Available online at www.sciencedirect.com

ScienceDirect

Procedia Manufacturing 00 (2018) 000–000

Procedia MANUFACTURING

www.elsevier.com/locate/procedia

7th International Conference on Through-life Engineering Services

Layered Security for IEEE 1687 Using a Bimodal Physically Unclonable Function

Maulana Randa[a,b]*, Mehmet Bozdal[a], Mohammad Samie[a], Ian K. Jennions[a]

[a]*Cranfield University, College Road, Bedford, MK430AL, United Kingdom*
[b]*Indonesia Ministry of Defense, Jalan Jati No.2, Pondok Labu, Jakarta 12450, Indonesia*

Abstract

In this paper, a layered security mechanism for IEEE 1687 is proposed using a new class of physically unclonable function (PUF) called Bimodal PUF. It moves beyond the conventional single-challenge single-response PUF by introducing a second response to the PUF gained from the same single challenge. As an advantage, a double-response PUF forms two-layer security solution, one at the hardware layer by limiting the access to the embedded instrument and the second one for the data layer by securing the output data that needs to be transmitted. Experiments conducted with FPGA show that such advantages come in place at a small silicon area overhead, up to 1.4%, for a 64-bit security key. This is known to be sufficient enough to resist brute-force and machine learning attack.

Keywords: IJTAG; IEEE 1687; physically unclonable function; encryption; linear-feedback shift register

1. Introduction

According to Moore's law, the density of transistor packed into Integrated Circuits (ICs) is doubled every 18 months. Such a rapid shrinking down the size increases the complexity of both VLSI devices and their testing procedures, too. By such a trend in the fabrication of ASICs, the manufacturer would be able to integrate more IPs into a single device

* Corresponding author. Tel.: +44-784-8042-639.
E-mail address: maulana.randa@cranfield.ac.uk

as on-chip embedded instruments which makes IPs less accessible by conventional probes. This, in turn, makes the necessary tests and quality checks more complex and challenging. Hence, it is a key requirement to develop methods and tools enabling test and characterise the VLSI devices, which is impossible to be done in a short time. From an economic point of view, while market competitions require manufacturers to release their products quickly, long testing time means loss of profit and competition in the current challenging market.

The latest industrial solution to overcome the problem is the extension of the existing design for testability, the IEEE 1149.1 [1] which enables us to employ the boundary scan techniques for testing the instruments integrated with VLSI devices. This feature makes to widely known the new standard (IEEE 1687 [2]) as internal JTAG (IJTAG). It uses the same Test Access Port (TAP) controller as JTAG for interfacing Instruments-Under-Test (IUT) with the test equipment. Although IJTAG was developed from the initial JTAG standard, it did not mean to replace the IEEE 1149.1 or any other standards; but in fact, it complements the others. There are a couple of differences between IJTAG and JTAG as shown in Table 1.

Table 1. JTAG VS IJTAG Comparison

JTAG (IEEE 1149.1)	IJTAG (IEEE 1687)
Board Level	Chip Level
Fixed scan chain	Dynamic scan chain
BSDL (Boundary Scan Description Language)	ICL (Instrument Connectivity Language) & PDL (Procedural Description Language)

IJTAG differs from JTAG in the physical level of the test, scan chain, and description language. With the first one, JTAG offers solutions to test instruments on the board level while IJTAG is featured explicitly for the testing instruments on both board and chip levels. The second difference identifies if the access ports support the fixed or dynamic scan chain. JTAG endorses the fixed scan chain that enables test data to be shifted to all the instrument on the board under test even if the user only wants to see the connection between two instruments. Hence, JTAG requires more time for testing even a single instrument, which is not efficient. IJTAG supports dynamic scan chain by implementing Segment Insertion Bit (SIB) that acts as a gate in front of the instrument on the chip.

Even though there are only a few devices in complying with the IJTAG standard, there is a rising number of studies being carried out regarding the implementation and security of IJTAG. Instruments embedded the on-chip need to be secured because the device may contain confidential data, patented IP, or even critical cores that if compromised will stop the whole system. One of the primary concerns regarding IJTAG security is how to provide secure access to the instrument on-chip via the IJTAG access port. The malicious party can use this feature for various hardware hacking or other purposes such as reverse engineering the IP by analysing the outputs when given a particular input vector. It is also possible to get access to the device and activate hardware Trojan hidden inside the chip.

In this paper, we proposed a novel security mechanism to prevent access to the IJTAG network as well as prevent access to the output data of the instrument from the unauthorised parties. The properties of a physically unclonable function (PUF) to create a secret key for SIB is used. The PUF developed to have two responses from a single challenge. The first response will be used for SIB unlocking and the other one for obfuscating the output data coming out from the instrument. Linear-Feedback Shift Register (LFSR) was utilised to de-obfuscate the output data. The user needs to provide a number of cycles to generate a signal from LFSR that match with obfuscation response from PUF. Therefore, even if the attacker succeeds to unlock the SIB, they still cannot read the real output data if they are failed to provide the right cycle number to get the de-obfuscation key from LFSR. The previous efforts conducted by other researchers to avoid unauthorised access to the IJTAG network are discussed in the next section. Section III discusses a type of PUF used to achieve the proposed security mechanism. Novel IJTAG security protocol will be presented in section IV, and continued by security analysis in section V. Finally; section VI concludes the paper.

2. Related Work

Segment Insertion Bit (SIB) is one of the main features that differentiates IJTAG from JTAG. It is a module that acts as a gate in front of the instrument facilitates IJTAG network to benefits from a dynamic scan chain as can be seen in figure 1. It has two working states, closing and opening states. The first one blocks the input test data to be shifted into the instrument, but the other one allows shifting. Hence, testing just two instruments requires opening the relevant, SIBs of the chosen instruments, and the others remain closed. Therefore, the time necessary to test IJTAG compliance chip can be done faster compared to the test time of JTAG.

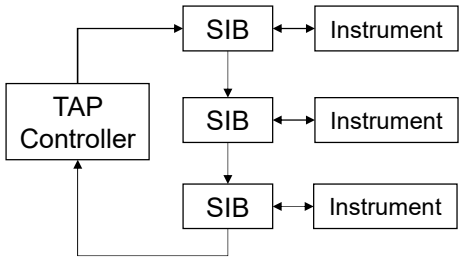

Figure 1. IJTAG network with SIB and 3 instruments

On-chip instruments may contain confidential data such as secret company-designed IP. Hence, the security of the IJTAG network that provides access to the device is essential. One way to do so is by securing the SIB. Dworwak et al. conducted initial attempts to develop a security mechanism for IJTAG in 2013 [3] by architecting locking techniques for the SIB using an n-bit signal. Whoever wants to access the instrument behind SIB needs to present the right n-bit signal before getting the SIB in open state. If an incorrect key is introduced, the system will stop working until the next reset be processed by the system administrator. This doubles the time needed for an attacker to open the SIB. Dworwak later improved the security measures by introducing honey trap LSIB [4]. Attacker's attempt to unlock a trap SIB causes locking another trap SIB; that in turn, makes attacker keep opening the trap because assuming success in guessing the secret key, but keys are wrong. In 2015, Liu et al. [5] proposed a secret key generation technique using LFSR. He showed that it would take a hundred years for the attacker to guess the secret key even if attackers employ brute force. A common disadvantage of methods presented by Dworwak [3], and Liu [5] is the use of a static secret key. Although the secret key can be kept in a secure location with encryption protection, sill attackers can use it to unlock the SIB and access instrument behind it once the key is known. To overcome this problem, Baranowski proposes a dynamic secret key generation using hash core [6]. It solves the primary drawback of the static key at the cost of additional routing congestion. This congestion depends on the location of the hash core related to the SIB. The second problem of Baranowski's method is scalability as it requires an external memory to store the generated key. For more complex systems, the routing congestion will become worse until the point it is not favourable anymore. In 2016, Sudeendra [7] proposed a method to overcome the scalability problem by using PUF for secret key generation and comparing it with the secret key generated by LFSR after a certain cycle. This technique gives a double layer of protection and solves routing congestion because it doesn't need external memory to keep the secret key. All the methods mentioned above did not consider what will happen when the attacker finally breaks the secret key and get access to the instrument. In fact, attackers may gain access to the test data output which might contain confidential data such as chip ID or useful data for reverse engineering the chip. To overcome this problem echeloned IJTAG data protection was proposed in [8]. They implement two Cipher Cores to encrypt both the Test Data Input (TDI) and Test Data Output (TDO) of the instrument. However, the presence of two Cipher can create excessive use of silicon area. Additionally, there is no need to encrypt the data input as it already stated clearly on the ICL/PDL file. The TDI encryption also means that it will take longer to test the system because the input data need to be decrypted before being shifted into the instrument.

3. Proposed Security Mechanism

3.1. Bimodal Physically Unclonable function

In 2002 Pappu et al., introduced a physical one-way function that can be used to provide signature or identity for electronic devices [9]. The initial Pappu's work gradually developed as a way to generate a secret key for authentication and encryption that is now becoming known widely as Physically Unclonable Function (PUF). PUF has many properties that make it suitable for reproducibility and uniqueness. For instance, when a PUF is given an input twice, it can generate a different response to each, depends on its reproducibility.

On the other hand, when a single challenge is given to two different PUFs, the two PUFs generate two different responses, depends on the PUF's uniqueness. This two parameters of PUF was produced as a side effect of manufacturing variance when the device was manufactured, such as variation in the transistors' length, widths, and thickness. There are a number of PUFs already proposed in the literature, which is nicely elaborated in [10].

In this work, a new class of PUF is developed so that it can generate two different responses from a single challenge. Hence, we call it bimodal PUF. A challenge is a bit string to choose which part of the PUF circuit to be compared to generate one bit of response. The bimodal PUF is based on a ring oscillator network because it can be easily implemented on any digital circuit. To overcome the problem of temperature variation, we are using comparison methodology as in [11]. To prevent machine learning attack, challenge generator based on LFSR utilised as in [12]. A de-multiplexer is added at the output of PUF to split the response in half which is needed to create the bimodality feature of the proposed PUF. The block diagram of the bimodal PUF is as in fig. 2.

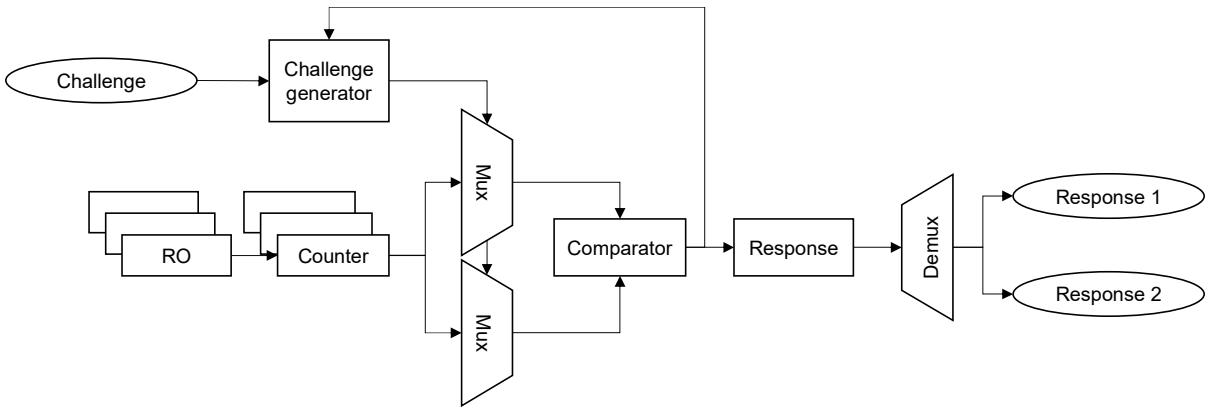

Figure 2. RO-based bimodal PUF

Table 2 presents three possible PUF networks that can be employed as candidates to develop added-security for IJTAG system. In the first option, two regular PUF networks can be utilised to generate two different responses, one to unlock SIB and the other one to obfuscate the output data. The advantage of such PUFs is making harder for an unauthorised user to unlock the SIBs because of involving two challenges. SIB is unlocked if only responses to both challenges are correct. It; however, has the disadvantage of occupying a more extensive silicon area when implemented in VLSI devices. Additionally, it suffers from a slower response for unlocking by the authorised user because requiring more IJTAG clock to shift both challenges to the PUF. The block diagram of this method is shown in Fig. 3(a).

The second option is by only using single PUF that can generate two different response, which is the bimodal PUF. The first response is used to unlock the SIB, and the second response from the same challenge is used to obfuscate the output data. To de-obfuscate the output data, LFSR is employed to generate the secret key for it. The user needs to provide a correct number of cycles for LFSR to generate a signal that matches the second PUF response. The advantage of this method is that it will only use a small area of silicon compared to the first method. The shortage of this technique is that it is easier for an unauthorised user to unlock the SIB because it won't compare the PUF response to open the

SIB as the first method. But still, even if the attacker successfully unlocks the SIB, they still need to provide a cycle for LFSR, which would be hard to guess. The block diagram for this method is shown in Fig. 3 (b).

Table 2.Comparison between PUF Options

Type of PUF	PRO	CON
2 PUF, 2 Response, 2 functionality	Harder to unlock by an attacker	Larger silicon area
1 PUF, 2 Response, 2 functionality	Smaller silicon area	Still, need further development
1 PUF, 1 Response, 2 Functionality	Smaller silicon area	Relatively Faster to unlock

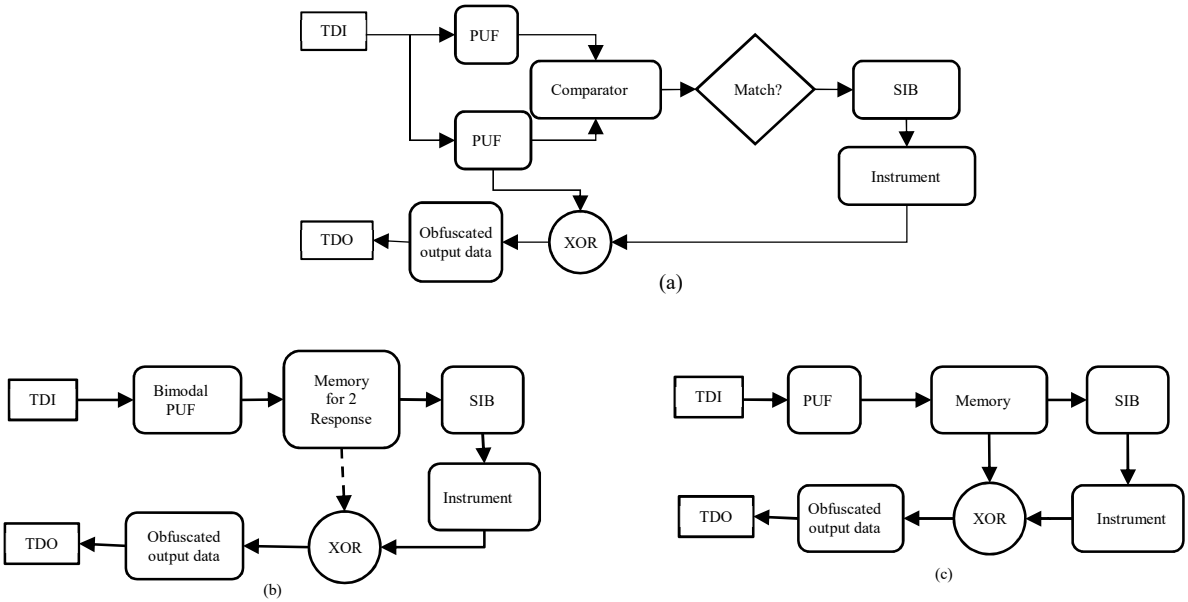

Figure 3. Multi-layer security mechanism for embedded instrument. (a) Using 2 regular PUF. (b) Using bimodal PUF. (c) Using 1 regular PUF

The third option is to use a single regular PUF that requires just producing a single response from a challenge. In this method, the single response used for both SIB unlocking and data obfuscation. To de-obfuscate the data, the user needs to provide a number of cycles for LFSR required to generate the secret key. The advantage of this method is that it will only use a small area of silicon, faster to unlock by an authorised user; but still, it provides protection as good as the second option. The block diagram of this approach is shown in Fig. 3(c).

In this paper, we are focusing on using the bimodal PUF to secure the IJTAG network, as in fig.3 (a) because it is the most balance option between security, area utilization, and speed.

3.2. Encryption VS Obfuscation

In this paper, the output data is obfuscated to make it secure from any unauthorised parties who may use it illegally for purposes such as stealing confidential data or acquiring the logic of the instrument for reverse engineering. An encryption-based data obfuscation, as suggested by this paper, provides higher security for data output in comparison with the conventional straight-forward encryption techniques. A shortage of the conventional encryption techniques is that attackers are usually able to recognise if the data is encrypted or not and then plan technique to break the encryption. Hence, straight-forward encryption technique alone is not a good option to secure the output data. Encryption-based data obfuscation, on the other hand, produces readable data but in an obfuscated form so that it is delivered as a wrong data if not de-obfuscated. The attacker won't realise data is being obfuscated and so assume it is what they expect from the instrument. Even if the attacker intends to inject signal to activate hardware Trojan hidden inside the instrument, the output of hardware Trojan will not affect the other instruments as the signal is obfuscated.

4. Security Analysis

In this section, the time needed to unlock the SIB and de-obfuscate the output data will be discussed. For the authorised user who has the right challenge to unlock the SIB and a proper number of the cycles for LFSR, unlocking process takes *N* number of clocks. *N* accounts as the total clocks needed to get the TAP controller ready, and shift the challenge to the PUF. In general, it requires five clocks to get the TAP controller ready (TRST) followed with the same amount of consecutive clocks as what was used to shift the challenge to the PUF. If the challenge generates a correct response for SIB unlocking, data is directly shifted into SIB, which needs two additional clock cycles. Thus, to unlock the SIB, it will take *N*+2 IJTAG clock. The PUF challenge can be simply increased with the trade-off of silicon overhead for cases that require higher security level from this mechanism. For the unauthorised user, the following two scenarios can be considered:

- If the attacker succeeds to guess the challenge for PUF but has no idea about obfuscation provided by the second PUF response, they will never get the correct output data from the instrument. Thus the extracted data cannot be used for reverse engineering. Even if hardware Trojan activation command is shifted to the instrument, the output will not affect another instrument as the output data was obfuscated.
- If the attacker knows that LFSR is incorporated to de-obfuscate the output data, they still need a lot of time to guess the length of LFSR and number of cycle to generate a signal that matches the second response of the PUF. The author of [5] has analytically proven that it will take years to guess the LFSR.

With this layered security protocol, not only it will prevent the instrument to be accessed by an unauthorised party, but it will also preclude the use of stolen data. It also protects another instrument from the effect of Hardware Trojan activation.

5. Experiment and Results

In this experiment, Kintex-7 XC7K325T-2FFG900C FPGA from Xilinx is used for implementation with an aim to verify the performance of the proposed techniques. In this regard, bimodal PUF and LSFR are the main blocks that should be implemented in the FPGA. The bimodal PUF that we are using here is a ring oscillator based PUF based on the architecture given in the reference [11] and [12]. The bimodal PUF comprises from 16 pair ring oscillators network needed to create 2×64-bit PUF response.

It is essential for the proposed method to store the responses of PUF in a memory (flip-flops in the actual system) mainly to hold the response until when the instrument releases the output data. The PUF responses are released from memory at the rising edge of TCK, and then further processed in conjunction with data to generate the obfuscated output. LFSR signal should be appropriately provided to get the data de-obfuscated back; otherwise, the obfuscated data is transmitted out. In the other word, a device enhanced with the proposed security remains locked and produces obscured data while the data is still readable. It is the user that should provide the right challenge to get the system unlocked and output data de-obfuscated. This requires the user to give a correct number of cycle of LFSR to generate the relevant signals. In our experiment, a 64-bit LFSR is used to match the 64-bit PUF response. If the unauthorised party cannot provide a correct number of the cycles for LFSR, the output data will be obfuscated even more.

The system is implemented in VHDL and verified using Vivado 2017.4. For comparison, the proposed design is also performed using 8, 16, 32, 64-bit PUF response to see the area impact of the design as it can be seen in table 3.

Table 3. FPGA resources for BIST with proposed IJTAG security protocol

Number of bits	Slice	LUTs	Flip-flop	% area overhead
8	4354	17416	1220	0.734
16	4360	17440	1240	1.008
32	4368	17472	1280	1.010
64	4384	17536	1360	1.414

Column 5 of table 3 show the percentage LUTs usage which compares BIST implementation using standard IJTAG with BIST implementation using the proposed method. Compared to the result in [7], it is apparent that using the same

primitives to secure the IJTAG network, the proposed design is not much affecting LUTs usage of FPGA, but have an advantage of secure output data by implementation of obfuscation. Therefore, it can also conclude that it will not much-affecting silicon area usage when implemented on ASIC.

6. Conclusion

In this paper, a multilayer security mechanism to protect access and data read of IJTAG network using bimodal PUF is proposed. The proposed technique benefits from a single challenge to generate two responses that are used to unlock the hardware, and obfuscate the output data. The user should provide an appropriate LFSR signal to get the output de-obfuscated back; otherwise, output data won't be meaningful but still readable which makes hackers assume getting access to the data they wanted. Hence utilisation of PUF to obfuscate the output data gives a high level of data protection. The analysis shows that it is faster to unlock when accessed by the authorised party, compared to previous work in this area. This means the time needed for testing will be faster while maintaining its security. Use of PUF for generating secret keys also adds to the advantages as each chip has its unique characteristic due to process variation which can be used to create a dynamic key for every single chip.

References

[1] *IEEE SA - 1149.1-2013 - IEEE Standard for Test Access Port and Boundary-Scan Architecture.* .

[2] IEEE Computer Society. Test Technology Standards Committee., Institute of Electrical and Electronics Engineers., and IEEE-SA Standards Board., *IEEE standard for access and control of instrumentation embedded within a semiconductor device - 1687*.

[3] J. Dworak, A. Crouch, J. Potter, A. Zygmontowicz, and M. Thornton, "Don't forget to lock your SIB: Hiding instruments using P16871," in *Proceedings - International Test Conference*, 2013, pp. 1–10.

[4] A. Zygmontowicz, J. Dworak, A. Crouch, and J. Potter, "Making it harder to unlock an LSIB: Honeytraps and misdirection in a P1687 network," in *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2014*, 2014, pp. 1–6.

[5] H. Liu and V. D. Agrawal, "Securing IEEE 1687-2014 Standard Instrumentation Access by LFSR Key," in *Proceedings of the Asian Test Symposium*, 2015, vol. 2016–Febru, pp. 91–96.

[6] R. Baranowski, M. A. Kochte, and H. J. Wunderlich, "Fine-grained access management in reconfigurable scan networks," *IEEE Trans. Comput. Des. Integr. Circuits Syst.*, vol. 34, no. 6, pp. 937–946, Jun. 2015.

[7] K. Sudeendra Kumar, N. Satheesh, A. Mahapatra, S. Sahoo, and K. K. Mahapatra, "Securing IEEE 1687 standard on-chip instrumentation access using PUF," in *Proceedings - 2016 IEEE International Symposium on Nanoelectronic and Information Systems, iNIS 2016*, 2017, pp. 56–61.

[8] S. Kan, J. Dworak, and J. G. Dunham, "Echeloned IJTAG data protection," in *Proceedings of the 2016 IEEE Asian Hardware Oriented Security and Trust Symposium, AsianHOST 2016*, 2017, pp. 1–6.

[9] R. Pappu, "Physical One-Way Functions," *Science (80-.).*, vol. 297, no. 5589, pp. 2026–2030, Sep. 2002.

[10] R. Maes and I. Verbauwhede, "Physically unclonable functions: A study on the state of the art and future research directions," in *Information Security and Cryptography*, no. 9783642143120, Springer, Berlin, Heidelberg, 2010, pp. 3–37.

[11] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proceedings - Design Automation Conference*, 2007, pp. 9–14.

[12] J. Ye, Y. Hu, and X. Li, "RPUF: Physical Unclonable Function with Randomized Challenge to Resist Modeling Attack."