Computers, Materials & Continua
DOI: 10.32604/cmc.2023.031617
Article

A Novel Secure Scan Design Based on Delayed Physical Unclonable Function

Weizheng Wang[1,2], Xingxing Gong[1], Xiangqi Wang[3], Gwang-jun Kim[4,*], Fayez Alqahtani[5] and Amr Tolba[6]

[1]School of Computer and Communication Engineering, Changsha University of Science and Technology, Changsha, 410114, China
[2]College of Information Science and Engineering, Hunan Women's University, Changsha, 410138, China
[3]College of Mathematics and Computational Science, Hunan First Normal University, Changsha, 410138, China
[4]Department of Computer Engineering, Chonnam National University, Gwangju, 61186, Korea
[5]Software Engineering Department, College of Computer and Information Sciences, King Saud University, Riyadh, 12372, Saudi Arabia
[6]Computer Science Department, Community College, King Saud University, Riyadh, 11437, Saudi Arabia
*Corresponding Author: Gwang-jun Kim. Email: kgi@chonnam.ac.kr
Received: 22 April 2022; Accepted: 08 June 2022

Abstract: The advanced integrated circuits have been widely used in various situations including the Internet of Things, wireless communication, etc. But its manufacturing process exists unreliability, so cryptographic chips must be rigorously tested. Due to scan testing provides high test coverage, it is applied to the testing of cryptographic integrated circuits. However, while providing good controllability and observability, it also provides attackers with a backdoor to steal keys. In the text, a novel protection scheme is put forward to resist scan-based attacks, in which we first use the responses generated by a strong physical unclonable function circuit to solidify fuse-antifuse structures in a non-linear shift register (NLSR), then determine the scan input code according to the configuration of the fuse-antifuse structures and the styles of connection between the NLSR cells and the scan cells. If the key is right, the chip can be tested normally; otherwise, the data in the scan chain cannot be propagated normally, it is also impossible for illegal users to derive the desired scan data. The proposed technique not only enhances the security of cryptographic chips, but also incurs acceptable overhead.

Keywords: Cryptographic chips; scan testing; scan-based attacks; hardware security; PUF

1 Introduction

Some emerging technologies, such as the big data [1,2], Internet of Things [3,4], wireless sensor networks [5–7], wireless communication [8,9], are developing rapidly. While they bring convenience to human life, they also face a series of security problems, for instance, information theft, malicious attack, etc. Therefore, information security has attracted more and more attention, at the same time, many researchers take care of security of the underlying hardware [10–12].

The security chip is the foundation of information security, if the security of the chip can't be guaranteed, the security of the information can't be promised. In recent years, with the increasing complexity of integrated circuits and expansion of the design scale, the testing of integrated circuits has become a huge challenge. Advanced design for testability (DFT) methods make manufacturing test and online debugging of chips easier and cheaper by embedding some logic structures such as scan chain, decompressor, test response compactor and X-masker into the circuit at the design stage, so they are particularly popular in the semiconductor industry. The scan design is the most universal DFT methodology which replaces internal flip-flops with the scan cells and makes the automatic test pattern generation (ATPG) very efficient [13,14]. At present, the vast majority of integrated circuits have introduced scan chains to improve the testability of the chip including the controllability and observability [14]. Unfortunately, while the scan design increases the testability, it also provides an attacker with a side-channel. Attackers can control and observe the internal state of the circuit-under-test (CUT) through the side-channel so that carry out illegal attacks on the circuit. Therefore, scan-based non-invasive attacks seriously affect the security of hardware [15]. The targets of scan-based attacks mainly include the following aspects:

(1) Obtain confidential information which is stored in the chip. The most common method is to crack the key of encryption chips [16,17]. A typical situation is that the attacker deliberately inserts pre-computed plaintext into chips in functional mode, then, the scan chain outputs intermediate results of encryption after one clock cycle (one round of encryption operation). As a result, the attacker inversely deduces the key from the output data.
(2) Reverse engineering the chips to extract organizational structures and functional characteristics. A timing circuit can be converted into a combinational circuit by full-scan design. An attacker can reveal the internal state of the circuit by the input-output relationships of scan design. Clearly, the scan design facilitates this attack, where the attacker only needs to rely on the most common test devices to access data in the scan chain, then uses the Boolean function learning methods to implement this attack [18].
(3) Illegal manipulation or destruction of chips. An attacker can implant illegal data into registers to manipulate and corrupt chips [19].

As seen above, it is easy to perform scan-based attacks on circuits, because such attacks do not need to pay an expensive price. Therefore, scan-based attacks are more likely to attack cryptographic chips compared with attacks based on timing analysis, power and electromagnetic radiation [20].

It is not wise for chip designers to ignore testability for security or security for testability, so maintaining a balance point between security and testability is the collective goal which every designer pursues. For the testability and security of encryption chips, researchers have proposed a number of countermeasures. Hely et al. [21] protected the test mode by inserting a test controller into CUT to resist the switching between functional mode and test mode. Although this countermeasure successfully prevents the mode-switching attack, they are vulnerable to the test-only mode attack. In order to prohibit arbitrary switching between two modes, Wang et al. [22] proposed to separate the key from the cryptographic module in test mode. This scheme is able to successfully prevent attacks with test-only mode and mode switching. Yang et al. [16] divided the CUT operation into two types, i.e., secure mode and insecure mode. In secure mode, the encryption module can't enter the insecure mode to start the test, but it can operate normally. In insecure mode, the chips can be tested but can't move the key into the register. This way makes the key more secure. Authors in [23–25] proposed several schemes to obfuscate scan data by altering the construction of the original scan design. For example, in [23] and

[24], the authors interfere with the intermediate results by changing the connection relationship in sub-chains of the scan chain. However, a skilled attacker is still able to carry out signature attacks despite not knowing the styles of connection between scan cells [26,27]. Cui et al. [25] proposed a scheme based on static and dynamic obfuscation. The test key is used to control the test control ports of multiple SFFs (scan flip flop) in this scheme. Before performing test, the test key is continuously scanned into the CUT, if the key is correct, the test proceeds normally, otherwise, the controlled units can't obtain the data of the previous SFF, but can obtain the data from the CUT. A lock and key solution based on Physical Unclonable Function (PUF) [12] was proposed in [28]. Although this modified design improves security, it induces excessive overhead. Vaghani et al. encrypted the test response with cipher keys, and decrypted the encrypted response with a specific device before using the CUT [29]. So it increases the complexity and overhead of the scan design. In addition, there are other countermeasures such as monitoring the behavior of users. When the system detects illegal activities, it will automatically initiate a protection mode. In [30], a method based on machine learning was proposed to detect the user's behavior. However, a drawback they have is that when a new attack occurs, the entire training process must be executed again.

To resist scan-based attacks, this paper proposes a novel PUF-based security architecture. In this scheme, the scan input code (SIC) is required to determine whether the test operation can be performed normally during test mode. If scan input code is incorrect, the scan chain can't transmit data normally. This is realized by inserting some logic elements around the scan cells to form a locking mechanism. Once a wrong code value appears, data obfuscation will occur during the shift. As a result, it is impossible for an attacker to infer the key. A non-linear shift register (NLSR) is added to store the scan input code, and the scan input code is determined by the configuration of the fuse-antifuse structures (referred to CF Unit) in NLSR and styles of connection between NLSR and scan chain. The main contributions of this paper are summarized below:

- A novel scan architecture is proposed to combat scan attacks. The security of the scan design is improved by embedding management circuitry into the circuit, and the proposed structure imposes no performance penalty, for example, it reduces overhead without reducing the testability and timing delay of the chip.
- We propose a PUF circuit to control fuse-antifuse structures. This method makes each chip have a unique key. In addition, bit-flip caused by external physical factors (such as environment, circuit aging, etc.) can be prevented by solidifying the response generated by PUF into the design.

The rest of this paper is organized as follows. Section 2 reviews a typical scan chain and PUF. Section 3 describes the design goals, basic ideas and architecture of the proposed protection scheme. The experimental results and analysis are presented in Section 4. Section 5 concludes this paper.

2 Review of Typical Scan Chain and PUF

2.1 Scan Chain

Since scan design provided good controllability and observability, scan chain was first used for IC test in 1973. Through the scan design, sequential circuits with low testability can be transformed into combinatorial circuits. Among the existing DFT techniques, it is recognized as the best technique [14]. A standard scan cell is formed by the modification of a D flip-flop. The SFF is composed of a 2-to-1 multiplexer and a D flip-flop, and a common scan chain is formed by connecting multiple SFFs in sequence.

2.2 PUF

Over the past 20 years, PUF has gradually changed from theoretical research to practical application, and it has great potential in the field of information security. In 2001, Srini Devadas (CSAIL, Massachusetts Institute of Technology) proposed an IC that used PUF to generate the key. PUF has been widely researched as a new security primitive for integrated circuits. It converts minor process deviations in the manufacturing process (e.g., threshold voltage Vth, drain-source current IDS and drain-source resistance RDSON) into digital information (e.g., current and delay). This bias can construct a number of challenge-response pairs (CRPS) for each chip. CRPS are highly random and unique, these properties cannot be cloned and are difficult to predict. It has come into play in many security situations such as device authentication, random number generation [31], cryptographic key generation, IP protection [32], trust computing and wireless sensor networks etc.

In 2001, Pappu et al. [33] formally introduced the concept of Physical one-way Functions and designed an optical PUF. This PUF exploits the irregularity of particle distribution within the transparent material to generate light spots, which are processed and converted into responses. Tuyls et al. proposed a coating PUF that exploits the capacitive effect [34], where a random coating is added on the chip to change the capacitance values and the measured capacitance values are used as the responses. They are difficult to apply to integrated circuits since the specificity of optics and coatings. In 2002, Gassend et al. [35] proposed a silicon PUF structure that can be applied to actual circuits, which is implemented by random differences generated during the manufacturing process, and the most important feature is that it can be directly connected to digital circuits and easily integrated. In 2004, Dodis et al. proposed the concept of obfuscated extractor [36], which provides a theoretical basis for PUF that is used for key generation. Lee et al. [37] proposed an arbiter PUF that obtains one-bit binary output by comparing the delay of two completely symmetrical paths, which determines the length of the delay by an arbiter and has been widely used in the field of integrated circuits security. In this paper, an arbiter is used to generate a unique response. In 2007, Suh et al. proposed the ring oscillator PUF [34,38], which mainly constructs a unique key for each integrated circuit by comparing the oscillation frequency difference of the ring oscillator. To prevent the phenomenon of bit-flip due to circuit aging, Liu et al. [39] proposed a special ring oscillator RO PUF on the basis of the traditional RO PUF to achieve goals of low power consumption, high reliability and anti-aging by replacing some common inverters in the design in 2017. Holcomb et al. [40] proposed the memory PUF, the most typical memory PUF is random static memory PUF, which generates two stable states of 0 or 1 by powering up SRAM, so that every SRAM will create a PUF output, the largest advantage of this PUF is that there is no need to add additional circuits and SRAM PUF can be implemented by FPGA.

In addition to the PUF mentioned above, there are many types of PUF. In 2008, Kumar et al. [32] proposed a butterfly PUF; In 2009, Helinski et al. [41] proposed a resistance-based PUF; In 2011, an improved inverter PUF is proposed based on Puntin et al. [42] by Stanzione et al. [43]. In addition, there are D flip-flop PUF [44], aging effect based PUF [45], buffer PUF [46] etc.

3 The Proposed Design Methodology for Secure Scan

3.1 Basic Idea of Proposed Secure Scan Design

In order to improve the controllability and observability of integrated circuits, DFT architecture is usually introduced to assist with testing, at the same time, the security of cryptographic chips will also be seriously compromised. Various countermeasures have been proposed by researchers, but they all have their own shortcomings. In this paper, a novel protection method is put forward to target scan-based attacks. In the proposed protection scheme, normal scan operations can be performed if the

authorized user knows the correct key. When an unauthorized user performs a scan operation, the internal state of the scan chain will be randomly modified by some combinatorial logic nodes and the incorrect key will shift dynamically in the non-linear shift register, which will eventually lead to obfuscation of scan data. If scan data is dynamically scrambled, the attack will end in failure.

The operation process of secure scan design is as follows. After power-on, the circuit is first reset, the shift enable signal SE of the circuit determines the operation mode. When SE is low-level (i.e., $SE = 0$), the encryption circuit enters the function mode. When SE becomes '1', scan input code needs to be sequentially scanned into a non-linear shift register in the next N clock cycles. If the scan input code is completely correct, the circuit will perform the normal scan operation and successfully shift the scan data into the scan chain without any external influence. If it is incorrect, the wrong scan input code will cause the circuit to operate in an abnormal test mode and NLSR will produce dynamic obfuscation. During the scan shift, some irregular values will replace values stored in the scan chain, so the attacker can't observe valid data from the output port of the scan chain, and then the encryption key can't be derived.

To make the chip more secure and prevent the circuit from aging, we use a strong PUF to generate keys for integrated circuits. The framework of PUF response solidification is shown in Fig. 1. After power-on, the PUF circuit first receives the corresponding pulse signal, and the output of the PUF will generate a set of binary data accordingly, which will reach T port of every fuse-antifuse structure. Meanwhile, when the enable signal EN of CF is 0, the initial structure of CF units are maintained, i.e., no solidification. When the enable signal EN is valid (i.e., $EN = 1$), the responses generated by the PUF are solidified into the design. The control port T fed by a bit of PUF responses determine the configuration of CF units. If T is 1, the connection between AF and C is maintained and the connection between F and C is disconnected. Otherwise, if T is 0, the connection between F and C is maintained and the connection between AF and C is disconnected.

The proposed scan design method in this paper is a novel protection architecture. In the next subsection, we will depict the proposed secure design and how the cryptographic chip performs the normal scan operation.

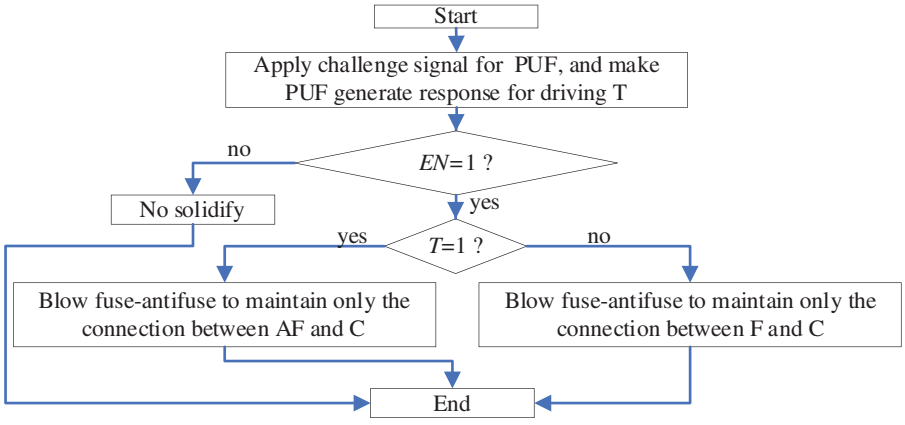

Figure 1: The framework of PUF response solidification

3.2 Architecture of Proposed Scan Method

The proposed protection design is presented in Fig. 2, which is mainly composed of the following components: 1) NLSR; 2) Scan Chain; 3) PUF Circuit; 4) Control logic for controlling the shift register and PUF circuit. In this paper, we implant only one scan chain in the circuit. As a matter of fact, multiple scan chains are also applicable to our proposed architecture. The NLSR contains x D flip-flops and y CF units, in which $x \leq y$. The size of x is determined by the length of scan key. It is worth noting that a 2-to-1 multiplexer is inserted in front of the first D flip-flop, whose two data inputs and control pins are driven by the scan input code, the output of the last CF unit in the NLSR and the output of the counter, respectively. A CF unit is inserted in front of each of the remaining D flip-flops. Its two input pins F and AF are respectively connected to the Q and $\overline{Q}$ of corresponding D flip-flops, and its design principle is described in Section 3.1. The NLSR is used to control the shift operation of the scan chain and the connection between two successive NLSR cells is reconfigurable due to the introduction of CF units.

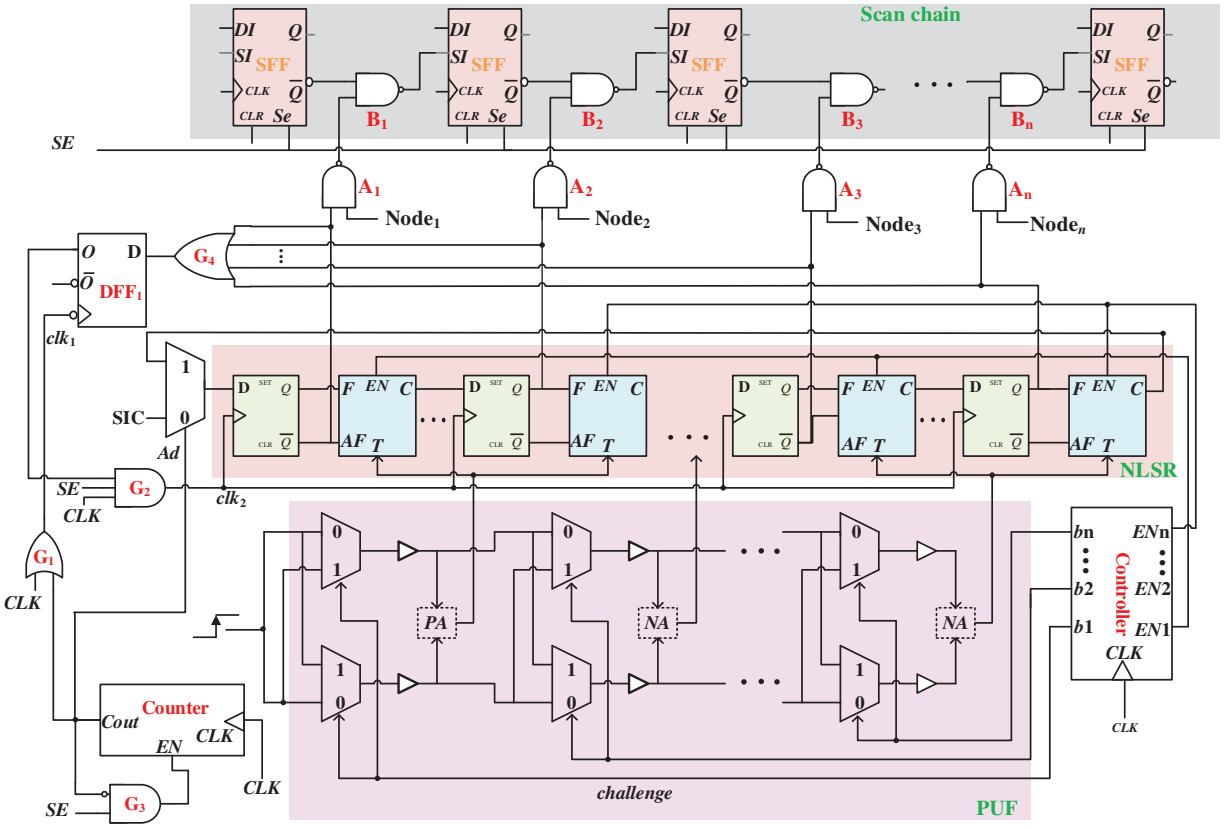

Figure 2: Proposed secure scan architecture

When solidifying, the port T that determines the configuration of each CF is driven by the responses generated by the PUF. In order to decrease the size of PUF circuit, CF units are divided into several groups and each group is driven by a same PUF unit. For example, if $y = 64$, we can divide the 64 CF units into 8 groups equally, i.e., each group has 8 CF units. The enable signal EN of the first CF unit of each group (i.e., 1^{st}, 9^{th}, 17^{th}, $25^{th}\cdots$) is controlled by the EN_1, the enable signal EN of the second CF unit of each group (i.e., 2^{nd}, 10^{th}, 18^{th}, $26^{th}\cdots$) is driven by the EN_2, and so on for the

rest. The control port T of the first 8 CF units is connected to the output port of the first PUF unit, and the control port T of the following 8 CF units is attached to output of the next PUF unit, the rest is similar. Two multiplexers, two buffers and a circuit for detecting the transmission speed of the input signal (marked as PA or NA) make up the design of a PUF unit. It is impossible that two timing paths in a PUF unit are completely symmetrical due to the difference of the manufacturing process, which will cause some delay difference. A timing path includes a multiplexer and a buffer. In the proposed scheme, an arbitration circuit is introduced to detect the delay difference of two paths and generates a random number when the pulse signal is applied. In order to avoid the unbalanced distribution of the generated PUF responses, the SR latch is introduced as an arbiter because it has good symmetry [47]. In a balanced SR latch, two NOR gates or NAND gates can be used. The following is an example of NAND latch to show their design principle, as shown in Fig. 3. First, outputs of the buffers in both paths are set to 0. Then, the signal 1 is distributed to the input of the two multiplexers. After a while, signal 1 should be sent to the output ports of both buffers in theory. Due to the differences of the manufacturing process, signal 1 will not arrive at the output of the buffers at the same time. Supposing that the transmission speed of the first path is faster, as shown in Fig. 3b, Q_1 changes from 0 to 1 at t_1, but Q_2 remains 0. When the signal passes through the NAND gate above, X will go from 1 to 0, however, $\overline{X}$ is still 1. After Q_2 changes from 0 to 1, X and $\overline{X}$ will maintain 0 and 1 respectively. Fig. 4 shows that the transmission speed of the second path is faster, i.e., Q_2 becomes 1 at t_1. When the signal passes through the NAND gate below, $\overline{X}$ changes from 1 to 0, but X remains 1. After Q_1 changes from 0 to 1, X and $\overline{X}$ will maintain 1 and 0 respectively. It can be seen that a SR-latch with NAND gates can be used as an arbiter to detect the speed of signal transmission. We also name this SR-latch as NAND-type arbiter (referred to as PA), similarly, an arbiter of SR-latch with NOR gates is called NOR-type arbiter (referred as NA) [48].

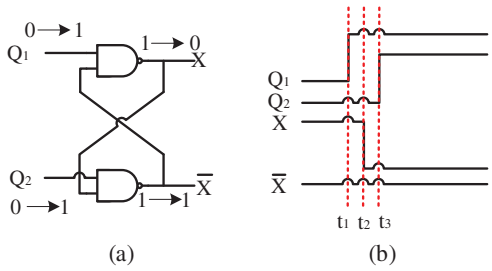

Figure 3: NAND-type arbiter and timing diagram of Q_1 running faster

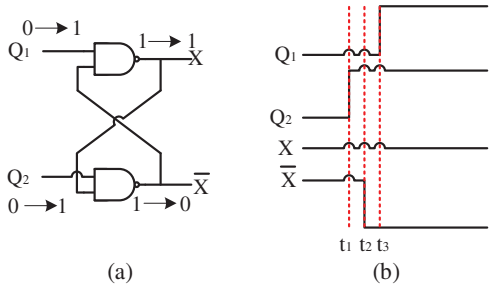

Figure 4: NAND-type arbiter and timing diagram of Q_2 running faster

The data selection ports of the multiplexers in each PUF unit are attached to the output signal b_n ($n = 1, 2, 3\cdots\cdots$) of the Controller. When the values of $\{b_n|n = 1,2,3\cdots\cdots\}$ are different, the pulse signal passes through different paths and the different responses can be generated. To solidify all CF units, the controller gives distinct values of $\{b_n|n = 1,2,3\cdots\cdots\}$ and enables only a bit of $\{EN_i|i = 1,2,3\cdots\cdots\}$ in one solidification operation. For instance, if $\{EN_1 \ldots EN_{16}\} = \{0100000000000000\}$, the enable signal EN of the second CF unit in each group is valid, then the configuration of the second CF unit in the i^{th} ($i = 1,2\cdots\cdots 8$) group is decided according to the output of the i^{th} PUF unit. We refer to this process as PUF response solidification.

In the proposed architecture, some logic gates will be introduced to modify the structure of the scan chain in order to lock scan design, i.e., some NAND gates (marked as A_i and B_i) will be inserted between SFFs. The output Q (or complementary $\overline{Q}$) of each NLSR cell is connected to an input of NAND gate A_i and the other input comes from a combinatorial logic node (i.e., a randomly selected node in the CUT). The output of A_i is connected to an input pin of B_i ($i = 1, 2, 3\ldots$) and another input of B_i is connected to the output $\overline{Q}$ of scan flip-flop. Assuming that A_i is driven by output $\overline{Q}$ of the NLSR, the following cases will occur: (1) If $\overline{Q} = 0$, the output of A_i is 1 and the output of B_n depends on the output of the previous SFF; (2) If $\overline{Q} = 1$, then the output of A_i is opposite to the value of $Node_i$ and the output of B_i can be represented by $B_i = Node_i + Q$. When $Node_i = 1$, the low-level output of A_i will cause the succeeding SFF to obtain a steady value 1. On the contrary, when $Node_i = 0$, the high-level output of A_i will reverse the input of the succeeding SFF to the output of the previous SFF. Thus, the logical obfuscation of the scan chain is achieved by this design, which makes it difficult for illegal users to analyze the key due to the uncertainty of the parameters such as $Node_i$. In order for the scan chain to perform a normal scan operation, it can be easily seen that if one input of A_i is driven by the output $\overline{Q}$ of the D flip-flops in NLSR, then the internal state of the NLSR units must be 1. Conversely, if Q is connected to A_i, the internal state of the NLSR cells must be 0. Now we need to define expected values that can perform the scan operation normally as the key to control SFFs. When the control signal $Ad = 0$, the scan input code is loaded into the NLSR serially so that the scan key is generated.

The output of D flip-flops in NLSR, in addition to being connected to An, drives a multi-input OR gate G_4. When the SIC is completely shifted to NLSR, the output of G_4 is latched to a D flip-flop DFF_1, whose clock port clk_1 is driven by the output of G_1. One input of G_1 is connected to the system clock CLK, and the other input is driven by the Carry output $Cout$ of a counter. The output O of DFF_1 together with the system clock CLK and shift enable signal SE is fed to the clock signal clk_2 through an AND gate G_2.

Before the chip is put in service, CF units are solidified by one-time programming. When the circuit is power-on or reset, the module-N counter, DFF_1 and NLSR are initialized to 0. For Counter, $Cout = 0$. The counter has an enable input signal EN, which is connected to the output of G_3. Two input pins of G_3 are driven by SE and $\overline{Cout}$. In test mode ($SE = 1$), since the output of G_3 is high-level, the enable signal EN becomes 1, at the same time, the Counter will be enabled and start counting from zero. During this period, $Ad = 0$ and the SIC is shifted into NLSR. When the correct SIC is fully entered, G_4 will generate a low-level and the output port O of DFF_1 will also become 0. Once the SIC is fully loaded, the Counter will reach the maximum value. Hence, $Cout$ will become high-level and G_3 is low-level. At this time, $EN = 0$ and the Counter will be disabled. In addition, DFF_1 is locked because the clock clk_1 is always equal to 1. At the same time, clk_2 (the output signal of G_2) remains 0, so the D flip-flops in NLSR will also be locked and the correct scan key is stored in NLSR. In this case, the output of the NAND gate A_i ($i = 1, 2, 3\cdots n$) is 1, thus the scan chain can also perform the normal scan operation.

When SIC is not completely correct, the scan key that controls the SFFs will also be wrong. When the signal *Cout* of Counter reaches the maximum value, the clock signal clk_1 of DFF_1 is disabled and the output 1 of G_4 is latched to DFF_1, that is, $O = 1$. From now on, clk_2 following *CLK* enables each D flip-flop in NLSR. In test mode, the wrong scan key will shift dynamically in NLSR. After the scan key passes through the NAND gates $\{A_i\}$ and $\{B_i\}$, the locking mechanism between scan cells will create obfuscation. So the attackers can only get wrong scan outputs and they will be misled.

As previously reported, the scan input code is related to the following two factors: (1) the configuration of the CF units; (2) the styles of connection between NLSR and scan chain. An example of deriving scan input code is given below. Let's assume that $n = 8$, the output $\overline{Q}$ of each D flip-flop in NLSR is connected to succeeding NLSR unit after solidifying the CF units and the expected scan key is 10011011 which is derived according to the styles of connection between NLSR and scan chain. The scan input code $X_1, X_2, X_3, X_4, X_5, X_6, X_7, X_8$ are shifted into NLSR in eight clock cycles. It can be seen from Tab. 1 that the state of NLSR is $\overline{X_1}, X_2, \overline{X_3}, X_4, \overline{X_5}, X_6, \overline{X_7}, X_8$ after eight cycles. According to expected scan key and the state of the NLSR after eight clock cycles, scan input vectors can be inferred. i.e., $X_1, X_2, X_3, X_4, X_5, X_6, X_7, X_8 = 00110001$.

Table 1: State of example NLSR

0^{th}	0	0	0	0	0	0	0	0
1^{st}	X_1	1	1	1	1	1	1	1
2^{nd}	X_2	$\overline{X_1}$	0	0	0	0	0	0
3^{rd}	X_3	$\overline{X_2}$	X_1	1	1	1	1	1
4^{th}	X_4	$\overline{X_3}$	X_2	$\overline{X_1}$	0	0	0	0
5^{th}	X_5	$\overline{X_4}$	X_3	$\overline{X_2}$	X_1	1	1	1
6^{th}	X_6	$\overline{X_5}$	X_4	$\overline{X_3}$	X_2	$\overline{X_1}$	0	0
7^{th}	X_7	$\overline{X_6}$	X_5	$\overline{X_4}$	X_3	$\overline{X_2}$	X_1	1
8^{th}	X_8	$\overline{X_7}$	X_6	$\overline{X_5}$	X_4	$\overline{X_3}$	X_2	$\overline{X_1}$
Expected	1	1	0	1	1	0	0	1

The designer should add an output interface to the last CF unit in the NLSR before the chip is tested. When the chip is powered on for the first time, first of all, the designer enters the scan input code. Then the scanned-out data will be observed in the added output port after a few clock cycles. Finally, the designer deduces the configuration information of the NLSR based on the scanned-out data and fuses the added output interface.

3.3 Timing Analysis of Proposed Secure Scan Scheme

In order to describe the operational flow of the scan design, Figs. 5 and 6 show the timing diagrams for entering the incorrect key and the correct key respectively.

When the system is reset, the main control signals in the circuit are initialized to 0. In order to enter the functional mode, both *RST* and *SE* are set to a low-level. In the functional mode, low-level *SE* causes *EN* to become low voltage, so the Counter is disabled, and clk_2 also becomes low voltage because of *SE*. The state of NLSR remains all 0. Therefore, the additional circuit is inactive in functional mode.

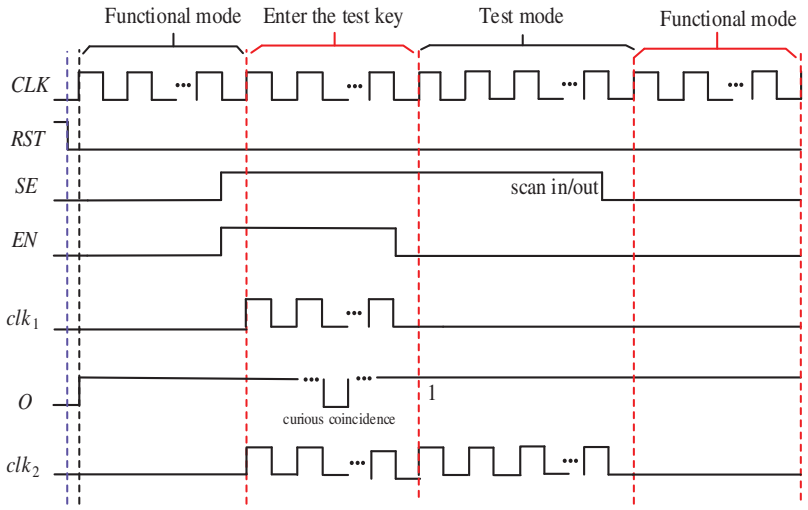

Figure 5: Timing diagram with incorrect scan input code

In order to enter the test mode, the shift enable signal *SE* is set to 1. At this time, the Counter is enabled and starts counting. At the same time, clk_2 is also activated, and *N*-bits scan input code is entered into the shift register bit by bit. When scan input code is completely entered, the output signal *Cout* (i.e., *Cout* = 1) of the Counter makes its disabled. As described in Section 3.2, if incorrect scan input code is loaded into NLSR during test mode, the output of G_4 will become high-level, so the output of DFF_1 is 1. The clock signal clk_2 is consistent with the system clock signal *CLK*, wrong scan input code will shift dynamically in NLSR. The timing diagram for entering the incorrect scan key is shown in Fig. 5.

If the correct scan input code is applied, the clock signal clk_2 will be disabled and the correct scan key will be stored in NLSR. This is because the output of G_4 becomes low-level. In this case, the system can perform scan operation normally. The timing diagram for entering the correct scan key is shown in Fig. 6.

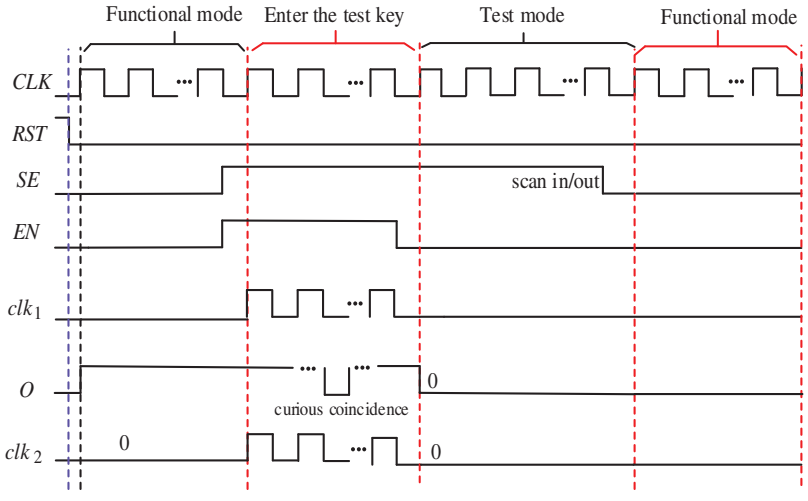

Figure 6: Timing diagram with correct scan input code

4 Experimental Results and Analysis

The proposed scheme has been implemented and verified on several benchmark circuits including Wb-Conmax, Aes-Ite, aeMB, Vga-Lcd, Aes-Pip [49]. We evaluate the proposed scheme in terms of testability, security, and performance overhead of the design.

4.1 Testability Analysis

We have added protection design to the original circuit, but added part will not affect the testability of the original circuit. When user enters the correct scan input key, the circuit can execute the normal scan operation. This solution is generally applicable to various test techniques including stuck-at fault testing, LoC-based delay fault testing and so on. Furthermore, the test process of these technologies does not change in nature. Hence, there is no impact on the testability of the original module.

For faults that appear in protection circuitry, in general, it is not necessary to perform an additional test operation. For example, if the output of G_4 is stuck at 1, the scanned-out response of CUT will be incorrect even if the scan input code is right. So this fault can be discovered by conventional test and the chip will be considered faulty. If high fault coverage must be ensured in special application, we can introduce build-in self-test (BIST) to test the protection circuitry.

4.2 Security Analysis

The security of the proposed architecture is discussed in detail against several known attacks.

(1) Brute Force Attack: It is almost impossible for illegal users to know internal structures of the protection circuitry via brute force attack. The reasons are mainly as follows: 1) The scan input code of the circuit is determined according to the configuration of CF units and styles of connection between the NLSR and the scan chain; 2) The configuration of the CF units is determined by the generated responses of PUF; 3) The responses are transformed by manufacturing process.

Hence, cracking the scan input code is difficult for illegal users by brute force attack without knowing internal structures of the protection circuitry. The probability of accurately guessing the L-bit scan input code is $(1/2)^L$. For $L = 64$ or 128, it is inferred that the probability of scan input patterns is only $5.4 * 10^{-20}$ or $2.9 * 10^{-39}$. In this case, it is impossible to obtain the key by brute force attack. In actual situations, the value of L is related to two factors: (a) hardware overhead; (b) attack probability.

(2) Differential Attack: In [50], the adversary first performs the system for one or more clock cycles in functional mode after resetting, then enters test mode to obtain intermediate values. Although the attacker can load the prepared plaintext through the primary input, the output of the scan chain will be obfuscated without the correct scan input key. Therefore, this secure scan design can effectively resist differential attack.

(3) Test-Mode-Only Differential Attack: In many security designs, scan chains are reset when switching between test mode and functional mode. Therefore, this can resist normal differential attack [50]. However, authors in [51] proposed a new test-mode-only differential attack, this attack achieves key scan cell identification by shifting under all-zero or special test patterns. However, in the proposed architecture, these data are not easily loaded into the scan chain since the protection of the logical obfuscation. Also, the wrong key is dynamically shifted in NLSR during test mode. This leaves the obfuscated bits in an uncertain state during every clock cycle. Therefore, the proposed design can overcome the test-mode-only differential attack.

(4) Resetting Attack: When CUT is reset, the attacker knows that the values of all flip-flops are initialized to 0 before scanning out, so the attacker analyzes the correctness of test key by the scanned-out values. However, in the proposed secure design, since the NLSR is dynamically shifted, the scanned-out data is elusive. Therefore, inferring scan input code bit by bit from the scanned-out data is not possible. This solution can effectively prevent resetting attack.

4.3 Overhead Analysis

To analyze the overhead, scan designs of the five circuits are synthesized using the Synopsys Design Compiler and Synopsys DFT Compiler respectively. Then, the proposed secure countermeasure is added to the netlist of the scan design and synthesized with DC. In the experiment, the length of test key (N) is set to 64 and 128. Tab. 2 depicts the synthesis results of the standard scan design and the proposed secure scan design, #SFF represents the number of sequential cells, and the columns marked "Scan" and "Secure" show area and power of IP cores with insertion of conventional scan chain and secure scan design respectively.

Table 2: Synthesis results of scan design and proposed secure design

Circuit name	#SFF	Area			Power		
		Scan	Secure		Scan	Secure	
			$N = 64$	$N = 128$		$N = 64$	$N = 128$
Wb-Conmax	818	331839	334600	336262	130345	131010	131455
aeMB	3458	263145	265906	267568	124815	125480	125925
Vga-Lcd	17071	922617	925378	927040	198165	198830	199275
Aes-Ite	1048	299267	302028	303690	292655	293320	293765
Aes-Pip	10776	1977833	1980594	1982256	112225	112890	113335

For different N, the percentage of area overhead and power overhead of the proposed secure design are given in Tab. 3. The third and fifth columns show area and power of the protection circuit respectively. The fourth and sixth columns show the percentage of area overhead and power overhead, respectively. From the table, we can see that the secure design with 128-bit key is slightly larger than the design with 64-bit key in area overhead for the same circuit. Fig. 7 intuitively shows the percentage of area overhead and power overhead of pipelined AES for different N. It can be seen that the area overhead and power overhead also increase as the number of bits of scan input password increases from the figure. For different IP cores, the area overhead percentage has a certain relevance with the circuit scale. In general, the area overhead percentage decreases with the increase of the circuit scale.

Table 3: Percentage of area overhead and power overhead of proposed secure design

Circuit name	Proposed scheme	Area overhead	ΔA(%)	Power overhead	ΔP(%)
Wb-conmax	$N = 64$	2761	0.83	665	0.51
	$N = 128$	4423	1.32	1110	0.84
aeMB	$N = 64$	2761	1.03	665	0.53

(Continued)

Table 3: Continued

Circuit name	Proposed scheme	Area overhead	ΔA(%)	Power overhead	ΔP(%)
	$N = 128$	4423	1.65	1110	0.88
Vga-Lcd	$N = 64$	2761	0.29	665	0.33
	$N = 128$	4423	0.48	1110	0.56
Aes-Ite	$N = 64$	2761	0.91	665	0.23
	$N = 128$	4423	1.46	1110	0.38
Aes-Pip	$N = 64$	2761	0.14	665	0.59
	$N = 128$	4423	0.22	1110	0.98

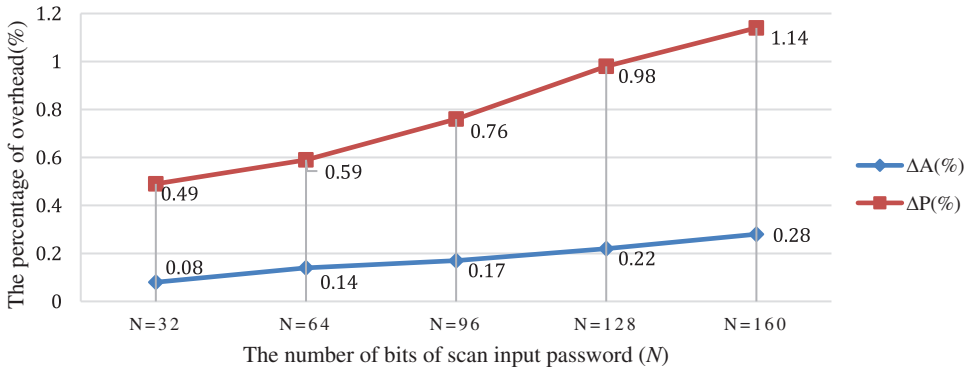

Figure 7: The percentage of area overhead and power overhead of pipelined AES for different N

The area overhead and performance of the proposed secure design are compared with existing techniques in Tab. 4, including MKR [16], Mode reset [21], DOSD-64 [25], DOSD-128 [25], Scan Chain Encryption [52], DOS-10% [53], DOS-30% [53], SLAKE-8-8 [54], FTSL-64 [28] and FTSL-128 [28]. Compared with other countermeasures, the proposed secure design has a low area overhead. Furthermore, the proposed design improves security without affecting performance and testing of IP core in terms of secure performance. MKR [16] uses a secure test controller to manage scan test, which makes brute force attack infeasible, requires no test preparation time and has high pattern application flexibility, however, it can't test key registers. Mode reset [21] has not only similar shortcomings to MKR [16] but also incurs high overhead and is vulnerable to test-mode-only attack. The DOSD [25] design is similar to the proposed design in many performances, but it incurs path delay overhead. Scan Chain Encryption [52] exists many shortcomings, such as high overhead, low pattern application flexibility and multi-cycle for pattern decryption. The area overhead of DOS [53] is relatively large and it is also vulnerable to Memory attack. SLAKE-8-8 [54] requires more cycles test preparation time. Much performance of FTSL [28] design is similar to our proposed design, but it has a larger area overhead.

As can be seen from Tab. 4, proposed secure design has the following advantages: high resistance against scan-based attacks, low area overhead, high pattern application flexibility and no impact on the testability of chips.

Table 4: Comparison of different secure scan designs

Design	Area overhead (%)	Security		Pattern application flexibility	Impact on testability	Impact on test time
		Vulnerability	Probability of brute attack			
Proposed (64-bit test key)	0.14	None	2^{-64}	Pattern application can be arbitrary	Nil	64 clock cycles before testing
Proposed (128-bit test key)	0.22	None	2^{-128}			128 clock cycles before testing
MKR [16]	0.15	None	Not applicable	Pattern application can be arbitrary	Limited by inability to test secret-key registers	NA
Mode reset [21]	≈10	Test-mode-only attack	Not applicable	Pattern application can be arbitrary	Nil	NA
DOSD-64 [25]	0.25	None	2^{-64}	Pattern application can be arbitrary	Nil	64 clock cycles before testing
DOSD-128 [25]	0.47		2^{-128}			128 clock cycles before testing
Scan Chain Encryption [52]	2.92	Memory attack	2^{-K} (K is the key length of scan chain)	Yes if $K < \lambda$; No if $K > \lambda$	Nil	Multiple clocks for pattern decryption
DOS-10% [53]	0.85	Memory attack	$2^{-k\lambda}$(k and λ are the number and the length of scan chain)	Pattern application can be arbitrary	Nil	NA
DOS-30% [53]	2.01					NA

(Continued)

Table 4: Continued

Design	Area overhead (%)	Security		Pattern application flexibility	Impact on testability	Impact on test time
		Vulnerability	Probability of brute attack			
SLAKE-8-8 [54]	0.19	None	$2^{-64}(c_{Ps}^{Cs})^{8\,(*)}$	Pattern application can be arbitrary	Nil	More clock cycles before testing
FTSL-64 [28]	3.09	None	2^{-64}	Pattern application can be arbitrary	Nil	64 clock cycles before testing
FTSL-128 [28]	3.80		2^{-128}			128 clock cycles before testing

Notes: (∗) Ps means the total skew between the clock and data and Cs means the correct skew to capture the desired value.

5 Conclusion

In this paper, a novel secure scan design is proposed to protect IP cores from scan-based attacks. In this technique, the data transfer of some selected SFFs is controlled by scan input code loaded into the NLSR, which is associated with the configuration of CF units and the styles of connection between the shift register and the scan chain. The configuration of CF units is determined by PUF responses. Finally, the proposed secure design is verified on Wb-Conmax, Aes-Ite, aeMB, Vga-Lcd, Aes-Pip and this scheme has good security, testability, and acceptable hardware overhead compared with other countermeasures.

We assume that the tester is not an attacker in this paper. In addition, this means that the tester needs to be taken into confidential. In the future, the secure design should be developed without the risk of revealing test password.

Funding Statement: This work was funded by the Researchers Supporting Project No. (RSP2022R509) King Saud University, Riyadh, Saudi Arabia. In addition, it was supported in part by the Natural Science Foundation of Hunan Province under Grant no. 2020JJ5604, 2022JJ2029 and 2020JJ4622, and by the National Natural Science Foundation of China under Grant no. 62172058.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] J. Wang, Y. Yang, T. Wang, R. Sherratt and J. Zhang, "Big data service architecture: A survey," *Journal of Internet Technology*, vol. 21, no. 2, pp. 393–405, 2020.

[2] J. Wang, Y. Yang, J. Zhang, X. Yu, O. Alfarraj *et al.,* "A data-aware remote procedure call method for big data systems," *Computer Systems Science and Engineering*, vol. 35, no. 6, pp. 523–532, 2020.
[3] B. Yin and X. Wei, "Communication-Efficient data aggregation tree construction for complex queries in IoT applications," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3352–3363, 2019.
[4] W. Li, Z. Chen, X. Gao, W. Liu and J. Wang, "Multimodel framework for indoor localization under mobile edge computing environment," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4844–4853, 2019.
[5] J. Wang, W. Chen, L. Wang, R. S. Sherratt, O. Alfarraj *et al.,* "Data secure storage mechanism of sensor networks based on blockchain," *Computers, Materials & Continua*, vol. 65, no. 3, pp. 2365–2384, 2020.
[6] J. Wang, Y. Gao, C. Zhou, R. S. Sherratt and L. Wang, "Optimal coverage multi-path scheduling scheme with multiple mobile sinks for wsns," *Computers, Materials & Continua*, vol. 62, no. 2, pp. 695–711, 2020.
[7] J. Wang, Y. Gao, W. Liu, W. Wu and S. J. Lim, "An asynchronous clustering and mobile data gathering schema based on timer mechanism in wireless sensor networks," *Computers, Materials & Continua*, vol. 58, no. 3, pp. 711–725, 2019.
[8] F. Yu, L. Liu, L. Xiao, K. Li and S. Cai, "A robust and fixed-time zeroing neural dynamics for computing time-variant nonlinear equation using a novel nonlinear activation function," *Neurocomputing*, vol. 350, no. 11, pp. 108–116, 2019.
[9] F. Yu, L. Gao, L. Liu, S. Qian, S. Cai *et al.,* "A 1V, 0.53 ns, 59 μW current comparator using standard 0.18 μm CMOS technology," *Wireless Personal Communications*, vol. 111, no. 2, pp. 843–851, 2020.
[10] J. Zhang, C. Shen, H. Su, M. T. Arafin and G. Qu, "Voltage over-scaling-based lightweight authentication for IoT security," *IEEE Transactions on Computers*, vol. 71, no. 2, pp. 323–336, 2022.
[11] W. Z. Wang, Y. Chen, S. Cai and Y. Peng, "Preventing scan-based side-channel attacks by scan obfuscating with a configurable shift register," *Security and Communication Networks*, vol. 2021, no. 5222670, pp. 1–9, 2021.
[12] J. Zhang and G. Qu, "Physical unclonable function-based key sharing via machine learning for IoT security," *IEEE Transactions on Industrial Electronics*, vol. 67, no. 8, pp. 7025–7033, 2020.
[13] W. Wang, J. Wang, Z. Wang and L. Xiang, "Access-in-turn test architecture for low-power test application," *International Journal of Electronics*, vol. 104, no. 3, pp. 433–441, 2017.
[14] L. T. Wang, C. W. Wu and X. Wen, *VLSI Test Principles and Architectures Design for Testability*, Amsterdam, Netherlands: Morgan Kaufmann, pp. 557–618, 2006.
[15] E. Valea, M. D. Silva, G. D. Natale, M. L. Flottes and B. Rouzeyre, "A survey on security threats and countermeasures in IEEE test standards," *IEEE Design and Test*, vol. 36, no. 3, pp. 95–116, 2019.
[16] B. Yang, K. Wu and R. Karri, "Secure scan: A design-for-test architecture for crypto chips," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 25, no. 10, pp. 2287–2293, 2006.
[17] B. Yang, K. Wu and R. Karri, "Scan based side channel attack on dedicated hardware implementations of data encryption standard," in *2004 Int. Conf. on Test*, Charlotte, NC, USA, pp. 339–344, 2004.
[18] L. Azriel, G. Ran and A. Mendelson, *Exploiting the Scan Side Channel for Reverse Engineering of a VLSI Device*, 2016, US10025896B2
[19] D. Hely, M. L. Flottes, F. Bancel, B. Rouzeyre, N. Berard *et al.,* "Scan design and secure chip [secure IC testing]," in *Proc.. 10th IEEE Int. On-Line Testing Symp.*, Funchal, Portugal, pp. 219–224, 2004.
[20] F. Koeune and F. X. Standaert, "A tutorial on physical security and side channel attacks," in *Foundations of Security Analysis and Design III*, Germany: Springer Berlin Heidelberg, pp. 78–108, 2005.
[21] D. Hely, F. Bancel, M. L. Flottes and B. Rouzeyre, "Securing scan control in crypto chips," *Journal of Electronic Testing Theory & Applications*, vol. 23, no. 5, pp. 457–464, 2007.
[22] W. Z. Wang, J. C. Wang, W. Wang, P. Liu and S. Cai, "A secure DFT architecture protecting crypto chips against scan-based attacks," *IEEE Access*, vol. 7, pp. 22206–22213, 2019.
[23] J. Lee, M. Tehranipoor, C. Patel and J. Plusquellic, "Securing designs against scan-based side-channel attacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no. 4, pp. 325–336, 2007.

[24] Y. Atobe, Y. Shi, M. Yanagisawa and N. Togawa, "Secure scan design with dynamically configurable connection," in *2013 IEEE 19th Pacific Rim Int. Symp. on Dependable Computing*, Vancouver, BC, Canada, pp. 256–262, 2013.
[25] A. Cui, Y. Luo and C. H. Chang, "Static and dynamic obfuscations of scan data against scan-based side-channel attacks," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 2, pp. 363–376, 2017.
[26] H. Kodera, M. Yanagisawa and N. Togawa, "Scan-based attack against DES cryptosystems using scan signatures," in *2012 IEEE Asia Pacific Conf. on Circuits and Systems*, Kaohsiung, Taiwan, pp. 599–602, 2012.
[27] R. Nara, N. Togawa, M. Yanagisawa and T. Ohtsuki, "A scan-based attack based on discriminators for AES cryptosystems," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E92-A, no. 12, pp. 3229–3237, 2009.
[28] A. Cui, C. H. Chang, W. Zhou and Y. Zheng, "A new PUF based lock and key solution for secure in-field testing of cryptographic chips," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 2, pp. 1095–1105, 2021.
[29] D. Vaghani, S. Ahlawat, J. T. Tudu, M. Fujita and V. Singh, "On securing scan design through test vector encryption," in *IEEE Int. Symp. on Circuits and Systems*, Florence, Italy, pp. 466–470, 2018.
[30] X. Ren, F. P. Torres, R. D. Blanton and V. G. Tavares, "IC protection against JTAG-based attacks," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 38, no. 1, pp. 149–162, 2019.
[31] V. V. D. Leest, E. V. D. Sluis, G. J. Schrijen, P. Tuyls and H. Handschuh, "Efficient implementation of true random number generator based on sram pufs," in *Cryptography and Security: From Theory to Applications*, vol. 6805. Germany: Springer Berlin Heidelberg, pp. 300–318, 2012.
[32] S. S. Kumar, J. Guajardo, R. Maes, G. Schrijen and P. Tuyls, "Extended abstract: The butterfly PUF protecting IP on every FPGA," in *2008 IEEE Int. Workshop on Hardware-Oriented Security and Trust*, Anaheim, CA, USA, pp. 67–70, 2008.
[33] R. Pappu, B. Recht, J. Taylor and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002.
[34] P. Tuyls, G. J. Schrijen, B. Skoric, J. V. Geloven, N. Verhaegh *et al.,* "Read-proof hardware from protective coatings," in *Int. Workshop on Cryptographic Hardware and Embedded Systems*, Berlin, Heidelberg, 4249, pp. 369–383, 2006.
[35] B. Gassend, D. E. Clarke, M. V. Dijk and S. Devadas, "Silicon physical random functions," in *Proc. of CCS'10*, Washington, DC, USA, pp. 148–160, 2002.
[36] Y. Dodis, L. Reyzin and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Int. Conf. on the Theory and Applications of Cryptographic Techniques*, Berlin, Heidelberg, pp. 523–540, 2004.
[37] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. V. Dijk *et al.,* "A technique to build a secret key in integrated circuits for identification and authentication applications," in *2004 Symp. on VLSI Circuits. Digest of Technical Papers*, Honolulu, HI, USA, pp. 176–179, 2004.
[38] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *2007 44th ACM/IEEE Design Automation Conf.*, San Diego, CA, USA, pp. 9–14, 2007.
[39] C. Q. Liu, Y. Cao and C. H. Chang, "ACRO-PUF: A low-power, reliable and aging-resilient current starved inverter-based ring oscillator physical unclonable function," *IEEE Transactions on Circuits and Systems I*, vol. 64, no. 12, pp. 3138–3149, 2017.
[40] D. E. Holcomb, W. P. Burleson and K. Fu, "Power-Up SRAM state as an identifying fingerprint and source of true random numbers," *IEEE Transactions on Computers*, vol. 58, no. 9, pp. 1198–1210, 2009.
[41] R. Helinski, D. Acharyya and J. Plusquellic, "A physical unclonable function defined using power distribution system equivalent resistance variations," in *2009 46th ACM/IEEE Design Automation Conf.*, San Francisco, CA, USA, pp. 676–681, 2009.

[42] D. Puntin, S. Stanzione and G. Iannaccone, "CMOS unclonable system for secure authentication based on device variability," in *ESSCIRC, 2008 34th European Solid-State Circuits Conf.*, Edinburgh, UK, pp. 130–133, 2008.
[43] S. Stanzione, D. Puntin and G. Iannaccone, "CMOS silicon physical unclonable functions based on intrinsic process variability," *IEEE Journal of Solid-State Circuits*, vol. 46, no. 6, pp. 1456–1463, 2011.
[44] V. V. D. Leest, G. J. Schrijen, H. Handschuh and P. Tuyls, "Hardware intrinsic security from D flip-flops," in *Proc. of CCS'10*, Chicago, Illinois, USA, pp. 53–62, 2010.
[45] S. Meguerdichian and M. Potkonjak, "Device aging-based physically unclonable functions," in *2011 48th ACM/EDAC/IEEE Design Automation Conf.*, San Diego, CA, USA, pp. 288–289, 2011.
[46] E. Ozturk, G. Hammouri and B. Sunar, "Physical unclonable function with tristate buffers," in *2008 IEEE Int. Symp. on Circuits and Systems*, Seattle, WA, USA, pp. 3194–3197, 2008.
[47] M. Cortes, G. Araujo and J. Capovilla, "Improving the statistical variability of delay-based physical unclonable functions," in *2015 28th Symp. on Integrated Circuits and Systems Design*, Salvador, Brazil, pp. 1–7, 2015.
[48] W. Wang, A. Cui, G. Qu and H. Li, "A low-overhead PUF based on parallel scan design," in *2018 23rd Asia and South Pacific Design Automation Conf.*, Jeju, Korea, pp. 715–720, 2018.
[49] Open IP cores, https://opencores.org.
[50] J. D. Rolt, G. D. Natale, M. L. Flottes and B. Rouzeyre, "A novel differential scan attack on advanced DFT structures," *ACM Transactions on Design Automation of Electronic Systems*, vol. 18, no. 4, pp. 1–22, 2013.
[51] S. S. Ali, O. Sinanoglu, S. M. Saeed and R. Karri, "New scan-based attack using only the test mode," in *2013 IFIP/IEEE 21st Int. Conf. on Very Large Scale Integration*, Istanbul, Turkey, pp. 234–239, 2013.
[52] M. Da Silva, M. l. Flottes, G. Di Natale, B. Rouzeyre, P. Prinetto *et al.,* "Scan chain encryption for the test, diagnosis and debug of secure circuits," in *2017 22nd IEEE European Test Symp.*, Limassol, Cyprus, pp. 1–6, 2017.
[53] X. Wang, D. Zhang, M. He, D. Su and M. Tehranipoor, "Secure scan and test using obfuscation throughout supply chain," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 37, no. 9, pp. 1867–1880, 2018.
[54] H. Woo, S. Jang and S. Kang, "A secure scan architecture protecting scan test and scan dump using skew-based lock and key," *IEEE Access*, vol. 9, pp. 102161–102176, 2021.