-channel attack resistant ICs, in Proc. Design Automation Test Conference, vol 3, pp. 58-63, 2005.

[88] Y. Shi, N. Togawa, M. Yanagisawa, and T.Ohtsuki, Design for secure test- a case study on pipelined advanced encryption standard, in IEEE International Symposium on Circuits and Systems, pp.149-152, 2007.

[89] M. Gomulkieciwz, M. Nikodem, and T. Tomczak, Low cost and universal secure scan: a design architecture for crypto chips", in International Conference on Dependability of computer systems, pp.282-288, 2006.

[90] M Tehranipoor, C Wang, Introduction to Hardware Security and Trust, Springer Science and Business Media, 2011.

[91] C.H. Chang, A. Cui, Synthesis for testability watermarking for field authentication of VLSI intellectual property, in IEEE Transactions on Circuits and Systems I: Regular papers: vol 57, no 7, pp.1618-1630, 2010.

[92] M. Fujishiro, Y. Shi, M. Yanagisawa, and N. Togawa, Scan based side channel attack against symmetric key ciphers using scan signatures, in IEEE international conference on Electron Devices and Solid State Circuits, pp.309-312, 2015.

VITA AUCTORIS

NAME:	Ankit Mehta
PLACE OF BIRTH:	New Delhi, India
EDUCATION:	Jaypee Institute of Information Technology, B.Tech., Noida, UP-India, 2014
	University of Windsor, M.Sc., Windsor, ON, 2016