Securing IEEE P1687 On-chip Instrumentation Access using PUF

Naini Satheesh

Department of Electronics and Communication Engineering

National Institute of Technology Rourkela

Securing IEEE P1687 On-chip Instrumentation Access using PUF

A thesis submitted in partial fulfilment

of the requirements of the degree of

Master of Technology

in

Electronics and Communication Engineering

(Specialization: VLSI Design and Embedded Systems)

by

Naini Satheesh

ROLL NO: 214EC2161

Under supervision of

Prof. Kamalakanta Mahapatra

May 2016

Department of Electronics and Communication Engineering

National Institute of Technology Rourkela

Department of Electronics and Communication Engineering
National Institute of Technology Rourkela

Prof. Kamalakanta Mahapatra

May 31, 2016

Supervisors' Certificate

This is to certify that the work presented in the thesis entitled *Securing IEEE P1687 On-chip Instrumentation Access using PUF* submitted by *Naini Satheesh*, Roll Number 214EC2161, is a record of original research carried out by him under our supervision and guidance in partial fulfilment of the requirements of the degree of *Master of Technology* in *VLSI Design and Embedded Systems.* Neither this thesis nor any part of it has been submitted earlier for any degree or diploma to any institute or university in India or abroad.

Prof. Kamalakanta Mahapatra

Dedicated to

My beloved lucky

Declaration of Originality

I, *Naini Satheesh,* Roll Number *214EC2161* hereby declare that this thesis entitled *Securing IEEE P1687 On-chip Instrumentation Access using PUF* presents my original work carried out as a master student of NIT Rourkela and, to the best of my knowledge, contains no material previously published or written by another person, nor any material presented by me for the award of any degree or diploma of NIT Rourkela or any other institution. Any contribution made to this research by others, with whom I have worked at NIT Rourkela or elsewhere, is explicitly acknowledged in the thesis. Works of other authors cited in this thesis have been duly acknowledged under the section "Reference". I have also submitted my original research records to the scrutiny committee for evaluation of my thesis.

I am fully aware that in case of any non-compliance detected in future, the senate of NIT Rourkela may withdraw the degree awarded to me on the basis of present thesis.

May 31, 2016

NIT Rourkela

Naini Satheesh

Acknowledgement

I would like to thank my project supervisor Dr. K. K. Mahapatra, Professor and Head of the Department, Electronics and Communication Engineering, NIT Rourkela for giving me the opportunity to work under him and lending every support at every stage of this project work. I truly appreciate and value him esteemed guidance and encouragement from the beginning to the end of this thesis. I am indebted to his for having helped me shape the problem and providing insights towards the solution.

I am also greatly indebted to Mr. Sudeendra Kumar, a Ph.D. scholar at NITRKL, for introducing the exciting topics in this domain to me and helped me a lot in every situation.

I express my respects to Prof A. k Swain Prof. D. P. Acharya, Prof. P. K. Tiwari and Prof. N. Islam, Prof. Shantanu Sarkar, Prof. Sougata Kar for teaching me and also helping me how to learn.

I would like to thank all my friends and especially my classmates for all the thoughtful and mind stimulating discussions we had, which prompted us to think beyond the obvious. I've enjoyed their companionship so much during my stay at NIT Rourkela.

Finally, I am forever indebted to my parents and sisters for their love, understanding, endless patience and encouragement when it was most required.

May 31, 2016

NIT Rourkela

Naini Satheesh

Roll Number: 214EC2161

Abstract

As the complexity of VLSI designs grows, the amount of embedded instrumentation in system-on-a-chip designs increases at an exponential rate. Such structures serve various purposes throughout the life-cycle of VLSI circuits, e.g. in post-silicon validation and debug, production test and diagnosis, as well as during in-field test and maintenance. Reliable access mechanisms for embedded instruments are therefore key to rapid chip development and secure system maintenance.

Reconfigurable scan networks defined by IEEE Std. P1687 emerge as a scalable and cost-effective access medium for on-chip instrumentation. The accessibility offered by reconfigurable scan networks contradicts security and safety requirements for embedded instrumentation.

Embedded instrumentation is an integral system component that remains functional throughout the lifetime of a chip. To prevent harmful activities, such as tampering with safety-critical systems, and reduce the risk of intellectual property infringement, the access to embedded instrumentation requires protection. This thesis provides a novel, Physical Unclonable Function (PUF) based secure access method for on-chip instruments which enhances the security of IJTAG network at low hardware cost and with less routing congestion.

Keywords: **IEEE 1687-2014, Physical Unclonable Function, Hardware Security.**

Contents

List of figures

List of Tables

Chapter 1
Introduction

1.1 Introduction:

Over the last decade the increased complexity and transistors count per chip has been increasing exponential rate. This development leads integrate more and more functionalities with in the chip and facilities the use of electronic devices in all branches of industry and in everyday life. The verification techniques and design methodologies has to be revised to facilitate this growth in VLSI industry. As the design complexity grows, it has become challenging to validate and verify the design so as to reduce the number of errors per design.

As the technology grows i.e transistor size shrinks causing the chips prone to manufacturing defects and process variations effects the on-field operations. The adverse effects also occur due to aging and soft errors. To meet the reliable operation throughout lifespan, the design constrains must deal with the decay of is reliability.

To facilitate the development and improve the product quality, VLSI chips incorporating on-chip instrumentation to meet the requirements or targets for time to market, maintainability, chip quality and reduce the cost of testing. This is also called as embedded instrumentation. Embedded instrumentation provides the in-field system maintenance and pre-production testing which are post-silicon validation structures, trace buffers, BIST structures, and on-chip sensors for system monitoring. Traditionally, scan networks are employed as a test mechanism schemes and extended as reconfigurable scan networks, to provide scalable and cost-effective mechanism for on-chip instruments. The embedded instruments are increasing the controllability and observability of chip internals.

Moreover, the improved controllability and observability of embedded instruments has conflict with safety requirements and security of chip internals. This requires the efficient technique to improve the security of chips.

1.2 On-chip Instrumentation:

On-chip instruments are module integrated with in the chip to improve the controllability and observability of chip internals so that to get the high test quality, reduce test time and cost. As the functional complexity of VLSI design grows, a very high amount of on-chip instruments is required that supports validation, verification, debug as well as in-field system monitoring and system maintenance.

1.2.1 Test & Measurement market trends:

Figure1.1 shows the evolutionary trends in the test and measurement unit.

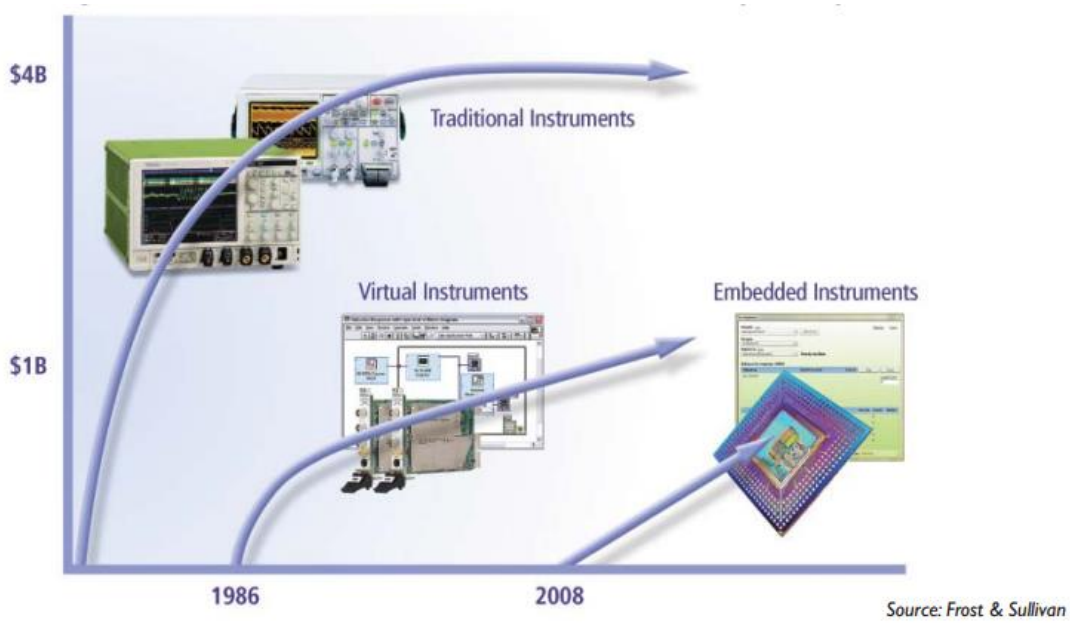

Figure 1.1 Test & Measurement trends

Traditional Instrumentation:

In the early days, the traditional instruments are used for test /& measurement. These instruments are pre-defined hardware structures used for specific type of analysis, which are bulk in nature. Examples of Traditional instruments are oscilloscopes, millimeters, logic analyzers and signal generators. These are expensive.

Virtual Instrumentation:

Virtual instrumentation is developed in the mid-1980s, which are user defined measurements systems. These are deals with customizable software and specific instrumentation hardware. Examples of virtual instrumentation is like National Instruments' LabVIEW.

The major difference between virtual instrumentation and traditional instrumentation systems is the software, which can be programmable. By using virtual instrumentation, the testing cost is reducing because the expensive traditional hardware components are replaced by software based systems. A special type of dedicated hardware and software is required for virtual instrumentation.

Embedded Instrumentation:

Embedded instruments are the blocks inserted with in modules to measure and test the designs. This is also called as on-chip instrumentation. Examples of on-chip instruments are trace buffers, LBIST, MBIST etc. These instruments are embedded mainly for reducing the test cost and time.

1.3 On-Chip Instrumentation Components:

On-chip instruments are used in various level of chip which are during production test, pre-silicon validation and maintenance.

Post-silicon validation & Debug:

Post-silicon validation and debug are the first steps done after prototype chips taped-out. During the post silicon validation, the chips tests in a virtual environment. Post-silicon validation identifies problems which were missed in pre-silicon verification due to low activation probability, inherent design indeterminism i.e. multiple clock domains, asynchronous communication, signal integrity issues and process variations. The diagnosis of complex circuits is hard task, even if the validation fails during the validation process but it is observed that the chips are working properly on ATE. The chips are added specific type on-chip instruments which improves the controllability and observability for post-silicon validation. Scan chains are included in the designs to observe the internal logic states of the system. Embedded logic analyzers and trace buffer are used observation of system states at high speed. Specialized recorders are used to validate the state at microarchitecture level in advanced microprocessor designs.

Volume production & Test:

After solving the all design errors, the volume production is beginning. Each and every chip goes to various production tests on ATE. The volume production tests are wafer test, package test and acceptance tests. The volume production gives the assurance about the quality of product and prevent the defective chips to be shipped to end users.

The instruments used to facilitate the volume production and test are DFT, wrapper cells, compressors and analog buses. Design for Test (DFT) infrastructures are used to

improve the testability and reduce test time. Wrapper cells are used to test the third party core-modules used in the design. Test pattern compressors are used to reduce the volume test data sizes.

Maintenance:

After production test, the chips are going various test to guarantee the on-field operations. The devices are exposed to various stress factors, including high ambient temperature, mechanical stress, electromagnetic interference, particle strikes, and aging processes.

To guarantee reliability throughout the lifetime of a chip, various methods for in- field monitoring, error correction, test, diagnosis and repair are adopted. Such techniques are often supported with on-chip instrumentation. Silicon odometers, workload meters, stability checkers are used for aging effects. Logical BIST and Memory BIST are used for checking for logical designs and memory modules in chips. These instruments are accessed with JTAG and IJATG structures.

1.4 Cost effective access to on-chip instrumentation:

The most commonly used interface for accessing embedded instrumentation is JTAG interface. JTAG interface is a 4-wire TAP controller based interface defined by IEEE std. 1149.1. Initially, the goal of JTAG is to test the interconnections of Printed circuit boards. But due to low cost and efficiency of JTAG interface, it is widely adopted to accessing the on-chip instruments.

1.5 Motivation:

Good observability and controllability of chip internals is requisite for low time to market, high product quality, as well as system reliability and maintainability. However, the accessibility of chip internals through on-chip instruments contradict with security and safety requirements.

The security of reconfigurable scan networks is crucial to prevent from side attackers such as unauthorized usage, sabotage or IP theft. The attacker may use the scan architecture to get the stored secret keys. The system operations can be altering by fault injection or by performing illegal operations. Embedded instruments may expose the sensitive data which

are protected in the system. The configurable scan networks are prone to the side channel attacks such as electromagnetic leaks, power analysis, and timing analysis.

Different levels of scalable architecture are required for on-chip operations, volume production and product development. During the production test, diagnosis and volume test, for increasing the product quality and low time market that the chip should have high controllability and observability. However, during maintenance and on-chip operations, the chip internals accessibility should be restricted for safety and secure reasons. If the accessibility is not restricted, then there may causes tampering or IP theft. Moreover, different user may require to have different level of accessibility depend on the place of usage. During the manufacturing and assembly test on the ATE, the chip should full accessibility of internals. But during maintenance and operation limited access should provide to prevent the unauthorized persons.

It is the fact that any security scheme can be broken with enough time and resources that is absolute security for designs is impossible. There is always trade-off between the cost, flexibility and security for scan based designs. The existing protection schemes are challenge-response protocol authentication, AES encryption, and key generation using Hash functions. In these mechanisms, it is assumed that the secret key is shared between the authorized persons only. If the secret key is known to intruder, then the full accessibility of chip is possible.

1.6 Organization of the Thesis:

The following section gives the overview of how the dissertation is structured:

- Chapter 2: This chapter gives the existing protection schemes available for IJTAG to prevent from the attacker. The advantage and disadvantage of these schemes also given in the chapter.
- Chapter 3: This chapter gives the fundamental of IEEE P1684 standards. The functionality of TAP controller, SIB cell, Test Data Register are explained. The need for reconfigurable scan networks are given.
- Chapter 4: This chapter gives the fundamental of Physical Unclonable Functions. How the PUFs are used in authentication purpose and to generate the challenge response pairs. And also discussed about various types of PUF structures and its functionality.

- Chapter 5: This chapter proposes a design for Authorized Access Management of on-chip instrument access and control through the TAP access port. And modified Ring Oscillator PUF is also explored here.
- Chapter 6: This chapter gives the implantation details of proposed design and experimental results are compared with the existing access mechanisms. Mathematical calculations for brute force attack is presented in this chapter.
- Chapter 7: This chapter gives the concluding remarks for this dissertation.

Chapter 2

Literature Survey

IEEE P1687 (IJTAG) standard is a well know mechanism for accessing of embedded instruments. Although IJTAG gives the high observability and controllability, it poses the security issues [7], [8], [9]. In P1687 network, anyone can shift the proper data through TAP controller and capable of accessing of any instruments embedded within the IC. If a person or attacker knows that the IC contains P1687 network inside and wanted to know the internals of the IC or information about the instruments behind the SIBs, he can simply shift the data and update the SIB cell to access. If the person wants know the length of the scan chain, and this length can be observed by passing the know data into the scan chain.

To restrict a IC from unauthorized/attacker, researchers suggested several methods using locking mechanism or challenge response pairs [10], [11], [12].

For example, the authors of [17] are proposed Protected JTAG authorization which is based on the challenge-response identification. This scheme capable of taking challenge input and generates the response output. Secure servers do the job of authorization process. This server takes challenge input and verifies the user authorization, if the user is authorized person, it generates an output response otherwise deny the access. The challenge-response algorithm is based on elliptic curve arithmetic. The secure server has a private key and the device owns a public key both has to match to give the access to the instruments.

In [18], the authors proposed a scheme based on hash functions to generate the challenge-response pairs. SHA256 hash engine and several ring oscillators to generate a random challenge are used. For a given random number generated from ring oscillators, a hash is generated using the secret key stored and hash engine, the user must compute the same hash to give the access. This design takes more area because of hash engine, ring oscillators, true rand number generator and also key storage.

In [19], to prevent the attacking of JTAG interface, two modules are designed to provide the security and control i.e Security module, Test Control Module. Security module is a state machine based design which controls the security mode of Test Control Module. The Test Control Module is operating in restricted mode or unrestricted mode based on the state of Security module. In the restricted mode, a limited access is permitted to the memory content and TDO output is goes high always. In the unrestricted mode, a full access is permitted to the memory content.

In [20], [21], The JTAG interface access is restricted by adding Secure Authentication Module (SAM) and Access Monitor. The Secure Authentication block contains Access management block and an instruction register. Upon reset, the JTAG interface is locked, only instruction register of SAM is accessible. The successful completion of Authorization protocol, the SAM gives permission to Access Monitor which allows the scan data to be shifted.

The researchers of [22], proposed a method to protect the scan chains. The N-key is associated with the scan in data during the initial stage of access. The specific bit input scan data is compared N-bit key after specified run cycles. If it is matched, the scan chain is granted for access otherwise denied. Which is lower area overhead mechanism but it weak authentication process.

The authors of [23] proposed a method for hiding the on-chip instruments behind Locking SIB (LSIB). A simple modification to standard SIB gives the authorized access i.e LSIB. The SIB cell can be opened or unlocked by applying a predefined key. This scheme is static password or key based mechanism means the key is same across the all chips which is a weak authentication method. To increase the brute force attack time, the same authors [24] extended the work by adding trap bits to LSIB cells. These strategies increase the cost of attempt or time required to open SIB.

To further increase the expected time to break, the authors of [25] are used linear feedback shift register. Linear feedback shift register is used here for generating the random sequence of bits that is feedback to LSIB [23]. The authors are hiding the scan chain length i.e hidden secure scan chain and two dimensional key. The key for LSIB is supplied from scan chain and from LFSR, and it has to match with the pre-defined to open SIB. The analysis shown in the paper [25], it takes several years for attacker to unlock the SIB.

The authors of [26] proposed reconfigurable networks using challenge response authentication protocol. The challenge response pairs are generating by using hash functions and TRNG circuits. The response is compared with the sequence stored in the secret memory. The standard SIB structure is slightly modified to scalable the scan chain. Different authorized person has distinct entry rights for each instrument. This scheme takes more area as compared to [23], [24], [25] but the man advantage of design is it provides the dynamic passwords. They assumed that the has core and TRNG are invulnerable to side channel attacks and synthesis of secret memory is not explained the paper [26].

Chapter 3

IEEE P1687 (IJTAG)

3.1 IEEE P1687 (IJTAG):

The emerging IEEE Std. P1687 (Standard for Access and Control of Instrumentation Embedded within a Semiconductor Device) [1], also known as IJTAG for internal JTAG, targets advanced scan-based interfacing and reuse of arbitrary on-chip instrumentation. IEEE Std. P1687 (IJTAG) defines the methodology for access and control of on-chip instruments through IEEE 1149.1 TAP Controller [2], [3] and other additional signals. This standard is an interface between the existing standards IEEE 114.1 JTAG and IEEE 1500 Core test [5].

IEEE 1149.1 gives a methodology to be embedded within the semiconductor chip for board level test using TAP controller and along with some additional internal registers. This method developed for mainly board level test only, but the TAP and TAP controller usage is widely speared to other applications like embedded instrument access in an ad-hoc manner. So the purpose of IEEE P16897 is give an extension to the existing standard IEEE 1149.1, mainly to manage the operations of embedded instruments.

3.2 Need of IEEE P1687 Standard:

The IEEE P1678 standard is to solve the issues that the industry is experiencing in the access and control of embedded instruments.

- With increase of more built in self-test functions, the testing process or schemes are internalized with in the chip to decrease the complexity and cost of the test.
- The access techniques are required for long scan paths.
- Engineers needed to be able to implement operational tradeoffs involving test/instrument scheduling, access path length, access time, power budgeting, interacting with on-off power domains and others.
- Engineers needed greater freedom to make certain design tradeoffs involving silicon area, route congestion, power consumption, timing impact and others.
- Additional mechanisms besides JTAG were needed to access embedded content in chips because many devices do not have a JTAG TAP, but they do have SPI, I2C (Inter-Integrated Circuit) and other minimal pin interfaces for test, debug and configuration.
- To cluster the on-chip instruments based on the functionality.

The Differences Between IEEE 1149.1, 1500, P1687:

P1687 is the extension of the boundary scan standard i.e IEEE 1149.1. These two are main other standards available for testing and diagnosis. IEEE std. 1149.1 boundary scan is widely adapted for board level testing and programing purpose also. This is also known as JTAG. IEEE 1500 is a standard for testing of IP cores.

Table I

The Differences Between IEEE 1149.1, 1500, P1687

Feature	**1149.1 JTAG**	**1500 ECT**	**P1687 IJTAG**
Purpose	For Effective circuit board Test	For validating the core embedded in a chip	For accessing of embedded instruments
Register Size	Fixed for instruction	fixed	flexible
Control of Internal IP	Vender Specific	Specific	Standard
Access of Internal circuit	Through TAP Controller	Through Wrapper serial port	Any i.e. TAP, I^2C,ISP etc
Includes Hardware FSM Controller	Yes	no	no
Includes Mandated Defined Instructions	Yes	Yes	No
Support of Network Instruction Bits	No	No	Yes
Architecture description language	BSDL	CTL	ICL,PDL

3.3 P1687 Access Network:

3.3.1 Introduction to P1687 network:

To access and control the on-chip instruments, mainly two key components are involved that is access network and embedded instruments type [10]. The access networks provide the control of embedded instruments through serial ports, wrapper cells or direct access to the devices. Serial Access Networks are well established technology by already existing standards and used widely across the industry.

3.3.2 Reconfigurable Scan Chains:

Reconfigurable scan Networks (RSN) are the most advanced scan architecture to integrate the instruments together with configurable register into scan network. Scan data are shifted from the primary scan-in, through a subset of instruments and configuration registers, down to the primary scan-out. Depending on the state of configuration register, a set of instruments are connected between scan-in and scan-out pins for a scan path. RSNs emerge as scalable option for on-chip instrument access. RSNs offers low cost, low latency and flexible.

An example of RSN is shown in figure 3.1, which contains two instruments S2 and S4 together with two configuration registers S1 and S3 using two scan multiplexers. The configure registers or shadow registers decides the path in which the data to be sent. If the content in the s1 is zero, the s2 connected instrument is bypassed otherwise data is sent through the s2 instrument. And s3 register decide the bypass or connected nature of s4 connected instrument. Several standards have been ratified recently for scan-based access to on-chip instrumentation which are IEEE std. 1532 and IEEE std. 5001 etc.

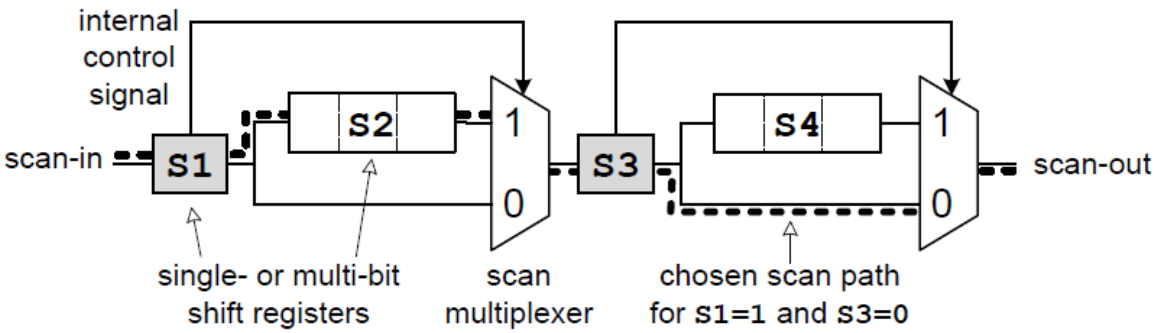

Figure 3.1: Example of Reconfigurable scan network

IEEE P1687 access network is composed of reconfigurable scan chains by SIB cells. To reduce the test time and cost, long daisy scan chains has to be avoided. In the long daisy scan chains all the instruments are accessible without depend on the use of instrument. If the daisy scan is broken at any point, the access to all the instruments are denied. Possibility of stuck-at false is also more in case of daisy chain scan network. As the number of instruments are increasing, scalable networks are required to access. Scalable networks are used form long scan paths so that the all instruments can be accessed through the port.

The problems, if we use the IEEE Std. 1149.1 boundary scan network is

1. Long daisy scan chains.
2. Each TDR has a separate instruction to configure.

To avoid these problem, a reconfigurable scan networks are defined by IEEE Std. P1687. Using the reconfigurable scan network one can connect the instruments ranging from tens to hundreds. SIB cells are responsible for making reconfigurable networks. The IEEE 1500 wrapper cells also can be configurable using these access network.

A typical IJTAG network structure is shown in the figure 3.2. SIB can open or close a particular scan path segment. If the SIB is open, it by passes the scan segment otherwise it connects the scan segment into Scan Path. The number of SIBs usage depends on the number of instruments deployed, and no limit on number of SIB. The control signals for SIBs are generated from TAP controller.

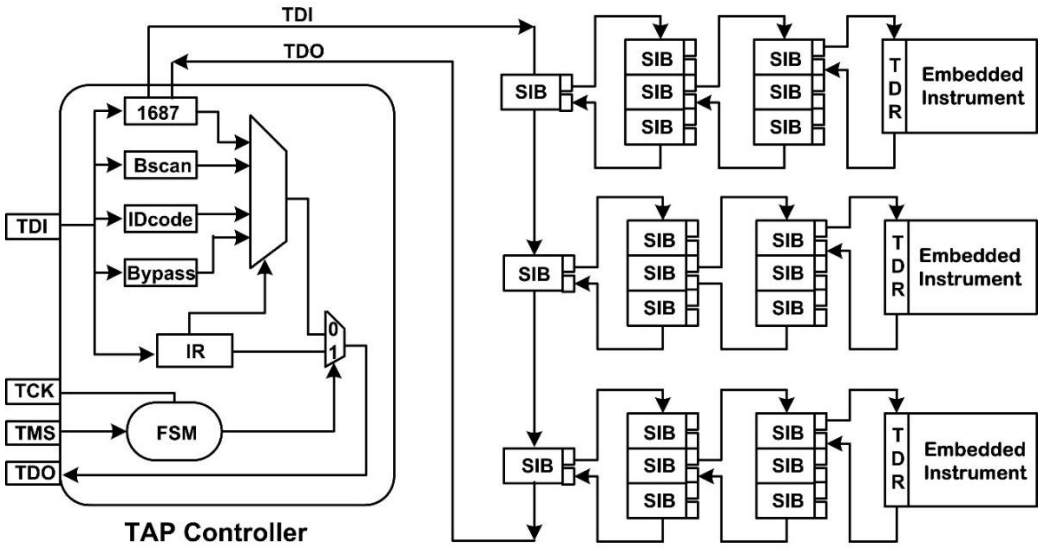

Figure 3.2: IJATG Scan Network

3.3.4 Serial Access Networks:

The protocol is used for IEEE Std. P1687 serial access is a common JTAG interface in other words the serial access of instruments is the IEEE Std. 1149.1 Test Access Port interface and its controller. And IEEE 1500 wrapper interface is also used for access and control of on-chip instruments.

3.3.5 Test Access Port (TAP):

TAP is an interface port between internal boundary scan architecture and external signals to provide the test access functionalities built with the integrated circuits. It is defined by IEEE 1149.1 standard. Due to easy access and minimum hardware structure, it is widely speared across electronic industry. Test access port is mainly used in boundary scan architecture for board level testing. TAP is also used in other built in self-test circuits like MBIST, LBISTs and I/O characterization in ad-hoc manner for accessing. This interface is also known as JTAG interface.

Interface signals:

The TAP interface or JTAG interface is having the following signals for providing the testing mechanism. These are the external signal available for test engineers.

1. Test Clock Input (TCK): This provides the input clock signal to test logic. The dedicated test clock input is provided because the serial test data between the modules should be independent of module specific system clock. It also provides parallel data transmission to test port and normal system operations.
2. Test Mode Select Input (TMS): This signal decides the next state logic of Test Access Port controller on the positive edge of TCK signal. TMS signal is sampled at every positive edge of TCK signal. The loading on TMS signal as small as possible because from a single driver, this signal branches to many components in the design. If TMS signal is zero or driven by any source, the TAP controller quickly geos to the Test_Logic_Reset state.
3. Test Data Input (TDI): TDI is also called as serial input. Test instruction and serial data are loaded through the signal. TDI signal is also sampled at every positive edge of TCK signal.
4. Test Data Out (TDO): TDO is the serial data output from test data registers. TDO signal is also outputted at every negative edge of TCK signal. To avoid the race free condition, TDI and TMS signals are sampled positive edge of TCK while the TDO signal is sampled on negative edge of TCK signal. The output signal will be delayed by half clock period. All the instruments available in the design or SoC design has to be configured between the TDI and TDO pins through SIB cells.

5. Test Reset Input (TRST): This is an optional signal defined by the standard, to provide the synchronization between the TAP controller and other test logic blocks. TRST is a asynchronous input to the TAP controller. If the TRST signal is logic zero, the controller goes to Test_Logic_Reset state.

3.3.6 TAP Controller:

The IEEE Std. 1149.1 TAP controller is a finite state machine that controls the operations of test logic embedded within the IC. The state transitions are change based on the signal value at TMS on every positive edge of TCK signal. TAP controller is having 19 states. The TAP controller state diagram is show in figure 3.3. The purpose of TAP Controller is to load the instruction into the Instruction Register and to load the data into Test Data Registers through TDI pin. The state diagram is having two symmetrical branches. One branch of state machine specifies the sequence of operations to the Instruction register and other provides to Data Register.

If the TMS signal is high for continuous three clock cycle, the TAP controller goes to Test_Logic_Reset state.

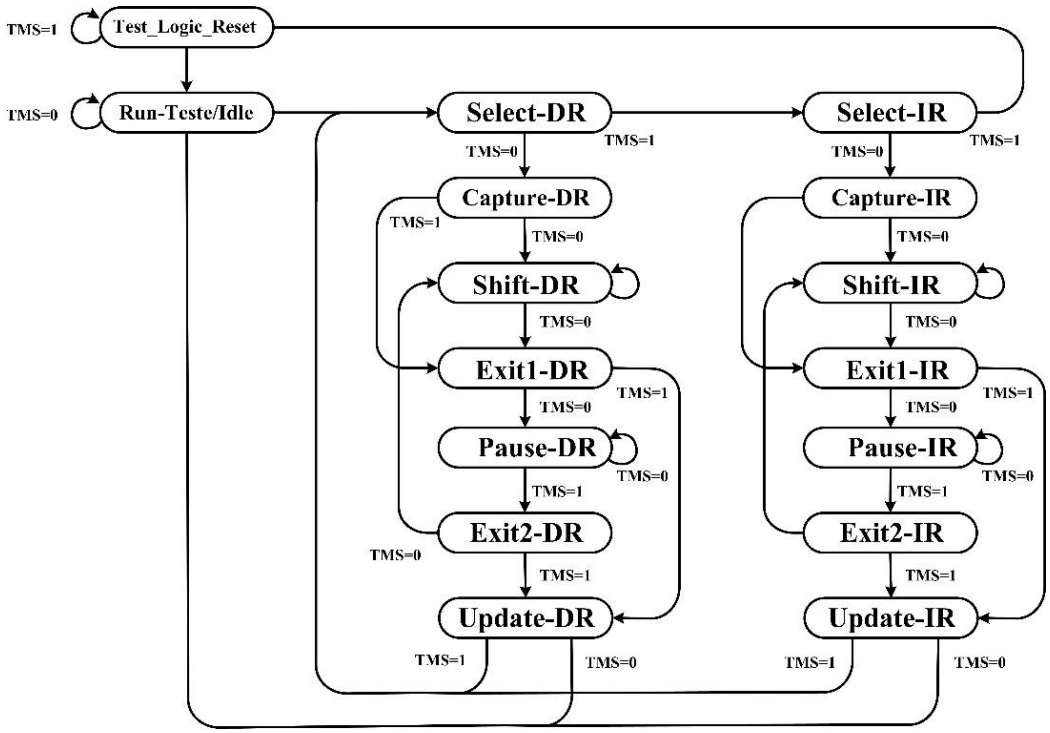

Figure 3.3: FSM of TAP Controller

3.4 Test Data Register (TDR):

TDR are cells that control and observation of on-chip instruments through the P1687 network interface. Read, write operations of TDR are controlled by TAP Controller. The IEEE std. 1149.1 TAP controller generates the required signals to configure, control, observe and operate the TDRs. The Test Data Registers are similar to Boundary cells defined by IEEE Std. 1149.1 but these are simple structure and takes less hardware area.

The TDRs can be designed in three types based on the operation.

1. Read-Only TDR.
2. Write-Only TDR.
3. Read-Write TDR.

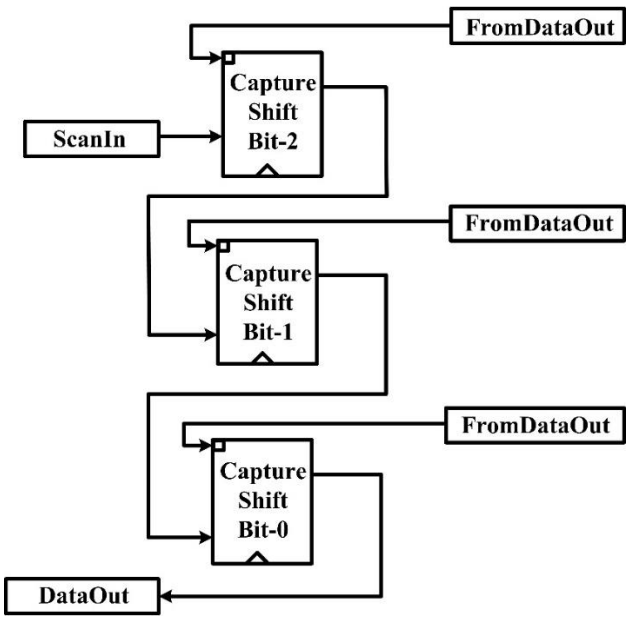

Figure 3.4: Schematic of Write Only TDR

An example of Write Only TDR is shown in figure 3.4, which is a 3-bit TDR. Each cell of TDR consists of two flip-flops that is Shift-Cell, Upadate-Cell. The Shift-Cell is positive edge trigger whose clock is fed from TCK, and Update-Cell is a negative edge trigger flip-flop. This type of TDR is used for give the data to embedded instruments, can't be read form the instrument. The ScanIn input signal is fed from the TDI signal of TAP controller when associated instrument is connected through the P1687 network. The ScanIn or TDI data flows to ScanOut Signal by single bit on positive edge of Test Clock Input (TCK) signal when

the TAP controller in ShiftDR state. The data flowing through the Shift register may create ripple, however the Update cell prevent the ripple in output of Shift cell. The binary data present in Shift cell transforms to Update cell on the negative edge of Test Clock Input (TCK) signal when the TAP controller in Update-DR state. The Output bits of Update-Cell is given to corresponding instrument connected to TDR.

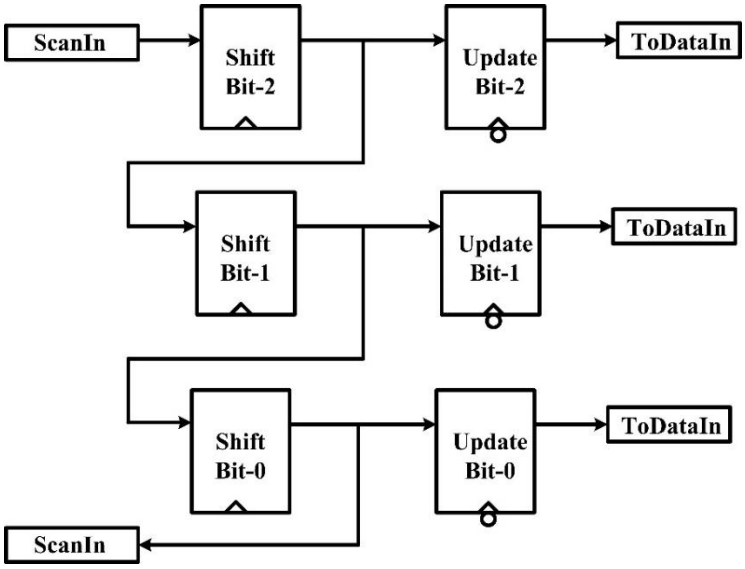

Figure 3.5: Schematic of Read Only TDR

An example of Write only TDR is show in figure 3.5, which is also a 3-bit TDR. Each cell of Write only TDR is consisting of only one flip-flop that is Capture-Shift cell with no Update-Cell. Capture-Shift cell is a positive edge trigger flip-flop. The read operation in TDR is done in two stages.

In first stage of read operation, the data present at the output of instrument is captured on the positive edge of Test Clock Input (TCK) signal when the TAP controller is in Capture-State. In second stage, the data captured is shifted out through Scan Out by single bit on positive edge of TCK signal. Before shift operation, the capture operation is done in the TAP controller state machine.

Example of Read-Write TDR is shown in figure 3.6, which is used for both reading and writing the data into the instrument that is it is a mixed type TDR. Which is similar to Read and Write only TDRs in other words this is combination both read only and write only TDRs. The read operation is done by capturing the instrument data and then shift the captured

data, whereas the write operation is done by shift the input data and then update the shifted data to the instrument.

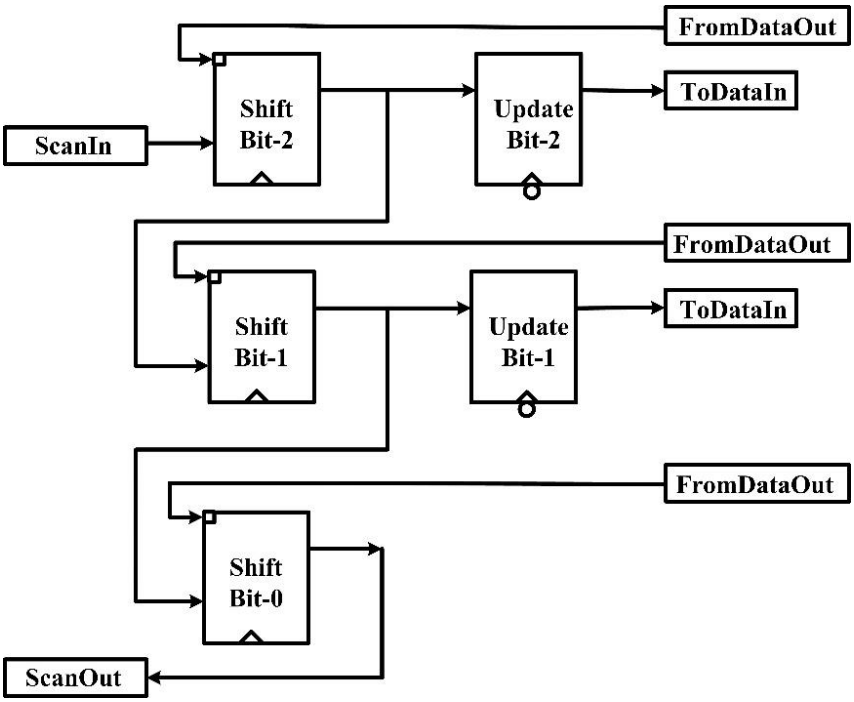

Figure 3.6: Schematic of Read-Write TDR

The TDRs has to be designed in such way that which are able to do the operations that is shift, capture, update when the control signals are given directly or from TAP controller. The TDR with complete controls signals are given in the figure 3.7.

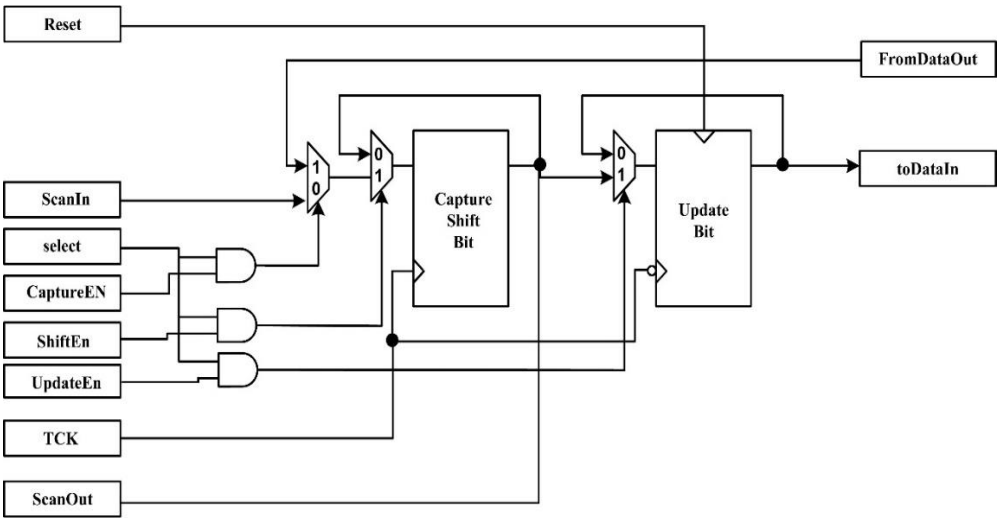

Figure 3.7: Schematic of Data Cell

- ShiftEn : if ShiftEn=1, the ScanIn data is shifts to ScanOut.
- CaptureEn : If CaptureEn=1, The instrument output data is captured.
- UpdateEn : If UpdateEn=1, the shifted data is passes to Update Cell.
- ScanIn : The ScanIn signal is connected to TDI of TAP controlled.
- ScanOut : ScanOut signal is connected to TDO of TAP controlled.
- fromDataOut: Instrument output is connected through this wire.
- toDataIn : The input given to instrument through this wire.

3.5 Segment Insertion Bit (SIB):

Segment Insertion bit (SIB) is used to establish the access network between the instrument and TAP controlled. Reconfigurable scan chains can be made by using the SIB. This is the key component in P1687 network. In modern day ICs, the count of on-chip instruments from ten to hundreds so this complex networks are need be configured by using IEEE P1687 network architecture. The scan length can be variable with assertion or de-assertion of SIB cells. When SIB is asserted, the scan path includes the particular sub scan chain or TDR. When SIB is de-asserted, the SIB bypasses the sub scan network. With the flexibility of Scan network, the engineer can create an optimized path to access and control of a particular instrument which in turn reduces the cost and test time. SIB design is not mandatory to implement a particular architecture. The designer can implement the SIB in any way but it must perform the standard functionality.

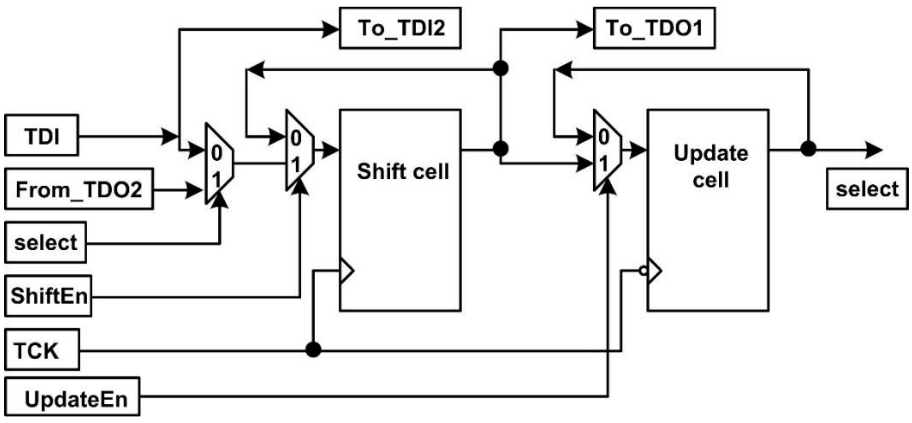

Figure 3.8: Segment Insertion Bit

SIB can be implemented in a simple way by using a Shift-Cell and Update-Cell. An example configuration of SIB is shown in figure 3.8 A ScanMux is added to Shift-Cell, which

decide the assertion or de-assertion of sub-scan path or TDR. The ScanMux is controlled bt select signal which is the output of Update-Cell. I_0 of ScanMUX is connected TDI and I_1 is connected to From_TDO2. If de-asserted (select=0) then next level scan network is by passed. If asserted (select=1) then From_TDO2 comes into the loop in other words next level scan network or TDR is connected into the Scan Path with one extra bit register. Select value in Update-Cell decide the Scan path length that is inclusion or exclusion of embedded instruments. Upon the reset the all the Update-Cells goes to reset state, therefore no instrument is connected. The Update-Cell is negative edge trigger flip-flop with clock signal is supplied from TCK. To assert an instrument or to set select signal, the TDI signal has to be one on negative edge of TCK signal when TAP controller is in Shift-DR state.

Chapter 4
Physical Unclonable Function (PUF)

4.1 Introduction to Physical Unclonable Functions

Physical Unclonable Functions (PUF's) are defined as physical functions that maps inputs to outputs, that physical functionality or mapping is based on the physical properties of devices. This functions are hard to characterize that means one can't guess the response information for a randomly selected challenge.

The PUF's are basically works based on uncontrollable/unavoidable process variation of IC, this process variations leads to variations in circuit characteristics like delay of device, interconnect wire delay, threshold voltages, start-up voltages in memory based circuits.

Fabrication of exact replica of a design is impossible for manufacture because of unavoidable process variations. Being negative at unavoidable process variations, what we can make out of this unavoidable process variations is key idea for development of PUF's.

Physical Unclonable Functions (PUF's) generates the challenge response pairs which can be used for IC identification etc [17]. The mapping between the challenges to response is unique that means for a given input signal, PUF will gives a unique. And the Response is different on other for the give same challenge because the process variations will exist from chip to chip.

4.2 PUF Classification:

PUF can be classified into different ways i.e depends on type of fabrication, applications, security levels etc. PUF are classified into three ways based on the security features and applications.

1. Strong PUF
2. Controlled PUF
3. Weak PUF

Strong PUF: Which are hard to clone, predict, characterize. This type of PUFs are used in authentication, key generation and identification.

Controlled PUF: The challenge response space of controlled PUFs are medium.

Weak PUF: Weak PUFs are having a few number of challenge response pairs. With the help

Of other cryptographic schemes, this PUF are used for key generation. This PUFs are used in low level security applications.

4.3 PUF Types:

Silicon based can be sub divided based on the type of variations, they are working. Examples of PUF types:

1. Delay Based PUFs
2. Memory Based PUFs

4.3.1 Delay Based PUFs:

Delay based PUFs works based on the random variations of interconnect delays of wires and delay of components [17]. As the transistor count increases, It is very difficult to get uniformity of physical properties in manufacturing of a Chip. This causes the variations in the dimensions of device like MOSFET gate length and thickness of oxide layer which results the propagation delay of transistors or circuits.

Example of Delay Based PUF Structures:

1. Ring Oscillator PUF
2. Arbiter PUF

Ring Oscillator Physical Unclonable Function:

Ring Oscillator PUF (ROPUF) uses delays of Inverter circuit to create unique challenge response pairs. ROPUF basically compares the frequency to generate challenge response pairs. The typical Ring Oscillator is shown in Figure 4.1. An Oscillator is designed using odd number of invertors connected in feedback loop.

The frequency of one ring oscillator is $f = \frac{1}{2*N*t}$

N= Number of invertor stages.

t= Propagation delay of each invertor.

So frequency of signal coming of oscillator is depending on the propagation delay of the inverter. These propagations delays always differ from gate to gate due to manufacturing.

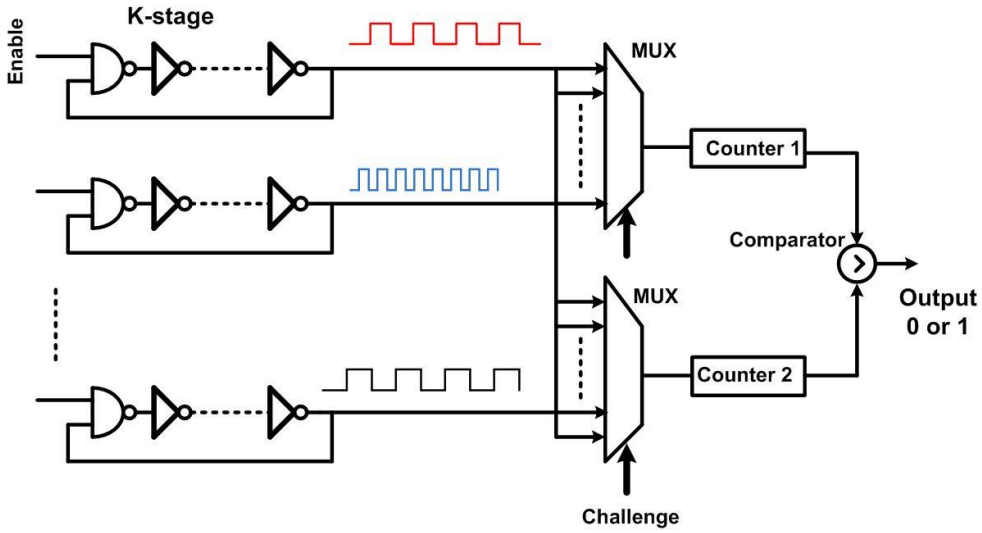

Figure 4.1: Basic Ring Oscillator PUF.

Ring Oscillator PUF contains identically designed ring oscillator circuits, each ring oscillator has own frequency, theoretically all Ring-Oscillators should have same frequency but because of process variations which leads to propagation delays of gate will defers the frequency.

The Ring Oscillator PUF designed using N-identical Ring Oscillators, RO_1 to RO_n and the frequencies of RO's are f_1 to f_n. The input challenge is connected as selection signals for multiplexers. For a given input, two of Ring-Oscillators are selected which fed to counters. By comparing the counter output after certain amount of time, the output signal geos to 1 if the counter1 is greater than counter2 and 0 if the counter1 is less than counter2. Here, we are indirectly comparing the frequencies of Ring-Oscillators.

$$\text{Output Bit} = \begin{cases} 1 & f1 > f2 \\ 0 & f1 < f2 \end{cases}$$

Arbiter PUF:

The arbiter PUF [32] works based on the interconnect wire delays, this PUF is also called as Switch based PUF. The architecture of arbiter PUF composed of N switch stages and a D Flip-flop. The output of PUF is depends on the interconnect wire delays of two parallel connected wires. The schematic arbiter PUF is shown in Figure 4.2. Each switch stage having two different MUXs which is controlled input challenge. By changing the challenge

bits to switching stage, we can get different combinations of interconnect wire with different delay.

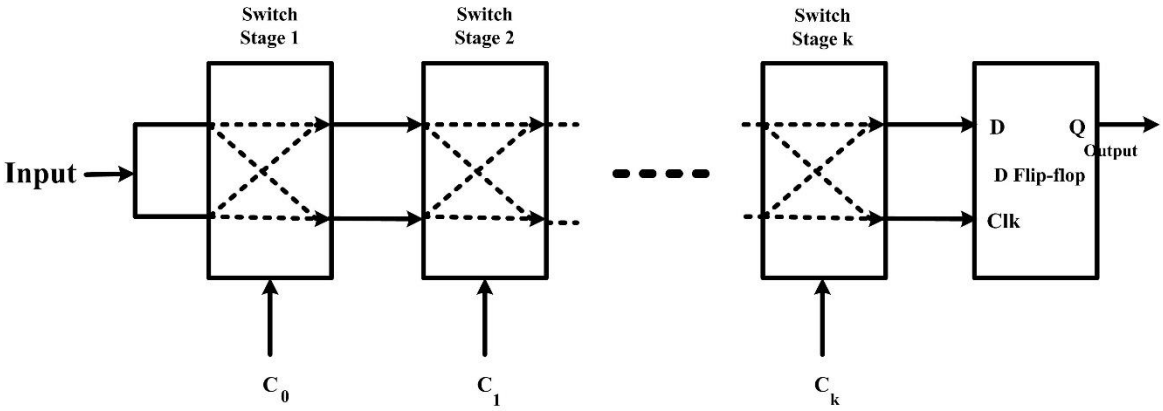

Figure 4.2: Arbiter PUF.

For a given input challenge, two different paths are established which are further connected to D input and clock input of D Flip-flop. This two paths are having different delays due to process variations. A signal is given to both lines at the same instance, the signal will pass through the both paths. One of the signal reaches the D flip-flop input or clock faster than other signal. The output of D flip-flop will be 1 if d input reaches faster than clock input otherwise output is 0.

4.4 Memory Based PUF:

SRAM based PUF works on the start-up voltage values of memory cells. The example of memory based PUFs are

1. SRAM PUF
2. Butterfly PUF

4.4.1 SRAM PUF:

It is proposed by Chang, Leland [29]. A conventional CMOS SRAM cell consists of six MOSFET transistors (6T). Two transistors are used for access the memory cell that is for writing and reading purpose, and the remaining four transistors are connected as a cross coupled invertor. Due to unavoidable process variations of dopant concentration in the channel of MOSFETs, the cross-coupled inverters always having a little bit difference in threshold voltage. SRAM cells are designed by proper width to length W/L ratios between

the MOSFET transistors, but due to manufacturing limitations always there exists small variations in widths and lengths which leads to effect on threshold voltage.

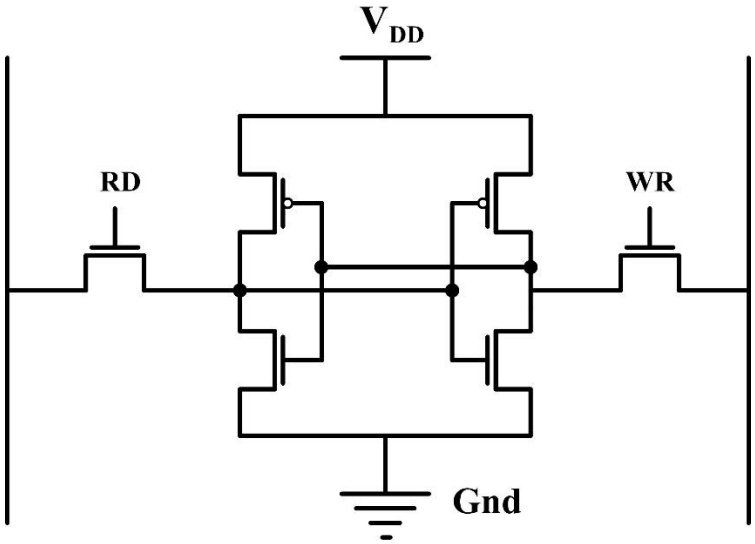

Figure 4.3: 6-T SRAM cell.

Hence, during the power up, the transistor with lower threshold voltage will switch firstly which leads either zero or one in the memory cell. This output value is purely depending on the mismatches in the threshold voltages. These start-up values are unique and different for each memory for a device. The random responses can get based on these start-up voltages of SRAM cells. For generating n-bit length responses, different CMOS SRAM cells are selected by different n-bit input challenges.

4.4.2 Butterfly PUF:

The Butterfly PUFs [30] also works on the principle of memory based PUF. The implementation of butterfly fly is same as SRAM PUF expect that cross-coupled inverts are replaced by latches as shown in figure 4.4.

The Butterfly PUF cell designed as two latches with the output of one latch is connected to input of anther latch. And output of 2^{nd} latch fed back to input of 1^{st} latch. Each latch consists of other two inputs to clear and to set latch which are labeled as CLEAR and PRESET signals. The PRESET of 1^{st} latch and the CLEAR of 2^{nd} latch are always connected to ground; the remaining two inputs are connected to input signals which is also challenge signal for PUF.

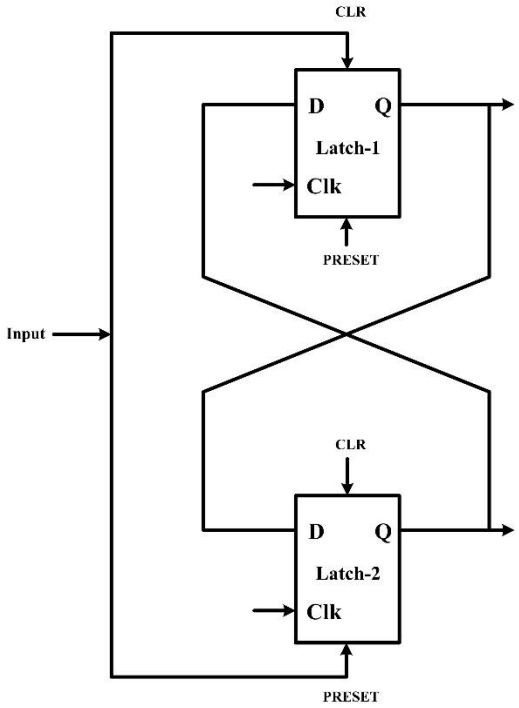

Figure 4.4: Butterfly PUF

When the input signal is applied, the laches goes into unstable condition after certain amount of time, the output state settle to either zero or one. This state will depend mismatches between the two latches. This output bit can be used as output of PUF. For multi bit response, we need to replicate the same structure.

4.5 Anderson PUF:

Anderson PUF [31] works based on the glitches present in the circuit, so this also is called as Glitch PUF. This PUF consists a chain of multiplexer and shift register that are the available basic components of FPGA. It is mainly implemented on FPGA boards by without creating any hard macros. It is simple to design and one can get unique and better responses compared to RO PUF.

On the FPGA board, the LUTs are used as the shift registers and each shift register output signal is connected to a MUX as a selection input. In this puf design two LUTs are used that is LUT-1, LUT-2. These shift resisters are initialized by 5555_{16} and $AAAA_{16}$ data which is a pulse train signal with 180^0 out of phase each other. The I_0 input of MUX1 connected to ground and I_1 is connected logic high. Output of MUX2 is connected to I_1 and I_0 is connected to logic zero.

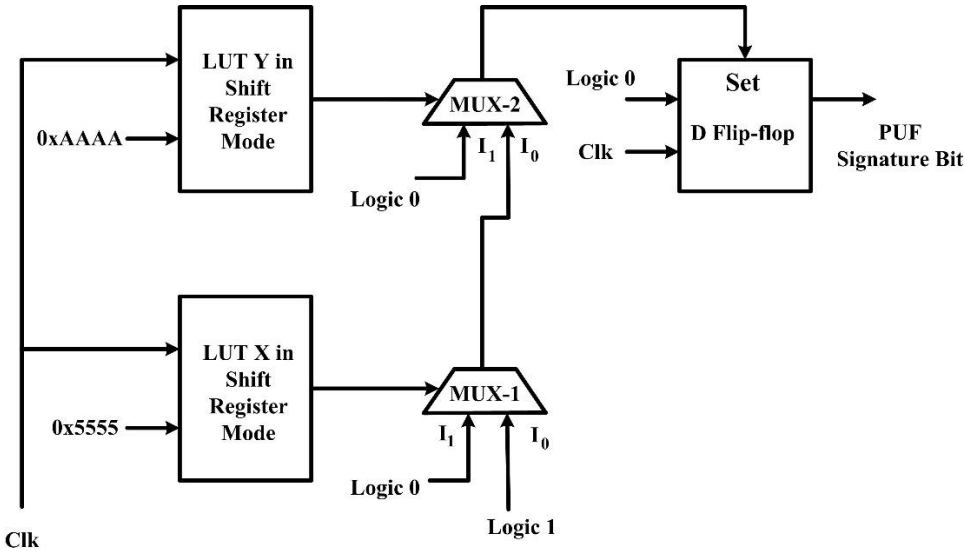

Figure 4.5: Anderson PUF

Theoretically, the output from MUX2 has to be logic zero always because of out of nature of initialized data but practically glitches presents in the output due to delay variations in the multiplexers. The Output of MUX2 is connected to PRESET of D flip-flop which basically stabilizes the glitch signal. The response bit or output of flip-flop is depends on the delay variations in multiplexer. For better response and uniqueness, one can add multiple multiplexers in between shift register.

Chapter 5
Authorized Access Management

In this chapter, we present the proposed a scheme for authorized access using PUF. Challenge response authentication protocol is used in proposed design. PUF is used for giving the dynamic passwords in other words to each instrument has a secret key and it has to be varied from chip to chip that can be done using PUF. To enhance the additional security LFSR are used in the design.

5.1 Authorization Principle:

In the proposed design, each instrument is protected by a unique key that is compared with the LSIB. To open SIB or unlocked an instrument, a requesting person has to give the challenge input to PUF such that the response of PUF is matched with the LSIB. To reduce the attacker guess to unlock an instrument, challenge response protocol is used, as described below.

All the instruments are locked initially or upon reset signal is applied. The entity has to give a request to unlock a protected instrument. For that challenge to supplied to PUF, which will generate the response. These responses all gives passes to all instrument in the corresponding level.

PUF Response=F {PUF (Challenge)+Manufacturing variations}.

Instrument Access Key=PUF Response + LFSR output sequence.

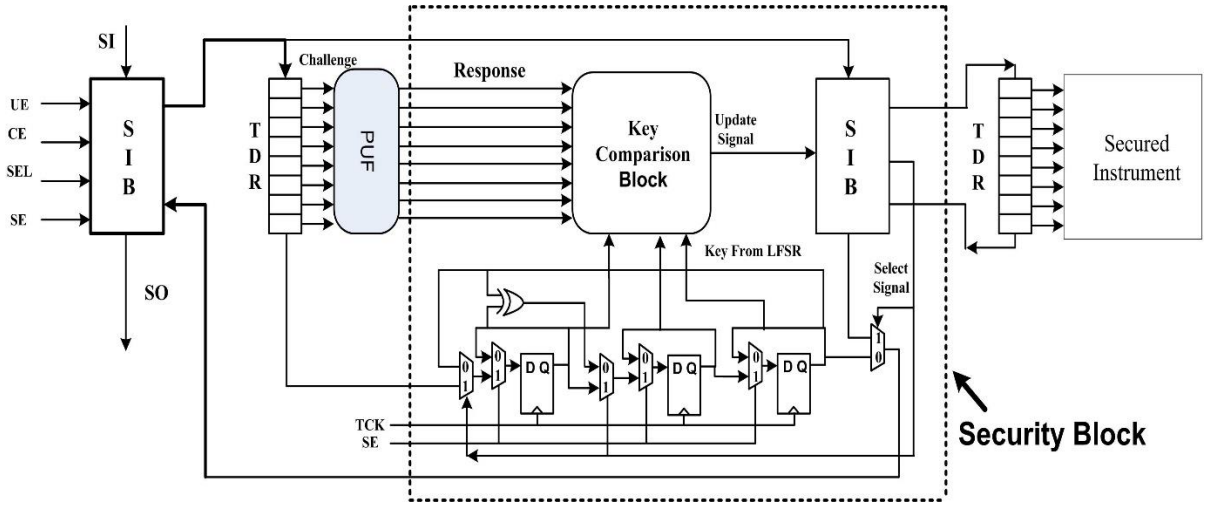

Figure 5.1: Proposed Design: SIB with Security Block

Figure 5.1 shows the proposed design with protected instrument. In the top level, the protected instrument is integrated to SIB.

If the instruments are added in a separate chain, the access time can be reduced to get better performance. Each instrument or SIB is associated with a particular LFSR network. LFSR network is used for generating the random number and to block the data coming out of TDO so the attacker can't guess the even input length of PUF. If the response is matched with LSIB then the instrument is unlocked. A specified response of PUF and LFSR output only matches in any other cases it won't match. For getting a specified output from LFSR, it has to run for a specified time. The protection can further have enhanced by adding traps to LSIB.

5.2 Secure IJTAG Network:

As the number of instruments are increasing, scalable networks are required for cost effective and efficient access the instruments. To meet the safety and security requirements, this scalable networks should be protected. Figure 5.2 shows the ways instruments has to be connected to meet the both requirements.

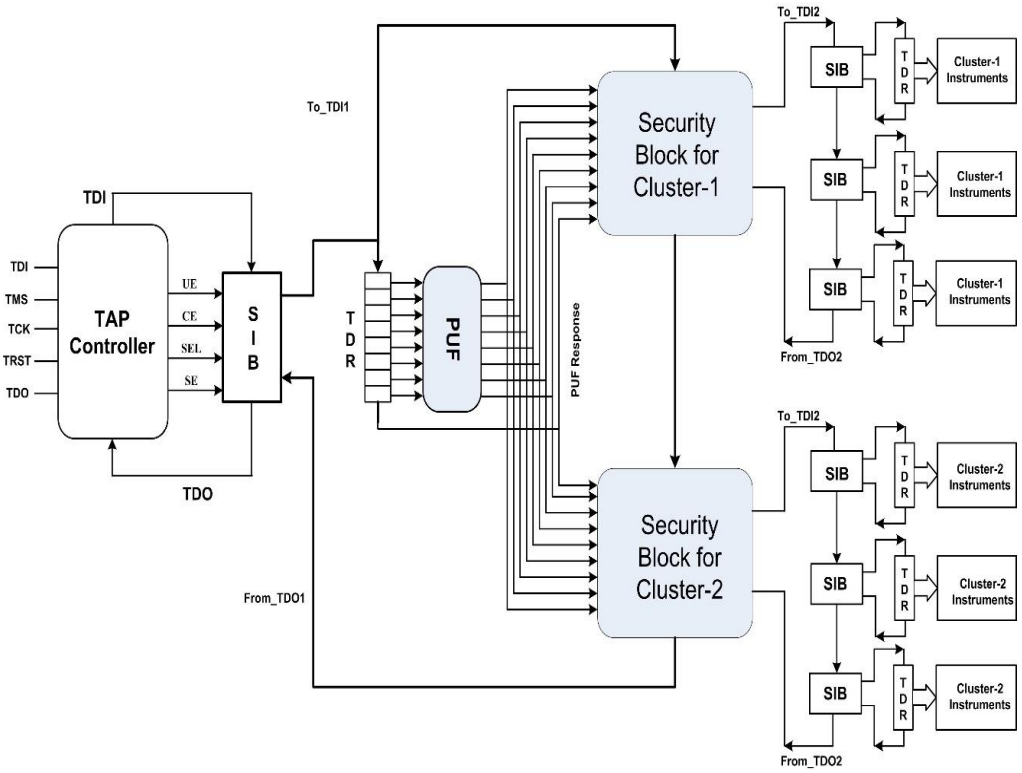

Figure 5.2: Proposed Design: IJTAG Network

Instruments are connected to various levels to provide different access keys. Instruments are characterized by functionality i.e instruments for system monitoring, in-field testing, pre-silicon validation, diagnosis and debug. For example, During the testing DFT instruments are used by test engineers, at the time of in-field system monitoring instruments like temperature sensors, pressure sensors are by the field engineers. To provide the different access to test engineer, field engineer, one type of instruments is place behind one cluster. Each cluster is assigned with different keys which provides the particular type of instruments can be accessed by authorized person.

5.3 Designed PUF Structure:

PUF used in the proposed for generating unique challenge response pairs. The challenge response pairs utilized for authorized authentication purpose. The secret key for authorization is proper input one to match the response of PUF to a specified key pattern. This specified key pattern or unlock pattern can have matched by using LSIB or LFSR pattern.

Generally, the RO PUF takes m-bit challenge input and generates a single bit output. But for authorized authentication purpose, we need a PUF it should take m-bit challenge input and generates m-bit output response. For n-bit output generation, the same RO has to be replicated n times. This consumes more area and power.

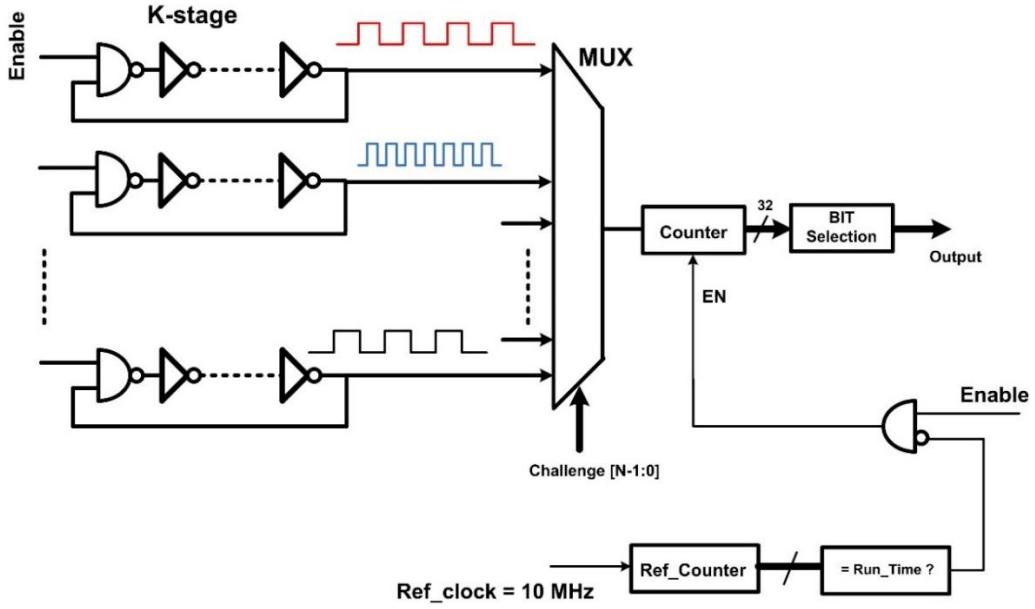

Figure 5.3: Modified RO PUF

Our aim is to use the concept of variable delays in the invertor based PUF for generating the m-bit output responses. Maiti et al.[32] introduced a RO based FPGA PUF that the multiplexers for selection of different delay paths. In this design, the authors used two ring oscillators with different path selection. However, in our design, LUTs are used as investors and paths between the LUTs are same in other words with the same path delays but only different the delay of invertors. So, the impact of wire delays on ring oscillator frequency can be minimized and randomness is purely depending on the LUTs. The deciding factor of PUF response is completely the LUT delay which depends on internal fabrication variation.

The modified ROF PUF is shown in the figure 5.3. It contains 2^Nx1 mux, 2^N ring oscillator and one reference counter. This PUF is a five stage RO i.e 1 nand gate and 4 invertors. Each invertor and nand gate is realized by using LUT element. The output of Ring Oscillator is a square wave.

The frequency of RO is $f = \frac{1}{(2*N*t)}$

N=Number of stages.

t=Delay of each stage.

We designed a five stage RO using LUT's, so the frequency is $f = \frac{1}{10*\text{tLUT}}$

The output of RO is given to a 32-bit up counter. This counter increments for every positive edge of RO output signal when EN signal is high. If the EN is zero, the counter will stop the counting which is fed from reference counter. The reference counter is used here to run the upper counter to specified to a time. The input to reference counter is 50MHz clock signal. Reference counter will generate active high EN pulse after specified time, which stop the counting of upper counter. The part of counter output selected as PUF response.

Each RO generate a different frequency signal because of propagation delay variations of each LUT i.e invertor. So the counter output for different frequency signal will differ. The control signal to 2^Nx1 MUX is N-bit challenge input. For each combination of challenge input, one particular RO is connected to Counter. The counter output is given to BIT selection unit. BIT selection circuit select the binary bits in such way that the frequency variations of RO should reflect at the response.

5.3.1 BIT Selection:

Part of counter measured i.e. counter output is used as PUF response. The counter output is represented in binary form; we select the part of counter output value as response. It is observed that the least significant bit of counter will vary more due to environmental conditions i.e temperature variations. The bits close to MSB will be stable and the temperature variations will have no effect on the output. The more we will be close to the MSB, the more stable bits will be. The example behavior of bit positon stability is shown in the figure 5.4.

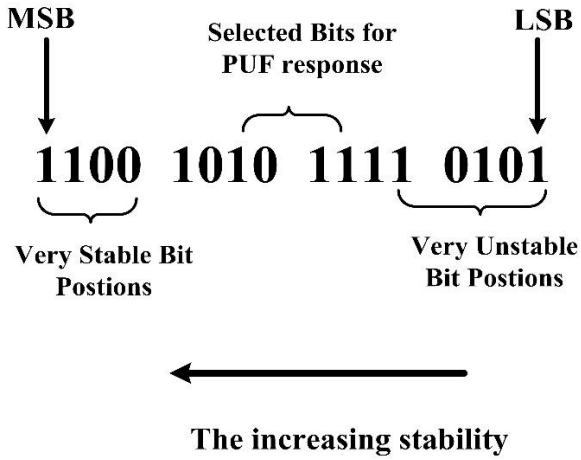

Figure 5.4: Bit position stability

5.4.2 N-Bit Input & M-bit Output PUF:

We designed the PUF structure in such way that it takes four input challenge gives the four-bit output as a one block. For generating the 16-bit output, we instantiated the same structure four times. Each RO PUF block will have one 16x1 MUX and 16 different set of ring oscillators.

The area requirement is less compared to Basic RO PUF design. For example, to design 8-bit input and 8-bit output. The upper four bits are connected to stage one, the lower four bits are connected to second stage, the total number of ring oscillator required is 32 for proposed design. But in case of basic ro puf to 8-bit PUF, we need 128 different ring oscillators and 8 MUX's. In figure 5.5 shows the multi bit input & output PUF.

In comparison to basic ring oscillator puf, we assume that the reference clock is generated from a stable so the fluctuations in the output is less in other words the reliability

Of proposed design is good.

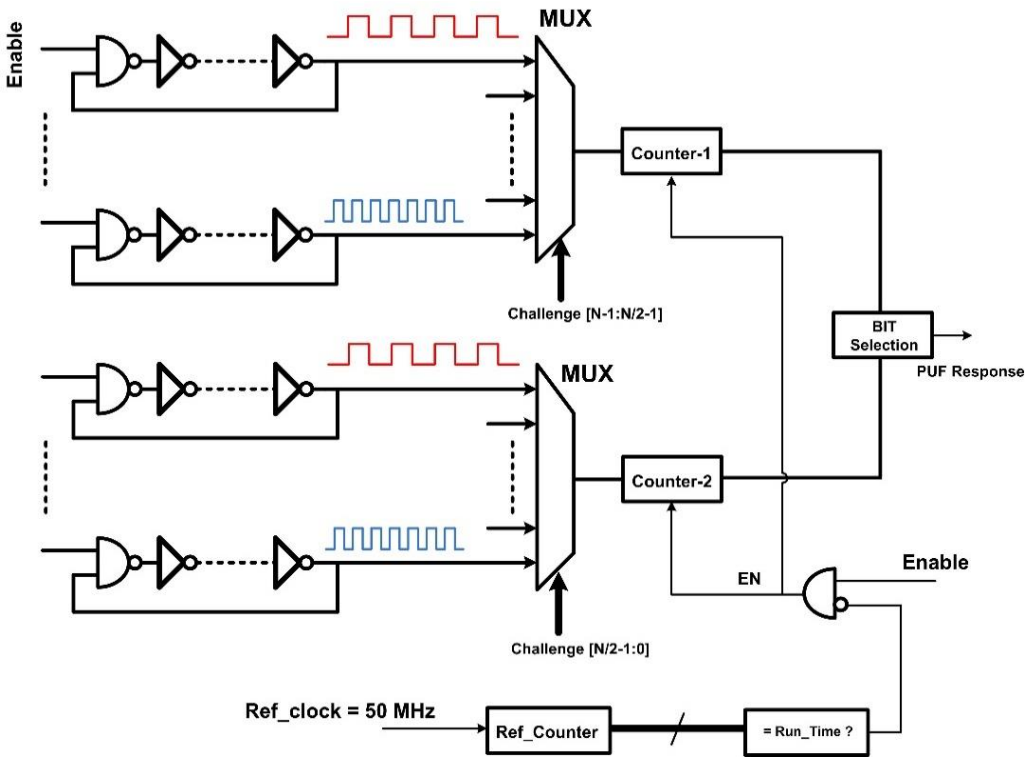

Figure 5.5: N input-M output RO PUF

5.4 Key Comparison: LSIB

Embedded hardware locks provide a standardized, repeatable and possibly portable security method. One form of a hardware lock, which was presented and published at the International Test Conference (ITC) in 2013 and Design Automation and Test in Europe (DATE) in 2014, is the Locking Segment-Insertion-Bit (LSIB). The LSIB is a JTAG-like cell based on the IEEE 1687 IJTAG standard's definition of a Segment Insertion Bit (SIB). SIBs support the JTAG Shift-Side and Update-Side, which allows a segment of a scan path to be added or subtracted from the active scan path within a chip. When updated with an 'assert' value, a SIB opens a port that contains a second TDI/TDO and activates a SELECT signal. This SELECT signal is used to unblock the ShiftEn/CaptureEn/UpdateEn that connects a Test Data Register (TDR) to the active scan path. A SIB can be 'locked' by requiring that other scan path bits provide signals from their Update-Side. These signals can be referred to as keys or Key-Bits (which support both logic 1 and 0 values). They gate the UpdateEn signal to the SIB, making it a LSIB. (Figure 5.6)

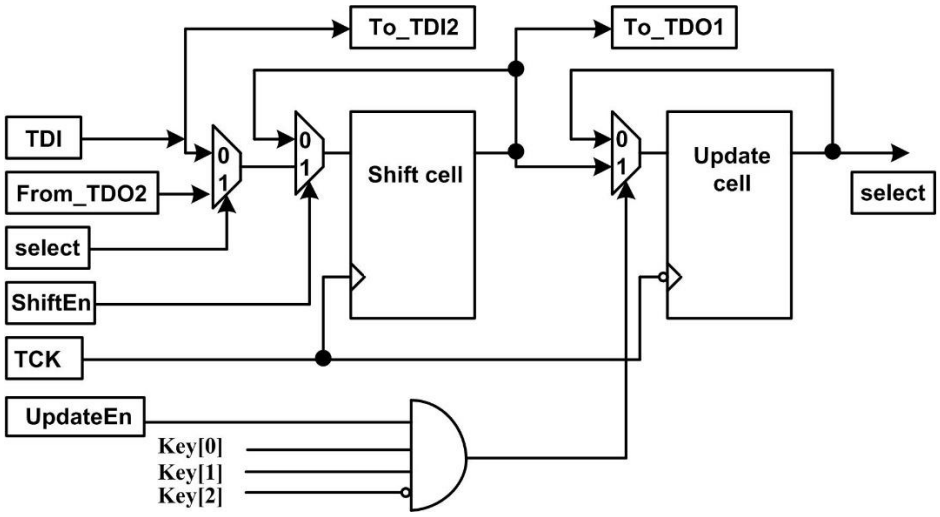

Figure 5.6: Locking Segment Insertion Bit

5.5 LFSR:

LFSRs are Pseudorandom Pattern Generator circuit, designed by shift registers and additional gates like XOR, XNOR etc. LFSRs are extremely good in random pattern generation compared to other existing generator. It consist of n numbers shift registers whose input bit stream is linear function of previous shift register states. Commonly XOR gate is used as linear function to generate the input bit. Thus, input bit is calculated by XOR operation of some of shift register output values. The initial value of shift register is crucial for generating random pattern and a long sequence of bits further. Because the LFSR is always generates a finite number of possible states, which are repeated once all the possible states are generated. So the initial values of LFSR has to selected in such way that it should be one of the possible state, otherwise the random sequence will not produce. It is necessity the LFSR should never enter into zero state because XOR operation of zero state is always zero, it will not go other state.

LFSR can be implemented by using simple hardware structure, and this is reason LFSRs are used is many applications.

Applications:

1. As a counters: The repeating sequence of LFSR output state is used as clock divider.
2. Uses in Circuit Testing: For Test pattern generation, for signature analysis, the LFSR circuits are used in testing.

3. Uses in Scrambler: In digital broadcast and communications, LFSRs are used to prevent the repeated sequence of zeros and ones.
4. Cryptography: In stream ciphers, LFSRs are used as pseudo-random pattern generators due to simple architecture by using electromechanical or electronic circuits and these gives a uniform output patterns.

LFSR based stream ciphers is also used in GSM phones, Bluetooth, and shrinking generators.

Types of LFSR Structures:

Based on the Feedback connections, LFSR can be divided in two types:

1. External Feedback
2. Internal Feedback

External Feedback LFSR:

Fibonacci LFSR is the example for External feedback type LFSRs, in which the left input bit is fed by XOR of shift resister values and other bits are not change, they just shift towards next shift register.

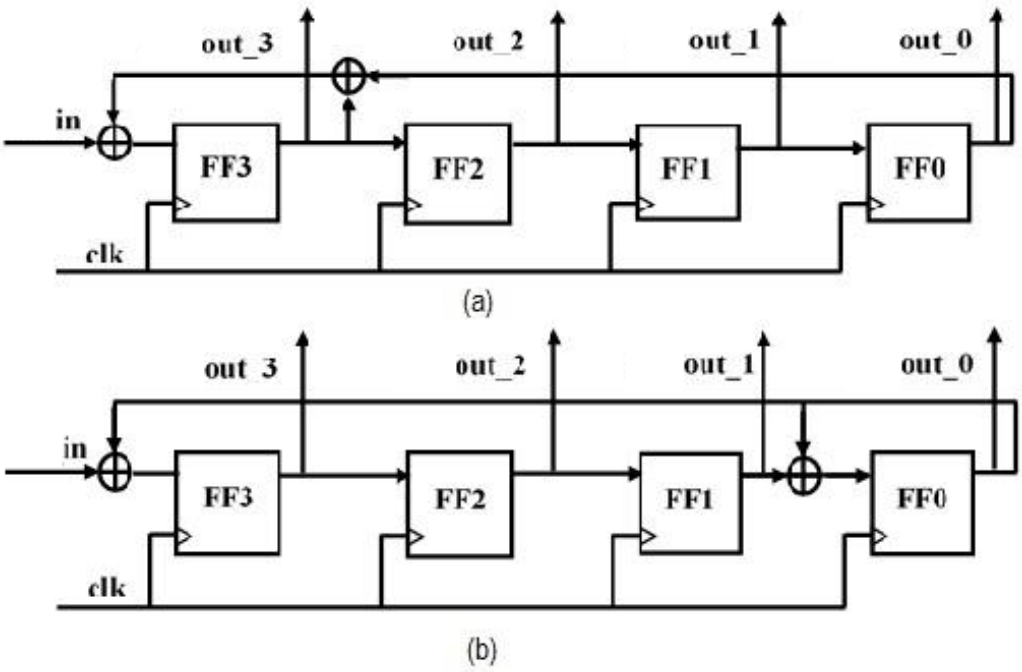

Figure 5.7: (a) LFSR using external feedback, (b) LFSR using internal feedback for the characteristic equations P(x)=1+x1+x4

Two types of LFSR configurations are possible for a give characteristic equation that is by using external feedback and internal feedback paths. For example, the characteristic equation $P(x)=1+x^1+x^4$. Figure 5.6(a) shows the LFSR schematic realization by using external feedback method. In this LFSR structure, for selected states of shift register values XOR operation is done and feedback to input or first stage of shift stage of Shift register.

Figure 5.6(b) shows the LFSR structure for the same characteristic equation using internal feedback logic. In this XOR gate are placed in between two shift register, for this XOR gate one input signal from previous shift register and other input signal form other shift register is fed. The output of XOR gate is given next shift register.

The two configurations are having same hardware utilization and output space for a same characteristic equation. But the output sequence in shift register stages are not same after every clock pulse.

In proposed, we are using LFSR for two purposes.

1. For Hiding the PUF input Length: LFSRs are used here as cover of PUF inputs that is for any attacker wants to give the input to the PUF, he should know the length of PUF but we can mask the length by using LFSR.
2. For key Generation: LFSR are generating random pattern outputs, we can use one of the output pattern as key for LSIB.

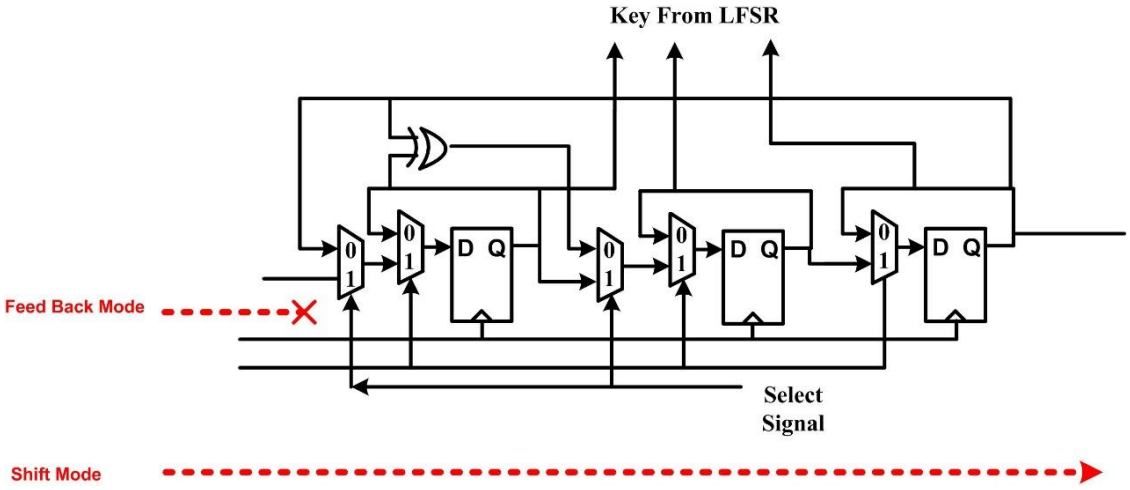

Figure 5.8: LFSR structure with TAP control signals.

Figure 5.8 shows that the modified LFSR structure by using TAP controller control signals, which contains LFSR schematic with additional multiplexers. The output from LFSR are used as the key in the proposed scheme. To unlock the Key comparison block, must shift a correct PUF response from PUF and a specific key from LFSR network.

LFSR network operates two modes:

1. Feedback Shift Mode: Used for key generation
2. Normal Shift Mode: To pass the input data to out.

The TCK signal, which is the TAP controller cock signal is fed to each D flip-flop in the LFSR network. So that upon the positive edge of TCK signal, input of D flip-flop is shift to output. The input signal of each flip-flop is fed by a MUX whose control input is connected to ShiftEn. The input signal I_0 to these multiplexers is fed back from every flip-flop and I_1 is fed from previous state. If ShiftEn is 0, the LFSR is in the same state. If ShiftEn is 1, the previous shift register is passes to next level shift register for every TCK clock signal. And MUX-1 and MUX-3 are used for connecting feedback signals, these MUXs are controlled by select signal. The input I_1 to MUX-1 and MUX-2 is connected to previous state and I_0 is connected to feedback signals. In locked state, the select signal is high, the LFSR gives the random patterns and this is called as feedback shift mode. In unlocked state of SIB, the select signal is zero, the feedback signal is disconnected and the LFSR network works as a shift register, which is called as normal shift mode. The possible output patterns from LFSR is 2^m-1 which is depends on the structure of flip-flop. We choose one of the pattern as unlocking output pattern.

Chapter 6
Implementations and Results

6.1 Implementation of Proposed Ring Oscillator PUF on FPGA:

In chapter 5, the modified RO PUF working model is explained in details, implementation details are given in this chapter.

6.1.1 Look Up Table as an inverter:

In RO PUF, each ring oscillator consist of five invertors with enable input and one output signal. 16 set of ring oscillators given to 16x1 multiplexer. The control inputs of multiplexer are fed from the challenge input.

We have designed this PUF on Xilinx Spartan 3E board. The invertor of each ring oscillator stage is implemented using 4 input LUT. The inputs for LUT are I0, I1, I2, I3. I0 is taken as input for invertor. The LUT output is connected to next stage invertor gate i.e input of Next stage LUT.

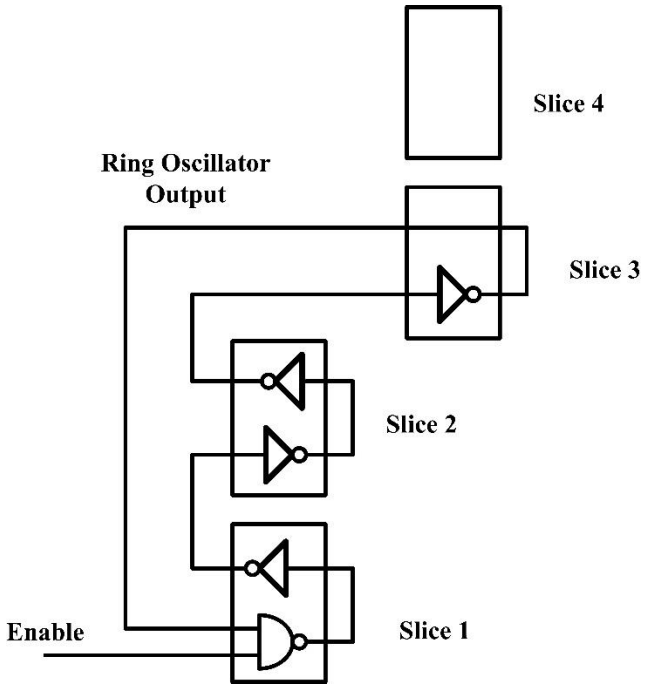

Figure 6.1: Placement of RO in 1 CLB

A CLB of Xilinx Spartan 3 devices consist of four slices, each in turn are comprised of two Look-Up Tables (LUTs). The number of inverters used in one ring oscillator design is 5. Each ring oscillator uses 5 SLICEs in 1 configurable logic blocks (CLB).

Look Up Table functionality depends on the initially loaded value into to it. Initialization is done by using INIT command.

Note that, the ring oscillator is created as a hard macro and is instantiated as many times as needed in the top-level PUF design. Figure 6.2 shows four identical ring oscillators implemented as hard macros.

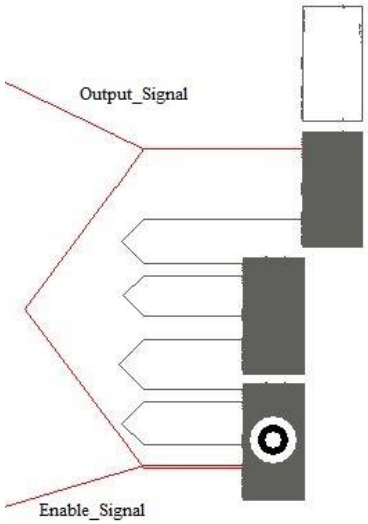

Figure 6.2: One Ring Oscillator circuit implimented as Hard Macro in Xilinx

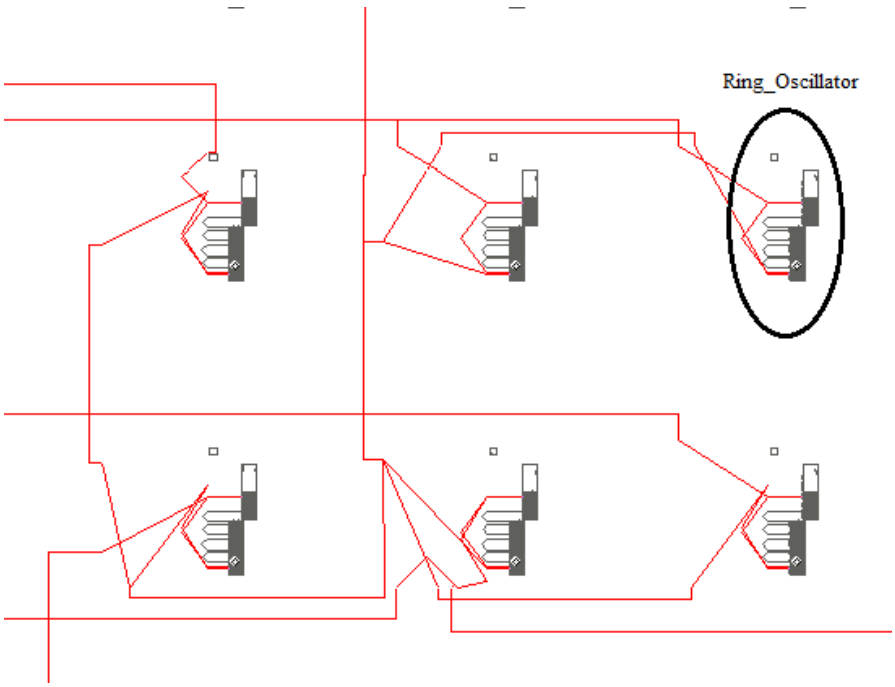

Figure 6.3: Placement Of Ring Oscillators at different locations on Xilinx Spartan 3E

All the ring oscillators are identically placed and routed. Thus, the only random parameter which influences on the oscillation frequency is the delay of the inverters. Each configuration will have its own distinct frequency of the RO due to delay variations of different LUTs and wires within the CLB. Hence, when comparing the frequency of a pair of ROs, both ROs must have the same configuration. This guarantees that the only difference between two ROs are solely based on manufacturing variations but not routing differences. It is important to notice that data dependency may exist among four bits, i.e. first four bits will always the same.

6.1.2 PUF Response collected from four boards:

Ring Oscillator Puf is Designed on four Xilinx Spartan 3E boards , got the different response for same challenge input.

Table II

PUF Responses on Different Boards

Challenge	01	05	25	34	A2	61	31	FF
Xilinx Board#1:	0F	5D	5C	44	14	54	4C	55
Xilinx Board#2:	39	3B	07	0E	23	22	32	04
Xilinx Board#3:	C9	CB	07	0D	0F	CA	4A	04
Xilinx Board#4:	4A	35	43	18	10	77	7E	06

6.2 TAP Controller, LSIB, LFSR:

The FSM of TAP controller is defined by the IEEE 1149.1 standard. The TAP controller, 8-bit LSIB, 8-bit LFSR, 8-bit TDR (Test Data Register) is designed using Verilog HDL code and verification of design is performed using Synopsys VCS tool.

Synopsys Design compiler is used for synthesis of secure IJTAG network. TSMC 65nm standard cell library are used for synthesis. Figure 6.4 shows control signal generated from TAP controller.

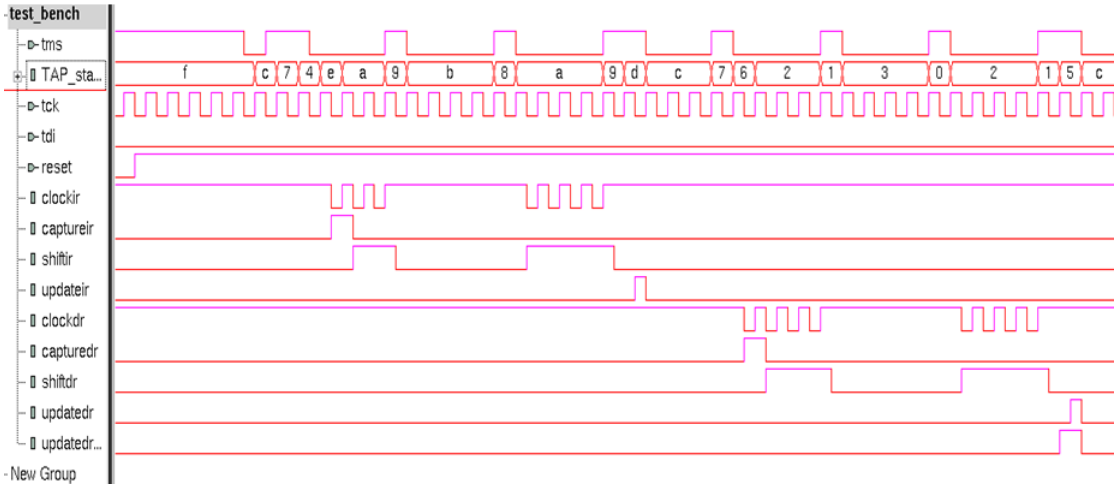

Figure 6.4: Control signals from TAP Controller

The control signal generated from the TAP control signals are used for reconfigurable scan chain formation in otherwords access contol of SIB cell. In figure 6.5 shows the unlock of SIB cell when the key is matched to specifeid password. We assume that the response of PUF for a particular input is 0xaf. LFSR network gives a 8 bit key to the network every positive edge of TCK signal when SE is high.

When the PUF response is matched with key, the select signal goes to high on negitive edge of TCK signal. The LFSR external will be close and works as shift register. Then the data from TDI input is goes to TDR during the Serial Enable state. And this data is applied to instrument when update signal is goes to high. The output data is captured back to SIB cell during the Capture State of TAP controller.

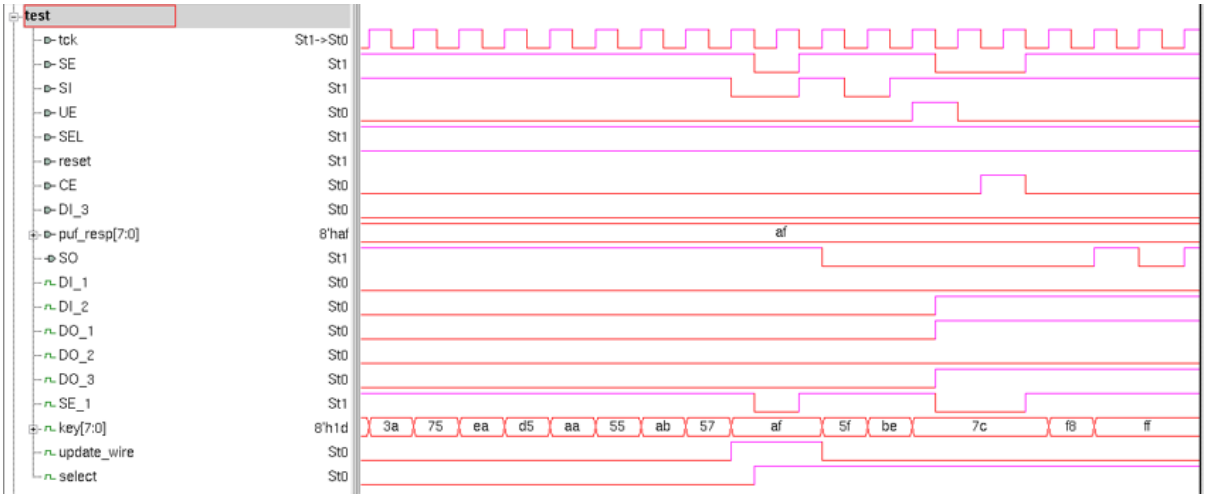

Figure 6.5: Simulation Result When key is matched

6.3 Performance overhead:

The authentic user knows key and number of cycles to run LFSR to unlock the SIB. This authorization verification is required only once per test session. The amount of time required to unlock the SIB for authentic user is as follows:

- The standard 1149.1 JTAG requires five clock cycles for the update and capture phases.
- Assuming the 8-bit PUF challenge, it needs 8 cycles+2 cycles to pump the challenge into the PUF.
- Assuming that, the LFSR generates the specified response after 'N' cycles.
- And another two clock cycles to unlock the SIB.

The total clock cycles can be calculated as: 5+8+2+N+2 = N+17 TCK (JTAG clock) cycles are required to unlock the SIB for authentic user. The value of 'N' varies from every instrument in a chip and between chips. The value of 'N' varies between 2 to 65535 cycles for 16 bit LFSR. The security level can be further increased by increasing the PUF Response length and LFSR bit length. This increase in length will also increase the access time and area of security block of the instrument, which tax the test time of the IJTAG network.

6.4 Security Analysis:

Initially, the attacker applies a reset to clear all possible states. There are 5 clock cycles required to move from the reset to shiftDR status. After shifting an n bit pattern, one has to test whether or not the pattern is working. Analyzing the output to distinguish the status of LFSR and locking state of SIB. The attacker needs at least 2L clock cycles in the shiftDR state to observe the repeating of TDO sequence, which also means SIB is in the locking status. If it is not repeating, it means SIB is unlocked. If it is failed, the intruder has to shift in the same pattern and update it with other output patterns of LFSR.

If the attacker is failed to open for all output pattern of LFSR, then he needs shift to new n bit pattern and has to check all possible in the same way. We assume that the attacker no idea about the length of PUF challenge, he has to guess the length of PUF challenge. He come across the possibilities 1) guess length < PUF challenge, 2) guess length = PUF challenge, 3) guess length > PUF challenge. In case 1, 3, the attacker will never get access to

the protected instrument. If attacker guesses the exact length of the PUF challenge, he has to check the all the possible case i.e brute force attack. Figure 6.6 shows the number of cycle required to check one pattern. Initial five cycles required to move TAP controller from reset state to ShiftDR state. Then attacker can give the data PUF, the number of cycle required for this depends on the TDR length i.e length of PUF.

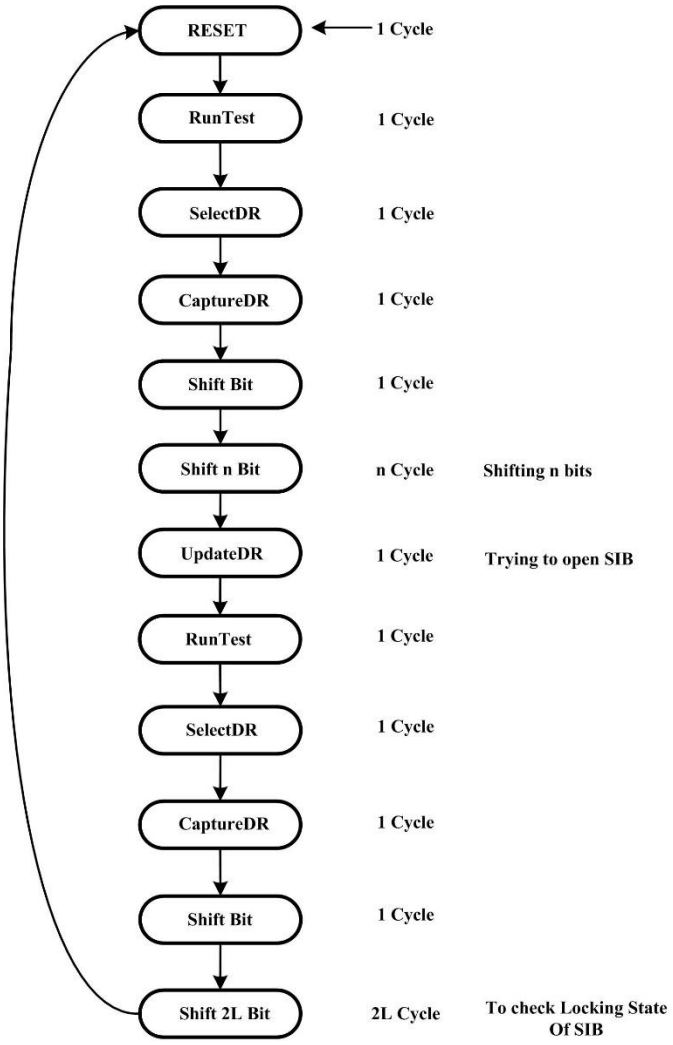

Figure 6.6 : Total number cycles required to test one pattern.

Cost of 1 Attempt = (n + 2L+ 10).

Total number output patterns from LFSR $L=2^K - 1$.

K=Number of key from LFSR

Total number of cycle required to test one n bit pattern = (n+2L+10)L

Expected cost = $(n+2L+10)L2^n$

Table III

EXPECTED TIME REQUIRED UNLOCK THE SECURITY BY AN ADVERSARY FOR DIFFERENT LENGTH OF TDR.

Sl.No.	'n' (length of TDR)	Number of cycles required for brute force attack	Number of Days	Paper(23)	Paper(25)
1	8	3.4E+7	3.9E-9	3.97E-7	2.32E-07
2	16	8.9E+8	1.03E-3	1.99E-4	9.34E-05
3	32	6.04E+14	6.99E+2	2.57E+1	1.06E+01
4	48	4.07E+19	4.7E+7	3.36E+6	9.85E+05
5	64	2.74E+24	3.17E+12	4.39E+11	8.37E+10
6	80	1.84E+29	2.14E+17	5.74E+16	6.74E+15
7	96	1.244E+34	1.44E+22	7.52E+21	5.24E+20

We calculated the total number of cycles required to test all possible case. Table II shows the expected cost of unlocking the SIB in days for several values of n and 8-bir LFSR key length. Here we taken clock speed is 10MHZ signal.

6.5 Discussion:

- The PUF implementation used for securing the IJTAG can be used for IP protection, cryptographic key generation in other applications.
- The comparison of different techniques with proposed method is shown in Table II. The techniques presented in [2] [3] [8] have static passwords. In [8], it makes use of LFSR and for a given chip, the password for secured SIB inside the chip may vary and passwords are same for all chips. The work presented in [9] supports dynamic passwords and passwords will vary across chips. In this paper, the proposed design support dynamic passwords with the help of PUF and password will vary for every chip and instrument on the chip.
- Table II shows the time required to crack the key by brute force method for proposed scheme and other techniques. As the bit-size of key increase, the proposed scheme

takes more time for an adversary to break the security in comparison with other techniques presented in earlier papers. The proposed scheme support dynamic passwords and more secured against brute force attacks in comparison with earlier techniques.

Table IV

Comparison of proposed method with other IJTAG security schemes

Parameter	Paper [23]	Paper [24]	Paper [25]	Paper [26]	Proposed
Password	Static	Static	Static	Dynamic	Dynamic
Area overhead	Low	Low	Medium	High	Medium
Routing	NA	NA	NA	High	Low
Expected time to unlock the SIB for an adversary	Low	Low	Medium	High	High
Performance overhead	Low	Low	Low	Medium	High

Chapter 7

Conclusion

Good observability and controllability of chip internals is requisite for low time to market, high product quality, as well as system reliability and maintainability. However, the accessibility of chip internals through on-chip instruments contradict with security and safety requirements.

Secure Access management for on-chip instruments is proposed by using Physical Unclonable Function. Additional LFSR structures are used to increase the security further. Even if the unauthorized person guess the correct challenge input to PUF, the LFSR structure restrict the access of on-chip instrument. The response of PUF and LFSR sequence are used as key to lock and unlock the LSIB. To access a particular instrument, the correct challenge input and fixed number of LFSR cycle has run. A new RO PUF structure is designed to get the multi-bit output response. This structure is validated on Xilinx Spartan 3E Board.

The advantage of proposed design is that it provides the dynamic passwords with minimum area and less routing congestion.

References

[1] IEEE Standard for Access and Control of Instrumentation Embedded within a Semiconductor Device, in *IEEE Std 1687-2014* , vol., no., pp.1-283, Dec. 5 2014.

[2] IEEE Standard Test Access Port and Boundary-Scan Architecture 1149.1-2001, 2001. Test Technology Technical Committee of the IEEE Computer Society, USA.

[3] "IEEE Standard for Test Access Port and Boundary-Scan Architecture," IEEE Std 11491-2013 Revis. IEEE Std 11491- 2001, pp. 1–444, May 2013.

[4] Altera Corporation, "IEEE 1149.1 (JTAG) Boundary-Scan Testing for the Cyclone III Device Family," in Cyclone III Device Handbook, vol. 1, 2011, pp. 12–1 to 12–8.

[5] "IEEE Standard for Embedded Core Test 1500-2005", 2005. Test Technology Technical Committee of the IEEE Computer Society, USA.

[6] H. Foster. "Challenges of Design and Verification in the SoC Era". In Design and Verification Conference and Exhibition. 2011.

[7] K. Rosenfeld and R. Karri. "Attacks and Defenses for JTAG". IEEE Design & Test of Computers, 27(1):36–47, 2010.

[8] B. Yang, K.Wu, and R. Karri. "Scan Based Side Channel Attack on Dedicated Hardware Implementations of Data Encryption Standard" . In Proc. IEEE International Test Conference (ITC), pages 339–344. 2004.

[9] K. Park, S. Yoo, T. Kim, and J. Kim. "JTAG Security System Based on Credentials". Journal of Electronic Testing (JETTA), 26:549– 557, 2010.

[10] B. Eklow and B. Bennetts. "New Techniques for Accessing Embedded Instrumentation: IEEE P1687 (IJTAG)". In Proc. IEEE European Test Symposium (ETS), pages 253–254. 2006.

[11] K. Agarwal. "Secure Scan Design", June 2011. US Patent App. 7,966,535.

[12] L. Sourgen. "Security Locks for Integrated Circuit", May 1992. US Patent App. 5101121 A.

[13] J. Lee, M. Tehranipoor, C. Patel, and J. Plusquellic. "Securing Designs against Scan-Based Side-Channel Attacks". IEEE Trans. on Dependable and Secure Computing, 4(4):325–336, Oct.-Dec.2007.

[14] K. Rosenfeld and R. Karri. "Security-Aware SoC Test Access Mechanisms". In Proc. IEEE VLSI Test Symposium (VTS), pages 100–104. 2011.

[15] F. Ghani Zadegan, U. Ingelsson, G. Carlsson, and E. Larsson. "Design Automation for IEEE P1687". In Proc. Design, Automation Test in Europe Conference (DATE), pages 1412–1417. 2011.

[16] J. Rearick and A. Volz. "A Case Study of Using IEEE P1687 (IJTAG)for High-Speed Serial I/O characterization and Testing". In Proc. IEEE International Test Conference (ITC). 2006. Paper 10.2.

[17] R. F. Buskey and B. B. Frosik, "Protected jtag," in 2006 International Conference on Parallel Processing Workshops (ICPPW'06), 2006, pp. 8 pp.–414.

[18] C. Clark, "Anti-tamper jtag tap design enables drm to jtag registers and p1687 on-chip instruments," in Hardware-Oriented Security and Trust (HOST), 2010 IEEE International Symposium on, June 2010, pp. 19–24.

[19] H. Little, J. Randell, R. Madter, and R. HICKEY, "Debugging port security interface," in Google Patents US20120278630, nov 2012.

[20] L. Pierce and S. Tragoudas, "Enhanced secure architecture for joint action test group systems," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 21, no. 7, pp. 1342–1345, July 2013.

[21] L. Pierce and S. Tragoudas, "Multi-level secure JTAG architecture," *-Line Test. Symp. IOLTS 2011 IEEE 17th Int.*, pp. 208–209, 13.

[22] S. Paul, R. S. Chakraborty, and S. Bhunia, "Vim-scan: A low overhead scan design approach for protection of secret key in scan-based secure chips," in 25th IEEE VLSI Test Symposium (VTS'07), May 2007, pp. 455–460.

[23] J. Dworak, A. Crouch, J. Potter, A. Zygmontowicz, and M. Thornton, “Don’t forget to lock your sib: hiding instruments using p1687,” in 2013 IEEE International Test Conference (ITC), Sept 2013, pp. 1–10.
[24] A. Zygmontowicz, J. Dworak, A. Crouch, and J. Potter, “Making it harder to unlock an lsib: Honeytraps and misdirection in a p1687 network,” in 2014 Design, Automation Test in Europe Conference Exhibition (DATE), March 2014, pp. 1–6.
[25] H. Liu and V. D. Agrawal, “Securing ieee 1687-2014 standard instrumentation access by lfsr key,” in 2015 IEEE 24th Asian Test Symposium (ATS), Nov 2015, pp. 91–96.
[26] R. Baranowski, M. A. Kochte, and H. J. Wunderlich, “Fine-grained access management in reconfigurable scan networks,” IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 34, no. 6, pp. 937–946, June 2015.
[27] G. E. Suh and S. Devadas, “Physical unclonable functions for device authentication and secret key generation,” in 2007 44th ACM/IEEE Design Automation Conference, June 2007, pp. 9–14.
[28] E. Ozturk, G. Hammouri, and B. Sunar, “Physical unclonable function with tristate buffers,” in 2008 IEEE International Symposium on Circuits and Systems, May 2008, pp. 3194–3197.
[29] Chang, Leland, David M. Fried, Jack Hergenrother, Jeffrey W. Sleight, Robert H. Dennard, Robert K. Montoye, Lidija Sekaric et al. “Stable SRAM cell design for the 32 nm node and beyond.” In VLSI Technology, 2005. Digest of Technical Papers. 2005 Symposium on, pp. 128-129. IEEE, 2005.
[30] Kumar, Sandeep S., Jorge Guajardo, Roel Maes, G-J. Schrijen, and Pim Tuyls. “The butterfly PUF protecting IP on every FPGA.” In Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on, pp. 67-70. IEEE, 2008.
[31] J. H. Anderson, "A PUF design for secure FPGA-based embedded systems," *2010 15th Asia and South Pacific Design Automation Conference (ASP-DAC)*, Taipei, 2010, pp. 1-6.
[32] K.Fruhashi, M. Shiozaki, A. Fukushima, T. Murayama and T. Fujino, "The arbiter-PUF with high uniqueness utilizing novel arbiter circuit with Delay-Time Measurement," *2011 IEEE International Symposium of Circuits and Systems (ISCAS)*, Rio de Janeiro, 2011, pp. 2325-2328.
[33] A. Maiti and P. Schaumont, "Improving the quality of a Physical Unclonable Function using configurable Ring Oscillators," *2009 International Conference on Field Programmable Logic and Applications*, Prague, 2009, pp. 703-707.