PUF-based Secure Test Wrapper for SoC Testing

Sudeendra kumar K, Saurabh Seth, Sauvagya Sahoo, Abhishek Mahapatra, Ayas Kanta Swain, K.K.Mahapatra
kumar.sudeendra@gmail.com, saurabhseth.030@gmail.com, sauvagya.nitrkl@gmail.com, kmaha2@gmail.com
National Institute of Technology, Rourkela

***Abstract*- The increased testability and observability due to test structures make chips vulnerable to side channel attacks. The intention of side channel attack are leaking secret keys used in cryptographic cores and getting access to trade related sensitive information stored in chips. Several countermeasures against test based side-channel attacks are available in research literature. One such countermeasure scheme is password based access protection to IEEE 1500 test wrapper, such that only an authentic user with valid password is allowed to access the test structures. IEEE 1500 is a core test standard for enabling the streamlined test integration and test reuse. The trust model of existing schemes assume outsourced assembly and test (OSAT) centre are completely trusted and design house will share secret keys to unlock the IEEE 1500 wrapper during testing. In this paper, we propose a Physical Unclonable Function (PUF) based technique incorporating challenge-response to support comprehensive test security in which there is no need for design house to share secret keys with untrusted OSAT centre to unlock the scan chains. The proposed scheme comes at the cost of reasonable area and performance overhead.**

***Keywords:* IEEE 1500, Physical Unclonable Function, Hardware Security.**

I. INTRODUCTION

Scan chains are common Design for Testability (DFT) structures found in modern day chips. DFT structures are used for better controllability and observability of the design during testing. DFT structures which are useful in testing are misused to leak confidential data through side channel attacks (SCA) [1]. Adversary will use SCA to leak secret keys used in encryption and critical data related to design. Different types of countermeasures to prevent SCA can be found in research literature [1]. The well-known countermeasures are: - partial scan design [2], scan compression schemes [3], obfuscation of scan chains [4], defusing the test pins [5] and secure test wrappers to prevent unauthorized access [6-8].

IEEE 1500 is a core test standard for enabling the streamlined test integration and test reuse. The IEEE 1500 standard defines the serial and parallel test access mechanisms and instructions for testing the embedded IP cores in a System on Chip (SoC). Security against DFT based SCA can be achieved by restricting the illegitimate access to IEEE 1500 wrapped cores in the chip. Countermeasures against attacks on IEEE 1500 wrapped cores have been proposed, including the following: -

- Authors of [6], propose a challenge-response based secure test access mechanism using KATAN lightweight block cipher. On-chip True Random Number Generator (TRNG) generates the random number and sends it to on-chip block cipher and also to ATE (Automatic Test Equipment). KATAN block cipher is also implemented on ATE as a software program. Both device under test and ATE run the same block cipher (KATAN) and generate same cipher texts for same secret key. On-chip comparator compare the cipher text coming from ATE and on-chip block cipher and generate the signal to enable the access to test wrapper after a successful match.
- Key based secure test wrapper (STW) for IEEE 1500 is proposed in [7]. IEEE 1500 test wrapper is unlocked when golden key is applied. The predefined seed is loaded into LFSR to generate the golden key. The test input bit stream should initially contain the key from ATE and it is compared with golden key generated by LFSR. After the successful comparison, wrapper enters the unlock state. The part of the scan chain is configured as LFSR to reduce the area [7]. The design changes in IEEE 1500 standard are required to implement this security scheme, which may not be accepted by all SoC integrators and IP core vendors.
- The Secure Test Wrapper (STW) proposed in [8] replaces the KATAN block cipher with physical unclonable function (PUF). PUF circuits are security primitives, which generate unique response for a given challenge. The PUF circuit exploit random process variations occurring during chip fabrication which makes challenge-response pairs (CRPs) are unique for a given chip [9]. In this technique, PUF CRP will be stored in ATE memory during production testing. This will add to test cost due to higher test time and utilization of tester memory.

In the current era of globalization, most of the post silicon validation procedures are outsourced to offshore OSAT (outsourced assembly and test) centres. In the earlier techniques discussed above, test centres (OSAT) are completely trusted and design house will share the secret keys/PUF CRPs with test centres to unlock the scan chains during testing. Sharing keys with 3rd party test centre may compromise the security of chip. In this paper we present a STW technique which has following advantages: -

- Design house need not to share any secret key to unlock the IEEE 1500 wrapper for testing with untrusted OSAT centres. The proposed technique prevents adversary in OSAT centre getting access to confidential information related to keys used to unlock the cryptographic and other sensitive cores.
- No changes required for IEEE 1500 standard.
- Unique keys for every chip manufactured.

The paper is organized as follows: The prior work and related background is discussed in section II and we discuss the design and functioning of proposed PUF based STW scheme

2159-3477/18/$31.00 ©2018 IEEE
DOI 10.1109/ISVLSI.2018.00127

in section III. In section IV, we present the implementation details and analysis and finally section V concludes the paper.

II. BACKGROUND

A. IEEE 1500 Core Test Standard: IEEE 1500 standard defines core wrapper and test specific language called core test language (CTL). CTL acts like a bridge between core providers and core integrators to exchange design details. The language is known as core test language (CTL). Fig 1 shows the IEEE 1500 test wrapped core.

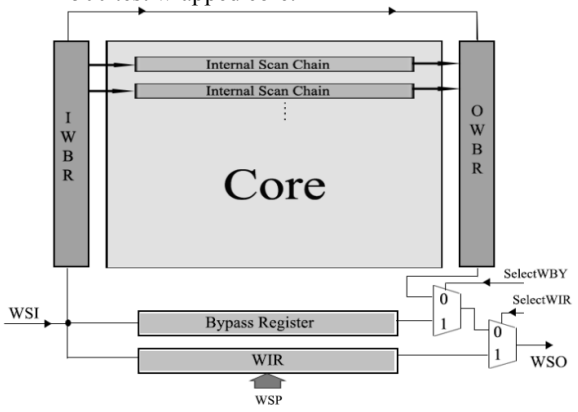

Fig. 1. IEEE 1500 Test Wrapped Core

IEEE 1500 standard define two ports: wrapper serial port (WSP) and wrapper parallel port (WPP). WSP is mandatory and WPP is optional. WSI (Wrapper Serial In) is basic serial input and WSO (Wrapper Serial Output) is basic serial output in WSP. IEEE 1500 standard defines three mandatory registers: - Wrapper Instruction Register (WIR), Wrapper Bypass Register (WBY) and Wrapper Boundary Register (WBR). Depending on the test requirements, any number of user specific registers can be added to wrapper. User specific registers are called Wrapper Data Registers (WDR). WBY provides a bypass path and connects WSI and WSO in bypass mode or functional mode. WIR generate the control signals to enable all wrapper operations. The test data stimuli and responses are captured using WBR register. WBR is used to test the core logic and also to test external connectivity to other cores and I/O ports. WSP comprises of ten terminals in which eight are mandatory and two are optional. The WSP signals are described in Table I.

The instruction loaded into WIR and control signals determine the mode of operation of the wrapper. IEEE 1500 supports 11 instructions, in which three are mandatory: WS_BYPASS, WS_EXTEST and WX_INTEST. The WS_BYPASS instruction is selected, when no test operation is required. This instruction connects WBY between WSI and WSO. WS_EXTEST instruction allows testing of off-core circuitry and core to core interconnections. In INTEST mode, the input test vectors are applied to the core and test response is observed. More details on the IEEE 1500 standard can be found in [10]. Fig. 2 shows the schematic of wrapper boundary cell. The WBR is constructed using WBR cells and each cell has four data terminals: cell functional input (CFI), cell functional output (CFO), cell test input (CTI), and cell test output (CTO). Cell functional input (cfi) and cell functional output (cfo) connects to the core functional path. In normal mode of the core, these terminals are used to perform functional operation of the core logic.

TABLE I
IEEE 1500 WRAPPER SERIAL PORT (WSP) SIGNALS

Signal	Description
WRCK	IEEE 1500 Wrapper Clock
WRSTN	IEEE 1500 active low wrapper reset. When reset is asserted, WS_BYPASS will be active.
SelectWIR	When SelectWIR is asserted, the WIR is selected and connected between WSI and WSO. Opcodes for operations like "shift", "update" and "capture" are loaded into WIR.
CaptureDR	When CaptureDR is asserted, the data present on the functional input is stored into WBR cell.
ShiftDR	When ShiftDR is asserted, the data stored in any register connected between WSI and WSO is shifted to next position upon the rising edge of WRCK.
UpdateDR	When UpdateDR is asserted, the data stored closest to shift output is loaded into off-shift storage element.

The cell test input (cti) and cell test output (cto) are test inputs to the core from WBR cell. Core test input (cti) connects to the scan input pin and core test output (cto) connects to the scan output pin on the scan path of the core. The control signals (shift_en, capture_en, safe_control, shift_clk) are sourced from the WIR to enable the shift, capture and update operations in the WBR cell.

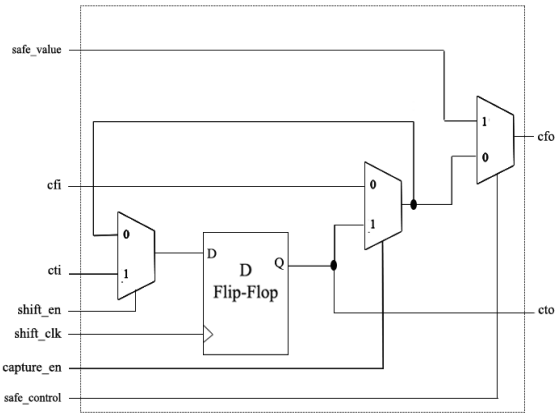

Fig. 2. Wrapper Boundary Cell

B. Physical Unclonable Functions: PUFs are well known hardware security primitives used in identification, authentication and cipher key generation. Even with a full knowledge of PUF design, it is nearly impossible to manufacture an identical PUF circuit which generate same CRP pairs. PUF circuits are used in variety of hardware security applications like IP protection, hardware metering and cryptographic key generation [11]. The quality of PUF is determined based on its CRP features like uniqueness, reliability and uniformity. More details on PUF design, characteristics and applications can be found in [12]. In this work, PUF is used to design the secure test wrapper to prevent unauthorized access to test structures of cryptographic and other critical IP cores.

C. Prior Work: - The secret key or any other confidential information can be ascertained by running an encryption in functional mode and switching the chip to test mode at appropriate time. Adversary can successfully uncover the secret key through scan based attack. In this work, we mainly focus on password protection schemes on IEEE 1500 standard. As mentioned above, challenge-response based test security schemes for IEEE 1500 wrapper is described in [6] [7] and [8].

In this work, we present the novel and improved challenge-response based test security technique which addresses the following issues: -

- PUF based STW support unique keys for every chip manufactured. In the PUF based STW proposed in [8], there is a need to share the PUF-CRP data with OSAT centre. Full CRP data or partial CRP data with test centre or with any other third party is not secure. Adversaries will perform model building attacks using the available CRP data, which compromise the complete security of the chip [15]. And also, there is a need to store CRP data in ATE, which increases test cost [16]. In the proposed PUF based STW scheme, there is no need to share PUF CRP data with untrusted OSAT centre.
- Block cipher (KATAN) based STW discussed in [6], does not support unique key for all manufactured chips. KATAN algorithm running on ATE will add to test time which will increase the test cost. Secret keys to unlock the test structures are shared with OSAT centre. In the proposed scheme, there is no need to share PUF CRP data with untrusted OSAT centre The increase in the test time in the proposed scheme is minimal in comparison with earlier schemes.
- The STW proposed in [7] does not support unique key for each chip manufactured and modifications to the IEEE 1500 standard wrapper is required. The golden key is part of test program and adversary in OSAT centre can easily retrieve the key from test program. The proposed PUF based STW scheme, there is no need to share any confidential information with OSAT centre and there is no need to change standard wrapper and also support unique password for each chip manufactured.

III. PUF BASED SECURE TEST WRAPPER

In this work, we propose a PUF based secure test wrapper activation mechanism, which support secure key management between the design house/SoC integrator and test house (OSAT centres). With this scheme, only genuine test centre or authentic test engineer will have an access to test structures.

A. Trust Model and Assumptions:-

The stakeholders of semiconductor supply chain are: Chip design house/SoC integrator, contract manufacturer (fabrication unit) and OSAT centre. Fabless companies must take more security measures than fab-owned companies. In the fabless model, design (GDS II) is shared with contract manufacturer and chips are packaged and tested at OSAT centres. These three entities are located in different parts of the world. The lack of trust between the three entities has led to several security issues in recent times. Design house/Original Design Manufacturer (ODM) will lose in terms of both revenue and reputation when security issues are compromised. ODM/Design house is a direct victim when security lapses. In our trust model, we consider ODM can be completely trusted and it is assumed that foundry and OSAT centres should not get access to PUF CRP data during wafer probing or final test (production testing).

B. PUF Enrolment: - Every PUF based hardware security application requires an enrolment phase. In this enrolment phase, PUF challenge-response pairs are collected and stored as reference database. Generally, the PUF CRP collection is performed on ATE at OSAT centre. The Fig. 3 shows the schematic of the proposed PUF based STW technique. The proposed scheme comprises of PUF, TRNG, RSA, OTP and comparator circuit. The challenge to the PUF is fed through the TDR (test data register) connected with JTAG pins of the chip. TDR is serially fed from TDI pin of JTAG and challenge stored in TDR is given to PUF inputs in parallel. In this work, custom made TDR is serial in parallel out register. The response of the PUF is encrypted using on-chip RSA encryption block. The public key is shared with OSAT centre to encrypt the PUF response using RSA. After completion of PUF CRP collection, the data stored in OTP (one time programmable) memory is encrypted using RSA. The TRNG will generate random number when chip is powered and random number is stored in OTP. The random number stored in OTP is permanent. The OSAT centre will send the challenges and encrypted PUF responses and encrypted TRNG value with respective chip ID to design house. The design house will decrypt the PUF responses and TRNG value and create a database of with chip ID, PUF CRP and TRNG value.

C. Secure Test Wrapper Activation: - The comparator circuit generates the 'unlock' signal (active high), when the comparison between value stored in the TRNG and PUF response match. The enable signal is used to gate the wrapper clock (WRCK) of IEEE 1500. When enable is high, wrapper clock is allowed into IEEE 1500 wrapper. Design house will choose the appropriate PUF challenge which will generate the TRNG value from the CRP database. The appropriate response with chip id is communicated to OSAT centre to unlock the wrapper. The PUF response and TRNG value are compared in comparator and 'unlock' signal is generated. Strong PUF with very large number of CRPs must be employed to avoid failures in unlock mechanism. The TCK clock (from JTAG) is connected to IEEE 1500 standard clock (WRCK). Inserting two input AND gate with 'unlock' signal and clock signal is used for gating the clock. Similarly, the unlock signal can be used to gate the 'cti' input (test input to wrapper) or WRSTN (wrapper reset).

The OSAT centre will have an access to encrypted responses coming out of RSA during CRP collection and encryption safeguards the PUF responses. During testing, PUF challenge with a corresponding chip Id is shared with OSAT centres to unlock the test access.

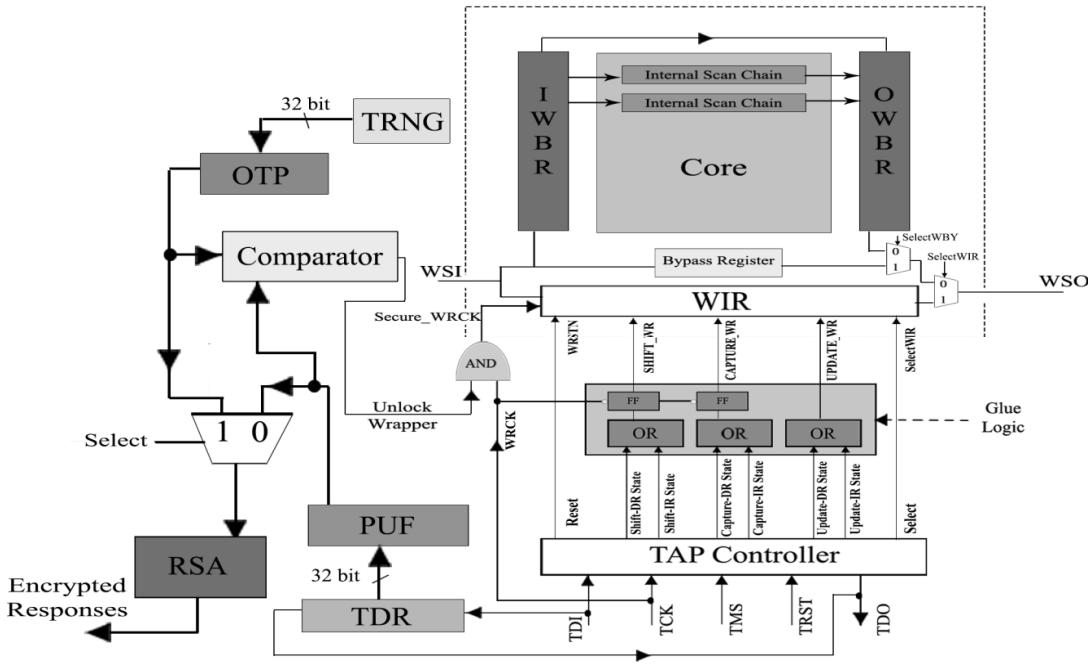

Fig. 3. Proposed PUF base Secure Test Wrapper

TABLE II
TAXONOMY OF IJTAG INSTRUMENTS

Parameter	Paper [6]	Paper [8]	Paper [7]	Proposed
Method	Block Cipher(KATAN) based scheme	PUF based scheme	LFSR based key generation scheme	PUF based scheme
Password	Static. All chips manufactured will have same 80-bit password, which is stored in secret memory.	Dynamic. PUF circuit support different password for every chip manufactured.	Static. Golden key is stored in memory, which is compared with key coming from test program to unlock test.	Dynamic. PUF support different password for every chip.
Modifications to IEEE 1500 standard to add security	Minimum modification	Minimum modification	Major modification to include security.	Minimum modification
Security	Secret keys are shared with OSAT centre. Adversary in OSAT centre will get an access to secret key which compromise security.	PUF CRP is shared with OSAT centre. Adversary in OSAT centre uses PUF CRP to unlock wrapper and perform SCA.	Adversary in OSAT centre will get an access to golden key through reading the memory or by analysing the test program, which contains key to unlock test structures.	There is no need to share secret key or any confidential information with OSAT centre.
Area Overhead	High. Due to inclusion of Block cipher and secret memory	High. Due to inclusion of PUF	Low. No large extra circuits added. Scan chains are used as LFSR.	High. Due to inclusion of PUF and RSA.
Effects on Test Time/Test Cost	Medium. RS-232 interface is used to unlock the scan chain which adds to test time. Executing the KATAN cipher on ATE adds to test time.	High. RS-232 interface is used to unlock the scan chain which adds to test time. PUF CRPs are stored in ATE memory which adds to test cost.	Very less. This scheme has no effect on test time or test cost. Key is fed into device under test as a part of scan test input. JTAG interface is used to connect with wrapper.	Medium. Unlocking the scan chains takes reasonable amount of test time. JTAG interface is used to interact with wrapper.

In the proposed technique, there is no need to share the PUF CRP with OSAT centre and an adversary in OSAT centre will not get an access to it. So the proposed security scheme is safe.

IV. Implementation and Analysis

A. Implementation: - The key components of PUF based STW are: - PUF, Comparator circuit, TRNG, RSA, OTP and custom TDR. Physical unclonable function is designed to get 32-bit response. The PUF design presented in [17] is used in this work. The Ring Oscillator (RO) PUF described in [17] will consume less number of RO's and capable of generating multiple output bits from each RO. The structure of RO PUF presented in [17] is shown in Fig. 4.

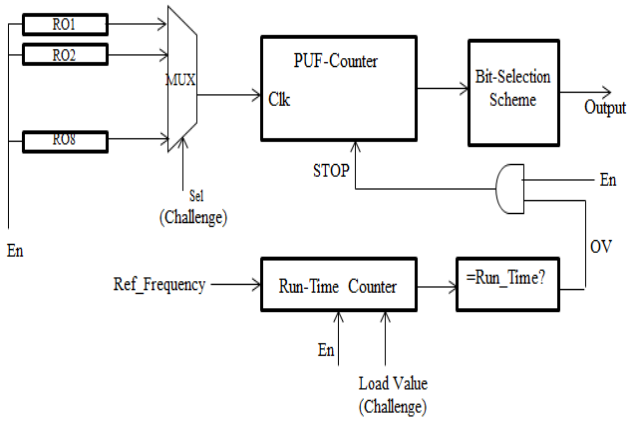

Fig. 4. Structure of Physical Unclonable Function

A runtime counter is connected with standard clock source which acts like a reference clock. The runtime counter is loaded with 'load value', from which it starts counting based on the reference clock. The challenge to PUF comprises of two components: - 'load value' to run-time counter and select lines to multiplexer. Once challenge is fed, the enable signal will trigger the RO and runtime counter at the same time instant. The runtime counter will drive the signal OV to logic '1' when it overflows, which in-turn drive the signal 'STOP'. The signal 'STOP' will stop the PUFcounter from counting. The bit selection scheme selects the bits from the central portion of the PUF counter output. The basic PUF consists of 8 ring oscillators and 3 select lines will go into multiplexer. In the proposed PUF based STW, 8 instances of basic PUF is used to generate the 32-bit response. The input challenge comprises of 32-bit load value into 32-bit run-time counter and 24 select lines to multiplexers. The bit size of the challenge will be 56 bits. Bit selection scheme select the four bits (15^{th}, 16^{th}, 17th and 18^{th}) from the central portion from the PUF counter output in each instance. By concatenation of 4-bit response from each basic PUF instance, 32-bit response is generated from 8 instances.

The length of the custom TDR is 56 bit. 32-bit comparator circuit is designed using XOR gates to compare random number stored in OTP and response generated by PUF. A register of 32-bit length is used as OTP in the experiment. RSA block is used to encrypt both PUF response and random value stored in OTP. Thirty two 2:1 multiplexers are used to switch at the input of RSA block. An extra input pin is required as a 'select line' to choose between PUF response and OTP data. The single select line is connected to all 32 multiplexers.

The complete system is implemented in Verilog HDL and verification of the design is performed in Synopsys VCS simulator. The proposed PUF based STW is implemented in both ASIC and FPGA. ASIC implementation of comparator, RSA, FIFO (as an example) core with IEEE 1500 wrapper, JTAG with custom TDR is implemented using Synopsys Saed90nm library. A complete system including PUF is implemented on Xilinx Spartan 3E FPGA. In PUF design, manual routing is performed during place and route of the cells in each CLB (configurable logic block in FPGA). Spartan 3E FPGA CLB consists of four slices and each slice comprises of two LUTs (Look-up Tables). The NOT gate for ring oscillator is implemented using one LUT. 5 NOT gates are used to design each ring oscillator. Five slices from each CLB is required to design one ring oscillator. The ring oscillator with five NOT gates is created as macro and instantiated to design the complete PUF.

B. Performance Overhead: - The authentic user with key can unlock the wrapper. The test engineer has to unlock the wrapper only once in a test session. After unlocking, all tests can be conducted and upon reset at the end, test structures are locked. The extra timing overhead added due to security is discussed in this section. The amount of TCK cycles required to unlock the wrapper is as follows: -

- 1149.1 JTAG FSM need five clock cycles for the update and capture states [18].
- For 32-bit PUF challenge, 32 cycles are required to load the challenge into TDR and three clock cycles to feed the challenge to PUF.
- Another four clock cycles are required to generate response and to generate unlock signal from comparator circuit.

The total number of TCK clock cycles is: - 5+32+03+4 = 44 TCK cycles. 44 extra TCK cycles are required to test structures.

C. Security Analysis: - The key component in the proposed technique is PUF and performance of the overall security system depends of quality of CRP and secrecy of CRP database. The attack scenarios are discussed below: -

- Case 1: - An adversary with full knowledge of security system implemented will try for brute force attack, trying all possible combinations will take large amount of test time even on ATE. With encrypted PUF CRP's are stored in secure database and private key is unknown to OSAT centre, the proposed technique is safe. And successful brute force attack on one chip does not reveal any data or secret of other chips.
- Case 2: - In the trust model, it is assumed that PUF CRPs are stored in secure database in design house/ODM. A successful model building attacks on PUF is possible when an adversary gets an access to

complete CRP data of one chip [15]. In such a case, adversary does not have knowledge of random value stored in the OTP generated by TRNG. Even with complete knowledge on PUF CRP, adversary has to try similar to brute force attack, which is time consuming.

D. Comparison: - A comparative analysis of password/challenge-response based secure test wrapper techniques is presented in Table II. The techniques presented in [6] and [7] have static passwords which is same of all chips produced. Authentic user can share password with adversary with or without malicious intent. The PUF based scheme in [8] and the technique proposed in this paper support dynamic passwords. A major modification to IEEE 1500 wrapper is needed to implement security scheme in [7]. In the all the earlier schemes [6] [7] and [8], both foundry and OSAT centres are trusted. The earlier techniques share the passwords with OSAT centre. Adversary in OSAT centre will get an access to PUF CRP/passwords easily. Earlier techniques prevent the attacks from outsider, but not sufficient against untrusted OSAT centres. The proposed scheme in this paper trust only design house/ODM and secure against untrusted foundries and OSAT centres.

In the techniques presented in [6] and [8], RS-232 interface is used to unlock the wrapper from external ATE or test setup. Generally, IEEE 1500 wrapper is accessed through JTAG 1149.1. Clock and other control signals to control the 1500 wrapper are derived from JTAG 1149.1. JTAG 1149.1 is a primary interface for test operations and it is logical to have a security mechanism to protect IEEE 1500 wrapper for sensitive cores through JTAG 1149.1. In the techniques described in [6] and [8], attacker can get access to IEEE 1500 wrapper through JTAG 1149.1 in test mode, which compromises the security of the sensitive core even in the presence of STW. In the proposed technique, JTAG 1149.1 is used to unlock the wrapper and test operations will continue through the same channel makes the sensitive/cryptographic cores more secure.

E. Reliability: - The reliability of the proposed technique mainly depends upon reliability of the PUF. PUF CRPs vary with changing environmental conditions, ambient noise and aging. In general, most of the CRP's will have high reliability and very few (1 to 10%) do not have a bias to resolve towards either logic 0 or logic 1 [19]. PUF with high reliability will be the best fit in hardware security applications. Designing PUF circuits with highest reliability is an active research area and it is better to choose the PUF with highest reliability for security applications. The PUF used in this research has got a reliability of 89% [17]. Designing PUFs with high reliability and building applications using PUFs will go hand in hand.

V. CONCLUSIONS

In this paper, we have proposed PUF based secure test wrapper design for IEEE 1500 core test standard. The challenge-response based protection scheme presented in this paper is a countermeasure against DFT based side channel attacks on IEEE 1500 wrapped cores. The earlier challenge-response based security schemes proposed share secret keys or PUF CRPs with OSAT centre to unlock the scan chains to perform test operations. Sharing keys and confidential information with OSAT centre makes the chip vulnerable to attacks. In the proposed scheme, only design house/ODM is trusted and proposed technique avoid sharing of secret keys or any other confidential information with untrusted foundry and OSAT centers. The proposed scheme adds reasonable area overhead, due to the addition of PUF and RSA blocks.

Various countermeasures against SCA have been proposed in the past like scan chain obfuscation and partial scan address the issue at core level affect the test quality. Scalable countermeasures for SoC devices can be achieved with password based access techniques. The proposed PUF based STW technique is more secure than the earlier similar schemes and suitable for SoC environment. The success of the proposed scheme depends on the reliability of PUF CRP.

REFERENCES

[1] 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.

[2] M. Inoue, T. Yoneda, M. Hasegawa, and H. Fujiwara, "Partial scan approach for secret information protection," in *IEEE ETS*, 2009.

[3] J. Da Rolt, G. Di Natale, M.-L. Flottes, and B. Rouzeyre, "Are advanced dft structures sufficient for preventing scan-attacks?" *IEEE VTS*, 2012.

[4] A. Cui, Y. Luo, and C.-H. Chang, "Static and dynamic obfuscations of scan data against scan-based side-channel attacks," in *IEEE TIFS*, 2016.

[5] O. K¨ommerling and M. G. Kuhn, "Design principles for tamper-resistant smartcard processors." *Smartcard*, 1999.

[6] A. Das, M. Knezevic, S. Seys, and I. Verbauwhede, "Challenge-response based secure test wrapper for testing cryptographic circuits," 16th IEEE European Test Symposium 2011 (ETS), 2011.

[7] Geng-Ming Chiu, James Chien-Mo Li "A Secure Test Wrapper Design Against Internal and Boundary Scan Attacks for Embedded Cores", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Volume 20 Issue 1, January 2012 Page 126-134.

[8] A. Das et al, "PUF-based secure test wrapper design for cryptographic SoC testing", Proceedings of the Conference on Design Automation and Test in Europe (DATE)-2012.

[9] 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.

[10] IEEE Computer Society, IEEE Standard Testability Method for Embedded Core-Based Integrated Circuits, IEEE Std. 1500-2005.

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

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

[13] D. Hely, M.-L. Flottes, F. Bancel, B. Rouzeyre, N. Berard, and M. Renovell, "Scan design and secure chip." in *IOLTS*, 2004.

[14] A. Das, B. Ege, S. Ghosh, L. Batina, and I. Verbauwhede, "Security analysis of industrial test compression schemes," *IEEE TCAD*, 2013.

[15] Model Building and Security Analysis of PUF-Based Authentication, Wenjie Che, *University of New Mexico*, Ph. D thesis, http://digitalrepository.unm.edu/ece_etds/307/.

[16] Rivoir, "Lowering cost of test: parallel test or low-cost ATE?" 12th Test Symposium, 2003. ATS 2003.

[17] N. Satheesh, "A Modified RO-PUF with Improved Security Metrics on FPGA", IEEE International Symposium on Nanoelectronic and Information Systems (iNIS), 2016.

[18] Bushnell and Vishwani Agarwal, "Essentials of Electronic Testing", Springer, 2nd print edition-2002.

[19] Mudit Bhargava, Carnegie Mellon University "Reliable, Secure, Efficient Physical Unclonable Functions" http://repository.cmu.edu/dissertations/238/.