Securing IEEE 1687 Standard On-chip Instrumentation Access using PUF

Sudeendra kumar K, Naini Satheesh, Abhishek Mahapatra, Sauvagya Sahoo, K.K.Mahapatra
kumar.sudeendra@gmail.com, sauvagya.nitrkl@gmail.com, kmaha2@gmail.com
National Institute of Technology, Rourkela

***Abstract*- Large number of on-chip instruments support post-silicon validation, volume test, debug, diagnosis and in-field monitoring of an integrated circuit. The IEEE 1687-2014 (Internal JTAG or IJTAG) standard is an effective method for accessing the on-chip instruments. Streamlined access to on-chip instruments through IJTAG is prone to abuse and lead to security issues. An adversary can leak confidential data or get an access to design details of IC through IJTAG network. Recently, locking and unlocking mechanism for IJTAG is proposed to secure the access to on-chip instruments. This paper presents a novel Physical Unclonable Function (PUF) based secure access method for on-chip instruments which enhances the security of IJTAG network and reduces the routing congestion in an integrated circuit.**

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

I. INTRODUCTION

Modern day chips have become much complex in terms of transistor density, functionality, and speed of operation. Due to rising complexity, testing, characterization of chips is more difficult, time consuming and demand sophisticated test equipment. The shrinking time to market targets put pressure on product development cycle which includes test, validation and debug. In this connection, developing a different test programs for evaluation, volume production and for testing the device at the place of deployment is difficult. And also in complex chips, availability of access points in design to test the chip effectively is diminishing which affects test quality. It is difficult to sustain and improve test quality with conventional test methods and equipment. To address this issue, industry has embraced embedded instrumentation for test, debug and characterization of devices. Generally, on-chip instruments can be accessed through chip's JTAG port. The different varieties of on-chip test and debug instruments are used in devices: memory BIST, logic BIST, sensors, trace buffers, clock generators, bus logic monitors and radio tuners etc. JTAG standard 1149.1 is used widely in industry for test and debugging. JTAG TAP (Test Access Port) is used as interface between test equipment and design inside the device to drive test inputs and collect responses. Another standard IEEE 1500 boundary scan is used in core based designs [1]. Generally, on-chip instruments are accessed through JTAG TAP. The number of on chip instruments is increasing and accessing instruments through JTAG demand a streamlined procedure or standard. The goal of IEEE 1687 Internal JTAG (IJTAG) is to streamline the use of on-chip instruments [1]. IJTAG standard will work in tandem with other standards

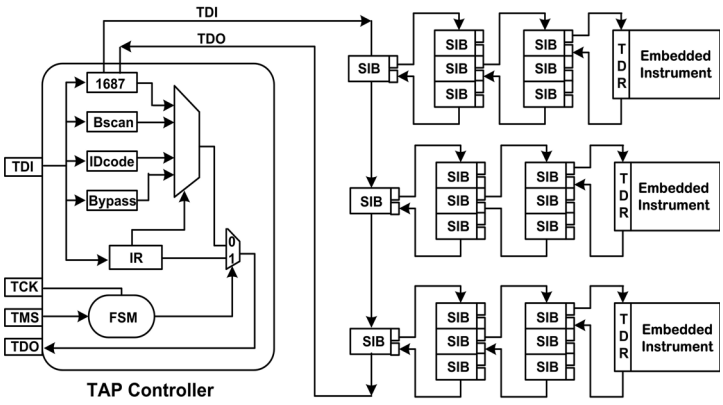

Fig. 1. Basic Structure of IJTAG Network

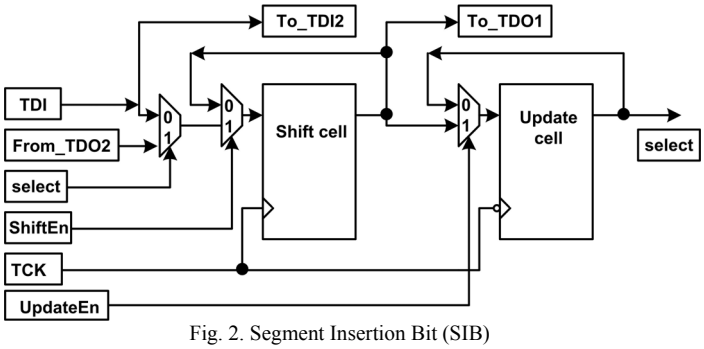

Fig. 2. Segment Insertion Bit (SIB)

(IEEE 1149.1, IEEE 1500 ECT) and is not a replacement to any standard which industry has already adopted and widely used. Activities associated with chip test, debug and on-field diagnosis use the different interfaces like IEEE 1149.1 JTAG, IEEE 1500 ECT for core test and Nexus standard for software debug. Addition of IJTAG standard will improve the use of embedded instruments.

IJTAG defines two languages: Instrument Connectivity Language (ICL) and Procedural Description Language (PDL). ICL describes the requirements for interfacing the instruments and PDL describes the operation of an instrument to facilitate the retargeting the vectors at chip level [1]. IJTAG is a broad standard and supports the structures of both IEEE 1149.1 and IEEE 1500 with ICL and PDL defined to support integration. The basic structure IJTAG network is shown in figure 1. The widely used JTAG 1149.1 TAP is used to communicate with embedded instruments in IJTAG network. Any IP (Intellectual Property) core, module or instrument can be accessed in

IJTAG network. IJTAG compatible instruments will have a digital interface like command register and associated commands to handle communication with TAP. A cell called Segment Insertion Bit (SIB) plays an important role in establishing communication between instruments and TAP. Inclusion or exclusion of SIB inserted in scan path will make or break the communication link with instrument. The SIB is also shown in figure 1. The diagram of SIB is shown in figure 2. The SIB is closed, when the value in the Update Cell and Select Signal is equal to '0', otherwise the SIB is considered open. The open status allows access to instruments. In a IJTAG network, anyone can shift the data into SIB and set the 1149.1 TAP to updateDR to open the SIB to access any confidential instrument [2][3]. More details on SIB can be found in [4].

We can find significant research literature coming out from both industry and academia related to IJTAG due to its flexibility. IJTAG is helpful in managing the number of on-chip instruments, but still there exist an open problems related to connecting few custom instruments which are incompatible, retargeting the test vectors for IJTAG, security, and access time optimization. In the list of open problems, security of the device is of prime importance. The well-known hardware security threats can be categorized as: Hardware Trojans, counterfeit devices, side channel attacks on cryptographic circuits and IP (Intellectual Property) theft [5]. The easy and improved access of on-chip instruments in IJTAG framework may increase the probability of successful attacks on IP, cryptographic circuits and other sensitive sections of the chip. On-chip instruments and scan infrastructure can be used for attacks [6]. Attacks and countermeasures against 1149.1 TAP are reported in [7]. An adversary can make use of well-structured IJTAG network to design attacks to leak secret data, IP theft and to understand chip internals. Authentic access to instruments will prevent IP theft or tampering and other security attacks. In an unsecured IJTAG access, adversary can shift appropriate data into SIB and use UpdateDR (update data register) instruction to open any SIB and gain an access to any sensitive instrument. An attacker can investigate the IJTAG network by pumping logic 0 or 1 randomly and open the SIBs and get access to instrument behind SIB.

In this paper, we present a security scheme to prevent the attacks on IJTAG network. And also, we discuss the security aware access management in complex IJTAG network. The presented mechanism assures authorized and authentic entities are allowed to use instruments. The next section discusses earlier endeavours to address the security of IJTAG. Section III introduces physical unclonable function (PUF), used in security design, section IV presents proposed technique and section V discusses security analysis. Finally, section VI concludes the paper.

II. PRIOR WORK

To introduce the security aspect into IEEE P1687, locking SIB (LSIB) was proposed in [2]. The same authors extended and introduced several types of LSIB using n-bit signals to gate UpdateDR [3]. SIB will remain closed or locked until correct key is applied. To make the attack difficult, trap-bit SIB is designed in [3]. Authors of [8] propose a LFSR based key generation mechanism to further enhance the security. LFSR is designed by reconfiguring the scan flip flops which generates key to open the SIB. Security analysis is discussed with various attack models in above mentioned literature. The major drawback of above mentioned techniques is static password. Key is same for all chips produced. The password is distributed to all authorized entities through some encryption mechanism, still there is a probability of the secret key getting leaked and security is compromised. An authorized user can share key with adversary. Another weakness is the limitation on the length of the key will depend on the size of AND gate used for key comparison routing problem may arise when the number of instruments increase and make this technique not scalable. The LFSR based security scheme proposed in [8] is more secured than above techniques and it is shown in the analysis that, it takes several hundreds of years for adversary to break the system, when key is unknown. A password to unlock SIB is static and authorized entities can share key with adversary. Researchers of [9] address the problem of static password and scalability. In the IJTAG based Reconfigurable Scan Network (RSN) in [9], makes use of hash function core and secret memory to design authorization mechanism to lock and unlock the SIB. The technique proposed and implemented in [9] has got following characteristics: Passwords are stored in secret memory and no need to share password with any end-user. The protected instruments are used through scan chain and there will be minimum routing congestion.

The proposed technique in [9] carries a few disadvantages also. They are: even though scan network is used to access instruments, the routing congestion depends upon location of hash function core, secret memory and authorization controller. Increase in number of instruments lead to routing congestion, which affects the scalability of the technique. Secondly, synthesis of secret memory is difficult issue to achieve, which is not explained. Thirdly, SIB interfaced with authorization controller needs modification as S^2IB (Secure Scan chain SIB) and finally, RSN access has not considered taxonomy of instruments based on their compatibility with previous JTAG standards and their functional requirement.

In this work, we address the disadvantages of [9] and our technique has got following features:

- Similar to [9], our technique support dynamic password for authentic users. Addition to that, passwords can be configured for each instrument.
- In the proposed technique, Physical Unclonable Function (PUF) is used and its placement beside the SIB in the IJTAG network causes no routing congestion.
- Taxonomy of instruments is taken into consideration in designing hierarchical IJTAG network which is useful in securing the access to instruments.
- The each chip produced will have a unique password for every on-chip instrument.

The on-chip instruments can be categorized based on their interface features with 1149.1 JTAG and also based on their functionalities. The on-chip instruments can be classified as Type A, Type B, Type C and Type D based on their connectivity with 1149.1 JTAG. This classification of IJTAG instruments is described in [10]. Further, IJTAG instruments can be categorized based on their functionality: Built in Self-Test (BIST) instruments, Environmental monitors (sensors), Process monitors, Debug capabilities and functional configuration registers [11]. The classification, description, usage of on-chip instruments is summarized in Table I.

III. PHYSICAL UNCLONABLE FUNCTION

The Physically unclonable functions (PUF) are promising hardware security primitive used in authentication applications and cipher key generation. Storing the secret data or key is vulnerable to various types of attacks. PUF circuit responds to challenge with unique response. PUFs derive a secret key in the form of unique response to a given challenge from the process variation that occurs during the chip fabrication [12]. With full knowledge of PUF circuit, it is nearly impossible to manufacture an identical circuit with same characteristics. The quality of PUF is determined based on its features like uniqueness, reliability and uniformity. The internal manufacturing process variability of PUF in each device is hidden, unique and distinct, which is useful in key generation for security applications. The more explanations on PUF and its characteristics can be found in [12]. Different types of PUF circuits are described in literature and we have to choose a PUF with better uniqueness and reliability in its CRPs for our applications. Composite PUF described in [13] is a strong PUF with acceptable levels of uniqueness and reliability [13]. The comparison between PUF is briefly described in [14]. In designing security of IJTAG network, composite PUF is used in this work.

IV. SECURE SIB AND IJTAG NETWORK USING PUF

A. Secure SIB using PUF:

To access the TDR of embedded instruments, one or more SIBs need to be opened. The diagram of SIB is shown in figure 2. SIB will be in a close state when select is '0'. When SIB is in a close state, TDI will be the input and scan out will be from To_TD0. Depending upon the placement of instrument in the scan path, number of SIBs will be getting opened to establish the connection. When shift cell of SIB is 1 and after updateDR command the value is clocked into update cell. To open the lock of SIB, the signal Update should become logic '1'.

The proposed PUF based secure SIB is shown in figure 3. In this work, the concept of using LFSR in [8] is extended to make the security system more effective. CRP's of PUF will make dynamic passwords for each instrument and user. Challenge to the PUF is fed through TAP controller (using TDR). The PUF generates the corresponding unique response. LFSR design is known and its output equal to the response of PUF will be produced at some cycle. That cycle number can be calculated and exactly at that particular cycle, SIB will get unlocked when XOR network produces logic 1 on Update signal. The key (challenge to PUF and cycle information) is shared with authentic users to use instruments. The key and cycle number will vary from chip to chip and also instrument to instrument in the same chip. This arrangement makes instrument more secure and key dynamic.

B. Secure IJTAG Network Design:

To prevent IP theft, tampering and other attacks on security, access to instrument infrastructure at various levels need security aware network design. Few instruments are required during product development activities like evaluation of new silicon, bench testing, characterization and test program development for production ramp-up. In debug and diagnosis of device, a moderate level of security is required. During in-field operation and maintenance, the secure access to instrument must be at place to prevent secret data, IP etc. During silicon bring up, access to all instruments is required these activities are performed in test labs which are considered safe. The passwords to unlock the secure SIB can be shared with test lab personnel. Secondly, instruments used for application development (software's like device driver etc) AND debugging is performed using 1149.1 compatible instruments (Type-B) and self- instructed instruments (Type-C). All these instruments can be kept as one cluster accessed through common password protected SIB. Finally, the instruments required for diagnosis, debug, in-field testing and maintenance can be clustered under one secure SIB. The diagram of secure IJTAG network is shown in figure. 4.

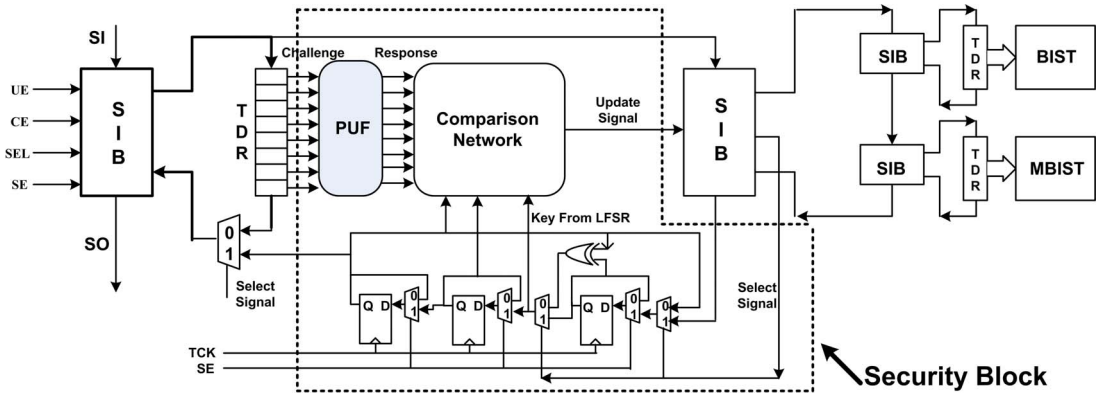

Fig. 3. Segment Insertion Bit (SIB) with Security Block

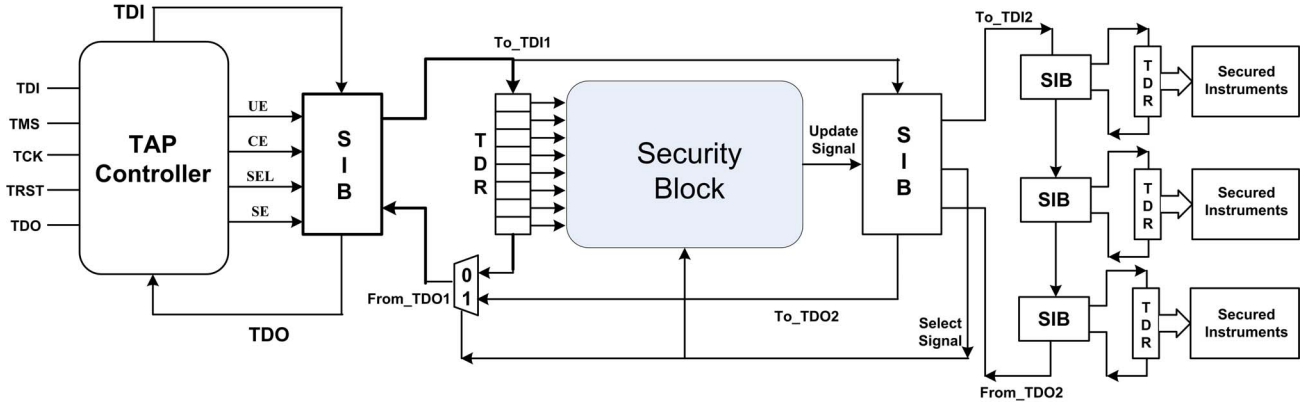

Fig. 4. Proposed Secure IJTAG network

TABLE I
TAXONOMY OF IJTAG INSTRUMENTS

Type	Class Description	Example	Functional Description	Use in test/debug/diagnosis in field
A	Self- contained instruments generally not compatible with 1149.1 and controlled by static signals applied on 1149.1 and sampled by capture-DR.	Logic BIST, Memory BIST	A System level instruments used in testing and debugging.	BIST is used in post silicon validation and production testing of devices. Generally not used in diagnosis.
B	1149.1 compatible instruments having serial scan path, directly managed by 1149.1 JTAG FSM.	JTAG Trace buffers used in application debugging	Traditional Debug instruments coming along with standard 1149.1 JTAG	These instruments are used in evaluation testing and application debugging.
C	Self-instructed instruments having dedicated control and data registers responsive to select-IR states. Generally Debug blocks come under this type.	Processor debug blocks like ETM and Nexus	Advanced Debug instruments deployed to observe and control important IP's like processor, crypto processor etc during diagnosis.	These instruments are used, diagnosis and in-field testing.
D	A signal or data of instrument is accessed with a clock other than 1149.1 TCK. Similar to Bus controllers in IEEE 1500 ECT.	Bus controllers, Functional configuration controllers.	Instruments used to observe bus signals and to programme a value into the registers of IP cores.	These instruments are used in device characterization, diagnosis and in-field testing.

The secure IJTAG network can be custom designed for given requirement. Each instrument can be made secure by an attachment of security block. The LBIST used to test the cryptographic circuit can be placed in a secured network to avoid DFT based side-channel attacks [6]. The advantage of this system is there is no need to make all SIBs secure and no modification of standard SIB defined in IEEE 1687. The secure JTAG network is shown in fig. 4. In fig. 4 shows the connection of JTAG compatible instruments in a secure network with security block. Instruments which are not compatible with JTAG can be connected in the similar way as shown in fig 3. The primary SIB in the fig. 3 can be controlled by any other wireline communication protocol like SPI or I2C, which is supported in IEEE 1687-2014 standard.

V. Implementation and Results

A. Implementation:

The secure instrument access is designed and its functionality is described in above sections. The key components used in designing the security block are: - Physical Unclonable function, LFSR and XOR network.

Physical unclonable function (PUF) plays a key role in securing the access to the instrument. The composite PUF [13] is used to generate the challenge-response pairs. LFSR is used to enhance the security. A 16-bit PUF is used in the design, which can generate 65535 CRP pairs. In tandem with PUF, 16-bit LFSR is used to generate the response of PUF to unlock the SIB at a pre-defined cycle. The authentic user will be provided by key (challenge to PUF) and number of cycles, the user has to run the LFSR to unlock the SIB. Each instrument in the chip can be locked and unlocked with a unique secret.

The complete system which include TAP controller, SIB, TDR, PUF, LFSR and XOR network is implemented in Verilog HDL and verification of design is performed using Synopsys VCS tool. The PUF based secure IJTAG network is implemented in both ASIC and FPGA. The result for ASIC implementation is shown in Table 2. ASIC implementation is performed using TSMC 65nm standard cell library. Synopsys Design compiler is used for synthesis and Cadence SoC Encounter is used for automatic place and route. The complete system is also validated on Xilinx Spartan 3E FPGA with 16-bit security block (16-bit PUF and 16-bit LFSR).

Table II
Area of security block (PUF + XOR network + LFSR)

No. of clusters	Area (in sq. microns) (Only Security Block)		
ASIC Implementation	8-bit PUF with 8-bit LFSR and XOR network	16-bit PUF with 16-bit LFSR and XOR network	32-bit PUF with 32-bit LFSR and XOR network
1	730	1036	1508
2	1522	2101	3090
3	2230	3190	4601
4	3042	4210	6104

Assuming one cluster needs one Security Block

B. Performance overhead:

The authentic user with key and number of cycles to run LFSR can unlock the SIB. This access authorization 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 16-bit PUF challenge, it needs 16 cycles+2 cycles to pump the challenge into the PUF.
- Assuming that, the LFSR generates the PUF response after 'N' cycles.
- And another two clock cycles to unlock the SIB.

The total clock cycles can be calculated as: 5+16+2+N+2 = N+25 TCK (JTAG clock) cycles are required to unlock the SIB for authentic user. The value of 'N' varies from an 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.

C. Security Analysis:

The proposed secure access management technique will enhance the security at normal conditions. The key element is PUF and overall security depends on the performance of the PUF. The different attack scenarios are discussed below:

- Case 1: The adversary assumes it is static key and with no knowledge of LFSR, it is very difficult to unlock the SIB and probability of success is very less.
- Case 2: The adversary knows that, PUF and LFSR are implemented, and then he may have confusion on length of the key (challenge to PUF). Guessing the length of the key and LFSR cycles, adversary has to try for all possible 65535 keys and for the same number of cycles (similar to brute force attack). This is impossible as it takes several years to break. The numerical analysis for this case is similar to the condition -2 in [8].
- Case 3: Each chip and instrument cluster or instrument will have different key and different cycles for LFSR to unlock the SIB. Adversary will get no information from the data of other chips. The successful key and cycle information of LFSR of other chips will be not useful to break security of a given chip.

After the manufacturing of chips, the CRP's of PUF and LFSR cycles must be collected in a trusted environment. The complete CRP data can be stored in a secure database of design house/original component manufacturer. The design is not verified for fault attacks like voltage variations, attacks on clock and EM waves attack.

D. Discussion:

- The number of CRPs collected in our work is 5000. The number of CRPs can even more or less

depending on the number of chips produced and other requirements. There is no standard available for how many numbers of CRPs should be collected in device authentication, hardware metering and counterfeit litigation.

- The PUF implementation used for securing the IJTAG can be used for IP protection, cryptographic key generation in other applications.
- The four clusters are designed to implement the IJTAG network. Clusters can be designed according to design requirement. Clustering of instruments can also be based on taxonomy as shown in Table 1. In this work, four clusters are created based on security requirement. In cluster-1, instruments used in production testing like BIST, JTAG for manufacturing testing is included. Cluster-2 consists of debug instruments like trace buffers, processor debug blocks. Cluster-3 consists of characterization instruments like process monitors, bus controllers and functional configuration registers. And finally in cluster-4 can have any sensitive IP core which needs protection can be accommodated. In this work, we have placed SCI (Serial Communication Interface) controller as an example in cluster-4. The area requirement of security block is shown in Table-2. Security block can be designed with 8-bit, 16-bit and 32-bit size of PUF and LFSR circuit. A brute force attack can easily break the 8-bit PUF and LFSR. 32-bit size PUF and LFSR will give good security, but this comes at the cost of area and access time.
- The comparison of different techniques with proposed method is shown in Table 3. 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. Dynamic passwords come at the cost of area and access time. Relative comparison for different parameters is shown in Table 3. In this work, due to clustering of instruments and number of secure SIBs are small in number and problem of routing congestion does not arise. In [9], connecting the output of hash function to SIB to unlock is required. Congestion depends upon the placement of hash core and number of SIB's in the IJTAG network. Scalability is affected as routing congestion increases with number of SIB's in the network. In proposed design we have used only five Secure SIBs at appropriate places on the scan chain. Access time to unlock the SIB for one session is higher in proposed technique than the technique used in [9].

TABLE III
COMPARISON OF PROPOSED METHOD WITH OTHER IJTAG SECURITY SCHEMES

Parameter	Paper [2]	Paper [3]	Paper [8]	Paper [9]	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

NA: NOT APPLICABLE

VI. CONCLUSIONS

The PUF based secure access system for on-chip instruments in IJTAG is proposed and implemented. The FPGA emulation of the same is also performed. The security system is important for the system security and safety. The CRPs of PUF are used as keys to lock and unlock the SIBs in the IJTAG network, which give access to on -chip instruments. In the proposed secure IJTAG network, with minimum number of secure SIB implementation, a cluster of on-chip instruments can be protected. The major advantages of proposed PUF based security are: dynamic passwords for each chip and instruments and no routing congestion in comparison with earlier techniques.

REFERENCES

[1] J. Rearick, *et al,* "IJTAG (Internal JTAG): A step toward a DFT standard" in *Proc. IEEE Int.Test Conf. (ITC),* Austin, TX, USA, 2005.

[2] J.Dworak, *et al*, "Don't forget to lock your SIB: Hiding Instruments using P1687", in *Proc. International Test Conference, 2013*.

[3] A. Zygmontowicz, J. Dworak, A. Crouch, and J. Potter, "Making it Harder to Unlock an LSIB: Honeytraps and Misdirection in a P 1687 Network", in *Proc. DATE Conf.* Mar. 2014.

[4] IJTAG, "IJTAG – IEEE P1687", http://grouper.iee.org/groups/1687.

[5] M. Tehranipoor and C. Wang, "*Introduction to Hardware Security and Trust*", Newyork, NY, USA; Springer-2011.

[6] J. Da Rolt et al., "Test versus Security:Past and Present", *IEEE Trans. Emerg. Topics in Computing*., vol.2, no. 1, pp. 50-62, Mar. 2014.

[7] L. Pierce *et al,* "Enhanced secure architecture for joint action test group systems," *IEEE Trans. On VLSI*.., vol. 21, no. 7, , Jul. 2013.

[8] Hejia Liu and Vishwani D. Agrawal, "Securing IEEE 1687-2014 Standard Instrumentation Access by LFSR Key", in *Proc. IEEE Asian Test Symposium* . Nov. 2015.

[9] Rafal Baranowski, Michael A. Kochte, and Hans-Joachim Wunderlich, "Fine-Grained Access Management in Reconfigurable Scan Networks" *IEEE Trans. on CAD of integrated circuits and systems,* June-2015.

[10] N. Stollon, *On-Chip Instrumentation: Design and Debug for Systems on Chip*. New York, NY, USA: Springer, 2011.

[11] IEEE-1687- IJTAG: Future for On-Chip Embedded Instruments- tutorial http:// www.asset-intertech.com/eresources/ieee-1687-ijtag-future-embedded-instruments.

[12] G.E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation", *in proc. 44th ACM/IEEE Design Automation Conference (DAC '07*), pp.9-14, 2007.

[13] Sahoo, *et al*, "Composite PUF: A new design paradigm for Physically Unclonable Functions on FPGA "*IEEE International Symposium on HOST,* May 2014.

[14] Abranil Maiti et. al, "A Systematic Method to Evaluate and Compare the performance of PUF". IACR Cryptology, 657, 2011.