IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 11, 2019, accepted June 19, 2019, date of publication June 26, 2019, date of current version July 15, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2925237

Scan Chain Based Attacks and Countermeasures: A Survey

XIAOWEI LI[1,2], (Senior Member, IEEE), WENJIE LI[1,2], JING YE[1,2], HUAWEI LI[1,2,3], (Senior Member, IEEE), AND YU HU[1,2], (Member, IEEE)

[1]State Key Laboratory of Computer Architecture, Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190, China
[2]University of Chinese Academy of Sciences, Beijing 100049, China
[3]Peng Cheng Laboratory, Shenzhen 518052, China

Corresponding author: Jing Ye (yejing@ict.ac.cn)

This work was supported by the National Natural Science Foundation of China (NSFC) under Grant 61532017, Grant 61704174, Grant 61432017, and Grant 61521092.

ABSTRACT Scan chains increase the testability but decrease security. Attackers may use scan chains to launch attacks to obtain sensitive information, which poses serious security threats. The scan chain-based attacks contain two steps: 1) scan data obtaining, including mode switching obtaining method and test mode only obtaining method, and 2) scan data analysis, including data mapping analysis method and signature analysis method. To prevent these attacks, various secure scan designs have been proposed. These designs are summarized into two categories: scan chain modification and scan input/output restriction. This paper gives a survey of the scan chain-based attacks and countermeasures. The secure scan designs are summarized and compared from the aspects of security, testability, test time, and hardware overhead.

INDEX TERMS Scan chain based attacks, test mode, mode switch, signature, secure scan chain, secret key, physical unclonable function.

I. INTRODUCTION

Testing is one of the most important steps in the Integrated Circuit (IC) manufacturing process to guarantee product quality. In order to facilitate testing, scan chain design is proposed and widely adopted. It connects selected storage elements to construct multiple shift registers [1], which improves the controllability and the observability of the internal states of circuits. Scan chain design is currently the most popular structured Design-For-Test (DFT) technique. However, it also brings security threats just like the sword of Damocles, which can be maliciously used by attackers to steal information such as cipher key and IP, even to control the chip illegally. These attacks are called the scan chain based attacks.

Scan chain based attack consists of two phases: scan data obtaining, and scan data analysis. Two ways are leveraged by attackers to obtain the scan data: mode switching obtaining method [2]–[15] and test mode only obtaining method [17]–[23]. Their difference is that mode switching obtaining method needs to switch the chip from normal mode to test mode, and then shift out the scan data stored in the scan chain, but test mode only obtaining method does not require mode switching. Then, the scan data is analyzed by attackers to retrieve sensitive information. According to whether the mapping relation between scan cells and sensitive information is inferred during analysis, it can be classified into two categories: data mapping analysis method [6]–[15] and signature analysis method [40]. The former one infers the mapping relation while the latter one does not. Currently, various cryptographic chips implementing Data Encryption Standard (DES) [2], Advanced Encryption Standard (AES) [3], Rivest-Shamir-Adleman (RSA) [8], Elliptic Curve Cryptography (ECC) [15], NTRUEncrypt [5], and Linear Feedback Shift Register (LFSR) based stream ciphers [4] are surrendered under scan chain based attacks.

In order to deal with the threats posed by the scan chain based attacks. Numerous secure scan designs have been proposed. In general, two strategies are used in these designs to improve the security of the scan chain. The first is scan chain modification. The original scan chain path is modified to obfuscate the data stored in the scan chain. Although attackers can get access to the scan chain, the effective information cannot be obtained from the obfuscated data any more. Specifically, in this paper, eleven common secure scan designs using this strategy is introduced: Flipped Scan [24], XOR Scan [25], Double Feedback XOR Scan [26], rXOR Scan [27],

The associate editor coordinating the review of this manuscript and approving it for publication was Songwen Pei.

TABLE 1. Summary of attacks.

		Mode Switching Obtaining		Test Mode Only Obtaining	
Target chip	**Advanced DFT Structure**	**Data Mapping Analysis**	**Signature Analysis**	**Data Mapping Analysis**	**Signature Analysis**
DES	×	[2]	[12]		
	✓		[15]		
AES	×	[3]	[6]	[17-20]	[40]
	✓		[9-11, 14, 15]	[21-23]	
RSA	×		[8]		
	✓		[13,15]		
ECC	×		[7]		
	✓		[15]		
NTRUEncrypt Cryptosystem	×	[5]			
LFSR based Stream Ciphers	×	[4]			

State Dependent Scan Flip-Flop [28], [29], Dynamically Obfuscated Scan [30], [31], Test Key Integrated Scan [32]–[35], Sub-chains based Scan [36]–[39], Static and Dynamic Obfuscation of Scan [40], [41], and Partial Secure Scan [42], [43]. The second is scan input/output restriction. By restricting the access to the scan chain with certain authentication module, attacker can no longer use the scan chain correctly without authority. Three designs exploiting this strategy are introduced: Encryption based Scan [44]–[47], Bias PUF based Scan [48], and Secure Test Wrapper [50].

In comparison with previous survey papers [52]–[54], this paper has two main contributions. Firstly, from the perspective of scan chain based attacks, this paper introduces the two phases, scan data obtaining and scan data analysis respectively to detail the attack process. Secondly, from a defensive point of view, this paper fully compares existing secure scan chain designs from the aspects of security, testability, test time, and hardware overhead, which are summarized in one table.

The rest of the paper is organized as follows: Section II describes scan chain based attacks. Section III analyzes and summaries existing secure scan designs. Finally, the conclusion is given in Section IV.

II. ATTACKS

This section will review the scan chain based attack methods. So far, they have been mainly used to attack various cryptographic chips. The attackers try to use the scan chain to recover secret keys from the cryptographic chips implementing certain encryption algorithms. For these cryptographic chips, if the scan cells store intermediate encryption results, attackers can obtain the sensitive information by shifting out the content stored in the scan chain under test mode. Then, the secret key can be retrieved through the analysis of these intermediate encryption results. All the above attack methods are summarized in Table 1.

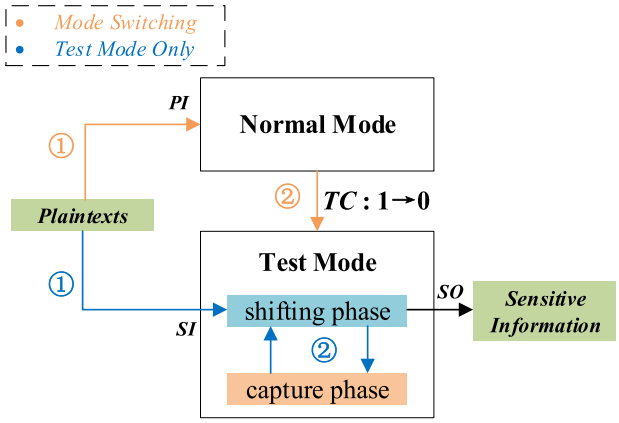

FIGURE 1. Mode Switching and Test Mode Only Obtaining.

A. MODE SWITCHING OBTAINING & DATA MAPPING ANALYSIS

In this attack, the scan data is obtained by switching the cryptographic chip from normal mode to test mode. Specifically, as shown in Figure 1, at first, the chip is reset and the plaintexts are inputted. Then the chip runs in normal mode for one clock cycle. In this way, the plaintexts inputted will be processed and the intermediate encryption result will be stored in the scan cells. Next, the chip is switched to test mode, and the intermediate encryption result is shifted out through the scan chain. This procedure is repeated by applying different plaintexts. In this way, enough scan data can be collected. Next, the scan data is analyzed to infer the mapping relation between scan cells and sensitive information. Once the mapping relation is speculated, the secret key can be recovered.

Earliest in 2004 [2], this attack on DES cryptographic chip is conducted successfully, and the secret key stored in the chip is retrieved. This is the first scan chain based attack.

The DES is a symmetric encryption algorithm developed by IBM in the 1970s. In DES, a 56-bit user key is used to encipher a 64-bit block of data into a 64-bit cipher text by permutation and substitution. The DES algorithm has a short key length of only 56 bits, so now is vulnerable to brute force attack. In addition to DES, the scan chain based attack is also applied to AES chip in [3]. AES is adopted by the National Institute of Standards and Technology (NIST) to replace existing DES as a standard for symmetric encryption. AES is also a block cipher algorithm with a block size of 128 bits, but has three different key lengths: AES-128, AES-192, and AES-256. With long enough key bits, it is computationally impossible to crack the AES algorithm by brute force attack. However, with the help of the scan chain, a cryptographic chip implementing the AES algorithm is also successfully cracked.

B. MODE SWITCHING OBTAINING & SIGNATURE ANALYSIS

The data mapping analysis method is based on the assumption that the scan chain only contains registers related to encryption module, and the mapping relation can be well inferred. Unfortunately, the assumption is not always realistic. In the real industrial environment, to reduce the test costs and achieve high fault converge, some advanced DFT structures are used such as multiple scan chains, response compactor, partial scan, X-masking, and X-tolerant. These advanced DFT structures are intrinsic countermeasures against data mapping analysis methods [10]. Therefore, to overcome such limitations, improved scan data analysis method, named signature analysis, is explored.

In [6]–[15], the scan data is still obtained by mode switching, but the data analysis is based on scan signature. In this method, a simulator is introduced to simulate the encryption algorithm implemented in the target cryptographic chip. The simulator and the target cryptographic chip are inputted with the same plaintexts. They run under normal mode with a guessed key and the real secret key respectively. In this way, two data sets are obtained after repeatedly switching from the normal mode to the test mode under different plaintexts. In Figure 2, each row of the data shown below the SFF represents the scan data to be shifted out of a plaintext. If N plaintexts are inputted, then N rows of corresponding scan data will be obtained. The scan signature means a particular 1-bit column scan data in the obtained N rows of scan data. Attackers do not need to infer the mapping relation between scan cells and sensitive information, but directly search the simulated scan signatures in the scan data of the target cryptographic chip. If all the simulated scan signatures can be found out, the guessed key is correct. Otherwise, a new guessed key will be applied. Such scan chain based attack using scan signature have been used to deal with DES chip [12], [15], AES chip [6], [9]–[11], [14], [15] and RSA chip [8], [13], [15] even in the presence of advanced DFT structures.

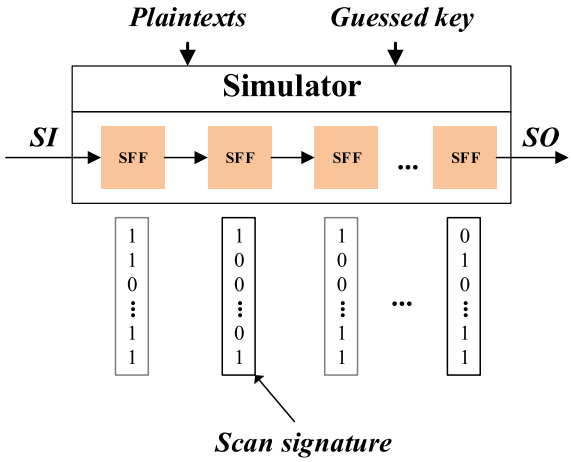

FIGURE 2. Signature Analysis Method.

C. TEST MODE ONLY OBTAINING & DATA MAPPING ANALYSIS

Mode switching obtaining method has one obvious limitation. It assumes that the data stored in the scan cells is intact during the switch process. Hence, to resist such method, [16] proposes to reset the chip whenever the chip is switched from normal mode to test mode. In this way, attackers cannot retrieve intermediate results through the scan chain any more.

Therefore, attackers try to use test mode only for obtaining useful information [17], [18]. Compared with mode switching data obtaining, test mode only obtaining method does not require the switching between normal mode and test mode. As shown in Figure 1, the plaintext is shifted in through the scan chain, then the encryption process is performed by capture, and the encryption result is shifted out through the scan chain. Here, attackers need to infer the mapping relation between the data shifted in and the input of the encryption circuit. In this way, attackers can still obtain intermediate results and the data mapping analysis can be applied. Such scan chain based attack has been used to crack the chip implementing AES in [17]–[23].

D. TEST MODE ONLY OBTAINING & SIGNATURE ANALYSIS

In [40], the scan data is obtained by test mode only, and the data analysis is based on signature. Since the test mode only data obtaining method is used, the simulator used here is a little different from Section *B*, but the core idea is the same. The AES chip is cracked in [40].

E. SUMMARY

For attackers, to launch a mode switch attack, the signals for controlling the test mode and the normal mode should be known in advance. If the switching from the normal mode to the test mode is not allowed, this method will fail. However, the test mode only method avoids this weakness without operation of mode switching. On the other hand, sometimes it is difficult for attackers to get the accurate data

mapping relation. Reverse engineering may be helpful to solve this problem, but expensive equipment is required. On the contrary, the signature analysis method has less requirements.

III. COUNTERMEASURES

Scan chain based attacks have severe threats, which make many popular cryptosystems vulnerable. Hence, to defend against such attacks, various countermeasures have been proposed. These countermeasures have large differences in structural design and security level. Some countermeasures are simple in design, but may have limited defense capability, and cannot impede all existing attacks. Others have higher security level, but may face with problems such as excessive hardware overhead and reduced testability. In this section, these countermeasures are summarized, and two main strategies are applied in the listed countermeasures:

1) Modifying the design of the scan chain such as inserting inverters, XOR gates, or other obfuscation logics, dividing the original scan chain into sub-chains, replacing traditional Scan Flip-Flops (SFF) to prevent attackers from fully controlling or observing the scan data along scan chains.

2) Adding modules such as cipher module or mask module before the scan in port and after the scan out port. In this way, the attackers are prevented from inputting specific test data into the scan chain, and obtaining sensitive information by shifting out the intermediate encryption results stored in the scan chain.

Some countermeasures combine multiple strategies to improve security. In the following content, each countermeasure is described including its design structure, security analysis, testability, test time, and hardware cost. Since different works use different ways or technologies to evaluate their hardware costs, and the hardware costs of some designs depend on the designer-defined parameters, this survey only roughly compares their hardware costs.

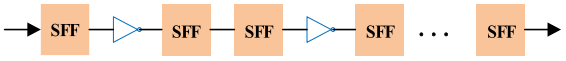

FIGURE 3. Flipped scan.

A. FLIPPED SCAN

To protect the sensitive information from being leaked, a flipped scan chain design is proposed in [24]. As shown in Figure 3, a certain number of inverters are inserted between randomly selected scan cells, and only the designers know where the inverters are inserted. The working principle of this method is that the randomly inserted inverters in the scan path change the values of scan data, which makes it difficult for attackers to ascertain the intermediate results stored in the scan chain. Hence, without obtaining effective data, the scan chain based attack cannot be conducted.

However, it is proved in [25] that the positions of the inserted inverters can be determined easily by resetting all the flip-flops in the scan chain. Specifically, if the chip is reset, all the content in the scan cells is initialized to zero. Then, attackers obtain the scan out pattern by running the chip under test mode. The scan out pattern includes the series of 0 and 1 because of the reversion of the inverters. By analyzing the scan out pattern, the locations of the inserted inverters can be deduced. Once the locations of the inserted inverters are known, the obfuscation to the sensitive information does not work, so this design is no more secure.

For testability, since only inverters are inserted, scan cells can still obtain required logic values of test vectors, so it is not affected. The test time includes three parts: the time for entering test mode, the shift time for loading and unloading test vectors, and the time of capturing. Among them, the shifting time occupies mostly. If the number of test vectors is N, and the length of scan chain is L, the shift time of test vectors is $(1 + N) \times L$ at least. Since no extra scan cells are added, and N and L are not changed, the test time is not affected. As for the hardware cost, the overhead depends on how many inverters are inserted.

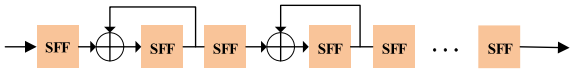

FIGURE 4. XOR scan.

B. XOR SCAN

Instead of inserting inverters, a different scan design named XOR scan is proposed in [25]. It is based on the insertion of XOR gates at the random point of the scan chain. Figure 4 shows an example of XOR scan design. One of the inputs to the XOR gate comes from the upstream scan cell, while the other comes from the downstream scan cell. If the positions of the XOR gates are unknown to the attackers, then it is hard for attackers to obtain effective data for analysis.

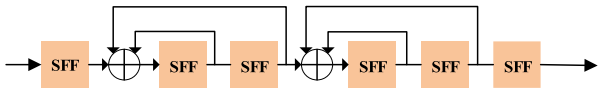

FIGURE 5. Double Feedback XOR scan.

However, similar as the flipped scan chain design, it is shown in [26] that such a countermeasure is still vulnerable. The adversary is able to determine the number and positions of the XOR gates in the scan chain. Reference [26] attempts to overcome this weakness. An improved scan design based on XOR scan is proposed, which is called Double Feedback XOR scan shown in Figure 5. This design is very similar to the previous XOR scan, except that the output of two downstream flip-flops are fed back to the XOR gate instead of one. Unfortunately, it still fails. The work in [27] found a way to deduce the locations of inserted XOR gate in the double feedback XOR scan design.

Later, [27] proposes a novel countermeasure based on randomization of XOR gates named rXOR scan shown

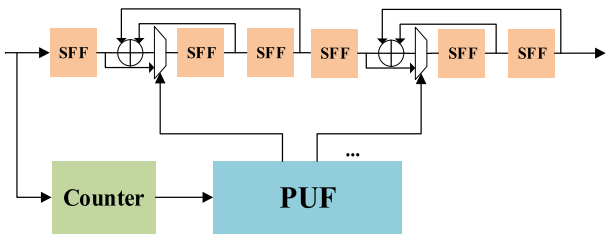

FIGURE 6. Random XOR scan.

in Figure 6. In this design, a multiplexer is inserted at the end of every Double Feedback XOR gate, which can select the input from the upstream flip-flop or from Double Feedback XOR gate. Besides, a Physical Unclonable Function (PUF) is introduced to generate selection signals of the multiplexers. The introduction of multiplexer and PUF improve the randomness and security of this design. Currently, no published works claim to crack this design.

In XOR scan design, the inserted XOR gates do not stop scan cells from obtaining required logic values of test vectors, so the testability is not affected. Meanwhile, the number of test vectors and the length of scan chain are not changed, so the test time is not affected either. As for the hardware cost, compared with the flipped scan chain, the hardware overhead of XOR scan, Double Feedback XOR scan, and rXOR scan are larger since the XOR gates are larger than the inverters, and multiplexers and PUF are added in some designs

C. STATE DEPENDENT SCAN FLIP-FLOP BASED SCAN

Instead of inserting inverters or XOR gates into the scan chain, [28], [29] proposes the State Dependent Scan Flip-Flop (SDSFF) to replace traditional SFF in the scan chain.

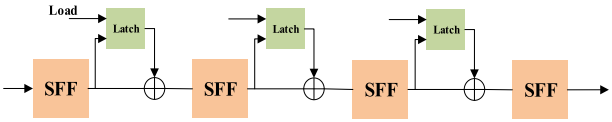

FIGURE 7. State Dependent Scan Flip-Flop.

As shown in Figure 7, in SDSFF, an XOR gate and a latch are integrated into the traditional SFF. The latch is used to memorize the past value of the SFF, and XOR with the data in the previous SFF before being shifted to the next SFF. According to the load signal, the value in the latch can be updated time by time. The output of a SDSFF can be switched from the current value of the SFF to its historical value. Hence, the scanned data is changed dynamically. In this way, the attackers are blocked from retrieving sensitive data from the scan chain.

To attack this SDSFF-based design, attackers have to know the number of SDSFFs, the positions of SDSFFs, and how the data in the latch changes by time. These all increase the difficulty of attackers. Hence, no published works claim to crack this design.

In this design, to use the scan chain, complex test data adaption is required to make scan cells obtain right test vectors. The fault coverage may be compromised [40], [41]. On the other hand, the length of scan chain is not changed. If the number of test vectors is not changed either, then test time is not affected. As for the hardware cost, compared with the XOR scan, the hardware overhead of SDSFF is larger since latches are added.

D. DYNAMICALLY OBFUSCATED SCAN

A Dynamically Obfuscated Scan (DOS) design is proposed in [30] and [31]. It obfuscates the scan data in the scan chain by inserted XOR gates dynamically selected by an obfuscation key.

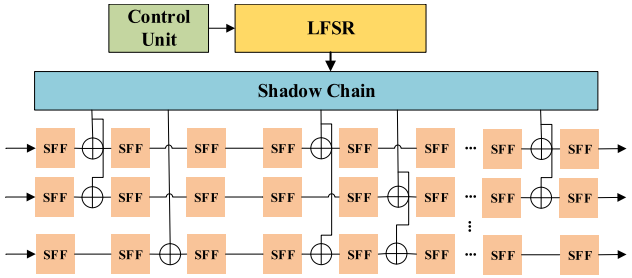

FIGURE 8. Dynamically obfuscated scan.

As shown in Figure 8, this secure scan design is composed of four parts: a control unit, a LFSR, a shadow chain, and scan chains with XOR gates. The control unit is used to generate signals that load control vector from the non-volatile memory in the secure zone, and determine the update frequency of obfuscation key. The input of the LFSR comes from the seed provided by the Control Vector. Then, the LFSR generates the obfuscation key, which is used to scramble the scan data. The shadow chain is used to protect the obfuscation key from being leaked, and propagate the obfuscation key to select correspond XOR gates. In this way, the scan data in the scan chain is dynamically obfuscated by the obfuscation key, which make it infeasible for attackers to get effective information.

Due to dynamic obfuscation to scan data, this design is robust against existing scan chain based attacks. Meanwhile, with protection to the obfuscation key, the risk of leaking obfuscation key is also eliminated. This design is similar to the XOR scan except that the XOR operations are controlled by the obfuscation key. Hence, the testability and the test time are not affected, but the hardware overhead is much larger than above designs. In above designs, only some inverters, XOR gates, multiplexers, or latches are inserted into the scan chain, but here a shadow chain is added with corresponding controllers.

E. TEST KEY INTEGRATED SCAN

In [32] and [33], a secure scan design based on integrating a test key into test vectors is proposed. The test key is verified by a checking circuit. If the test key in the test vectors

is right, correct response will be scanned out. Otherwise, unpredictable responses will be scanned out, which makes the analysis of scan data infeasible.

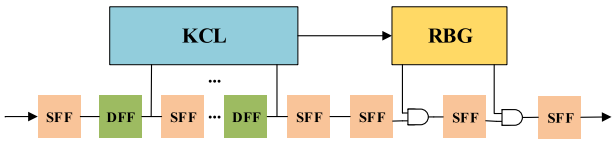

FIGURE 9. Test key integrated scan.

As shown in Figure 9, this design composes of three components: scan chain inserted with dummy flip-flops, Key Checking Logic Module (KCL), and Random Bit Generator (RBG). The dummy flip-flops are used as test key register, and each dummy flip-flop is similar to the scan flip-flop except that they have no connection with the combinational circuits. The number of dummy flip-flops is decided by the size of the test key. The KCL is used to check whether the test key stored in the dummy flip-flops is right. If the test key fails to be checked by KCL, the RBG will play a role in making the scan chain output unpredictable. The similar idea is also used in [34] and [35]. Only if a specific sequence of test keys is scanned in, the response can be scanned out correctly.

In this design, the security is ensured by the test key integrated in the test vector. Without right test key, the unauthorized user can only get random responses. However, though the testability is not affected, the test time is increased. For each test vector, the test key is integrated, so the test data volume and the shift time are increased. As for the hardware overhead, it depends on the length of the test key. Generally, its hardware overhead should be less than the dynamically obfuscated scan because it only adds several dummy flip-flops along the scan chain instead of adding a whole shadow chain; its hardware overhead should be also larger than the XOR scan since KCL and RBG are added for control.

F. SUB-CHAINS BASED SCAN

In order to defend against scan chain based attacks, some secure scan designs based on dividing the scan chain into several sub-chains are proposed. Then, by obfuscating the scan order of these sub-chains, the sensitive information is protected from being retrieved.

In [36] and [37], the Lock & Key scan design is proposed. As shown in Figure 10, in the design, the original scan chain is divided into multiple smaller sub-chains with equal length. Then, a Test Security Controller (TSC) is introduced to control the work sequence of the sub-chains. The TSC works in two modes: secure mode or insecure mode, which is decided by the authority of the user. The TSC consists of four parts: a test key comparator, a Finite State Machine (FSM), a LFSR, and a one-hot decoder. The test key comparator is used to determine whether the user inputs the correct key. Without the correct key, the FSM will set the TSC into insecure mode. The decoder transforms the output of LFSR into a one-hot code, which enables one sub-chain to work at a time. Only when

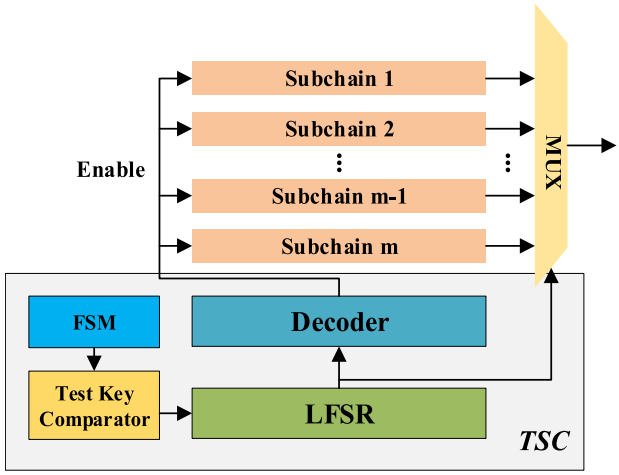

FIGURE 10. Sub-chains based secure scan.

the TSC is under secure mode, can these sub-chains work in the correct order. Otherwise, the work order is unpredictable. Similarly, in [38] and [39], a Random Order Scan (ROS) design is proposed. The scan chain is also divided into sub-chains, and the connection order of these sub-chains can be dynamically changed.

Although the original scan chain is divided into sub-chains in this design, the scan cells can still get required logic values of test vectors, and the total scan chain length is not increased. Hence, the testability and the test time are not impacted. However, [42] has proven that designs by obfuscating scan chain order cannot provide sufficient security as predicted. As long as complete scan chain states are obtained, this design may be cracked by attackers. As for the hardware cost, though we do not have the specific implementation of the TSC, according to its content, we consider its hardware cost is similar to that of test key integrated scan.

G. STATIC AND DYNAMIC OBFUSCATION OF SCAN DATA

In [40] and [41], secure design based on static and dynamic obfuscation of scan data is proposed. Different from other designs, the obfuscation is achieved by changing the mode of some selected scan cells in the scan chain.

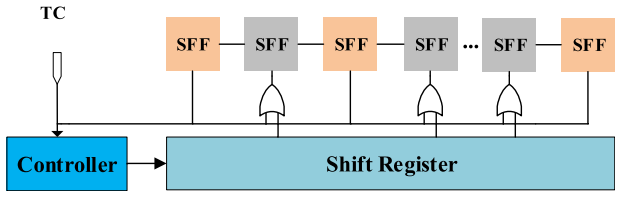

FIGURE 11. Static obfuscation of scan data.

As shown in Figure 11, the secure scan design named Static Obfuscation of Scan Data (SOSD) is presented. this design consists of a controller and a Shift Register (SR). The SR is used to control the selected scan cells from the scan chain. The working principle is that only when the SR is configured

with the right key, can the selected scan cells work normally under test mode. Otherwise, the selected scan cells will fetch the status of CUT (Circuit Under Test) to shift in the scan chain, which makes it difficult for attacker to get sensitive information from the obfuscated scan data.

Although the design of SOSD improves the security of the scan chain, it may still suffer from test mode only based signature attack. This is because once the scan cells are selected, the design will not change again, i.e. it is static. So, attackers may still use signature analysis method to crack it. Hence, on the basis of SOSD design, an improved secure design named Dynamic Obfuscation of Scan Data (DOSD) is proposed in the same paper. DOSD dynamically changes the selected scan cells, which increases the attack difficulty enormously.

Compared with SOSD, DOSD design is secure enough against existing attacks, and no newly attacks have been proposed to crack this design so far. Although some scan cells are controlled by the shift register, they can work the same as original ones if correct key is inputted. Hence, the testability is still preserved, and the test time is not increased. As for the hardware cost, the DOSD costs more than SOSD to achieve dynamic property. Though we do not have the specific implementation of the DOSD, according to how it works, we consider its hardware cost is similar or no more than that of sub-chains based scan.

H. PARTIAL SECURE SCAN

In [43], secure scan design based on the partial scan is used to prevent scan chain based attacks. The main idea is to remove the scan flip-flops storing sensitive information from the full scan chain. In this way, the attackers are unable to get access to such sensitive information. However, this design also limits test engineers from controlling and observing the internal states of the circuits, which reduces the testability. To deal with this challenge, a novel secure partial scan design is introduced in [44].

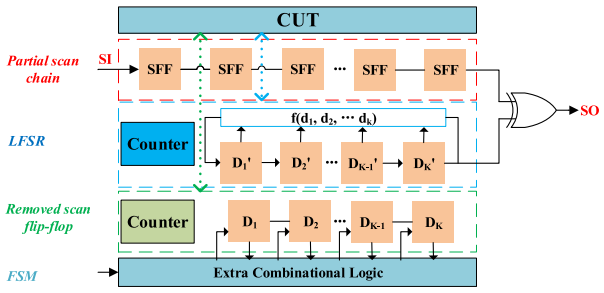

FIGURE 12. Partial secure scan.

As shown in Figure 12, the design consists of four major components. The partial scan chain contains scan flip-flops which do not contain sensitive information. The un-chained flip-flops removed from the scan chain store sensitive information. They are connected to the CUT but not to the SI/SO ports. To ensure the controllability of the un-chained scan flip-flops, extra combinational logic, a FSM, is introduced to set their values.

The LFSR stores a backup copy of the removed scan flip-flops to ensure the observability of these flip-flops. Meanwhile, the output of the LFSR is XORed with the partial scan chain output. Without knowing the state of the FSM and the configuration of the LFSR, attackers cannot control and observe the value in the un-chained flip-flops. Consequently, the scan chain based attacks will fail.

In conclusion, by removing scan cells storing sensitive information, the partial scan design can effectively prevent scan chain based attacks. At the same time, the full testability is maintained by ensuring the controllability and observability to the circuit. Moreover, with shorter scan chain length, the test time is decreased. However, to achieve these benefits, the hardware overhead is large.

I. ENCRYPTION BASED SCAN

In [45]–[48], a novel secure scan design based on scan data encryption is proposed. The working principle of this design is to use scan data encrypted by a lightweight block cipher for test so that only trusted users with right secret key can control and observe the data shifting along the scan chain.

As shown in Figure 13, in the design, an input cipher and an output cipher are added to the input end and output end of the original scan chain respectively. The input scan cipher is used to decrypt test data, while the output scan cipher is used to encrypt scan response. At first, the encrypted test pattern is inputted through the input cipher module for decryption. Then, the decrypted test pattern is shifted into the original scan chain. At last, through the output cipher, the encrypted test response is shifted out. The test data is encrypted and decrypted with the same secret key provided by the Secret Key Management Unit (SKMU) embedded in the circuit. In this way, without the right secret key, attackers cannot input specific test patterns and obtain true test response. Hence, sensitive information cannot get from the encrypted test response for analysis. Consequently, scan chain based attacks cannot be conducted successfully.

With scan data encryption, this design can prevent attacks conducted by unauthorized users. With the correct secret key, test vectors can be shifted into scan cells without any loss of testability. However, the test time is increased because of the process of scan data decryption and encryption. The hardware cost depends on what decryption and encryption circuits are used. It may not less than that of partial secure scan.

J. BIAS PUF BASED SCAN

In [49], a Bias PUF based secure scan design is proposed. The main idea of this design is to mask input and output data of the scan chain when unauthorized user uses it. As shown in Figure 14, two mask modules are added at the input and output port of the scan chain respectively. Then, a Bias PUF module is introduced to control these two mask modules.

Different from the traditional PUF which produces response bit 0 and 1 in similar probability, the Bias PUF

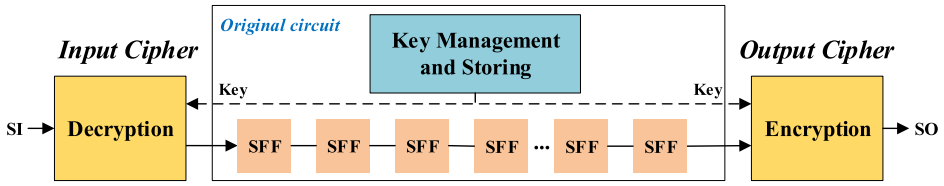

FIGURE 13. Encryption based scan.

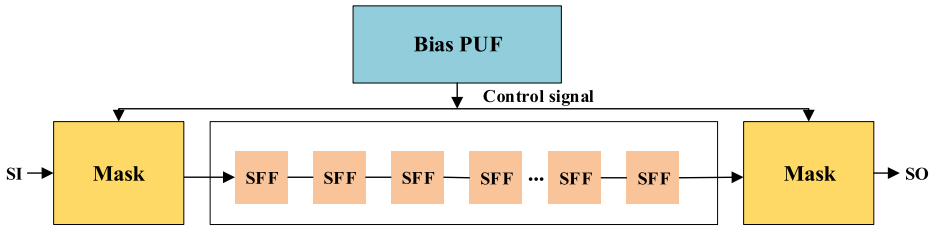

FIGURE 14. Bias PUF based scan.

can only generate response bit 1 (or 0) in rare challenges. Specifically, the Bias PUF proposed in [48] is based on the arbiter PUF. The arbiter PUF produces a response bit by comparing the delays of two paths controlled by challenge bits. By adding a buffer in one path of the arbiter PUF, the delay of the path is increased. In this way, the responses of the new PUF tend to be 0 (or 1) under most challenges. Hence, only a few challenges can produce response bit 1 (or 0). Then, these special challenges are used as secret keys to authorized users. The response of this Bias PUF is used as control signal to determine whether the mask modules work or not.

The mask modules are used to protect the input and output data of the scan chain. To use the scan chain, users have to input the secret key. Then, the Bias PUF verifies the correctness of the secret key. If the secret key is right, the control signal generated by the Bias PUF will disable the mask modules under test mode. Otherwise, the mask modules will make the data shifted in and out through the scan chain to be all zero, which make it impossible for attackers to input special test patterns and extract effective information. So, the security of this design is ensured.

For this design, except the added I/O mask modules, the original scan chain is not changed at all. Once the authentication is passed, the scan chain works just as before. Hence, the testability is not influenced. The authentication only executes once, not for every test vector, so this design has negligible effect on test time. In addition, PUF, as a lightweight authentication circuit, normally has less hardware cost than encryption/decryption circuits.

K. SECURE TEST WRAPPER BASED SCAN

IEEE 1500 test wrapper is a standard architecture for enabling test reuse and integration for embedded cores and associated circuitry [50]. Reference [51] proposes a Secure Test Wrapper (STW) on the basis of original IEEE 1500 test wrapper.

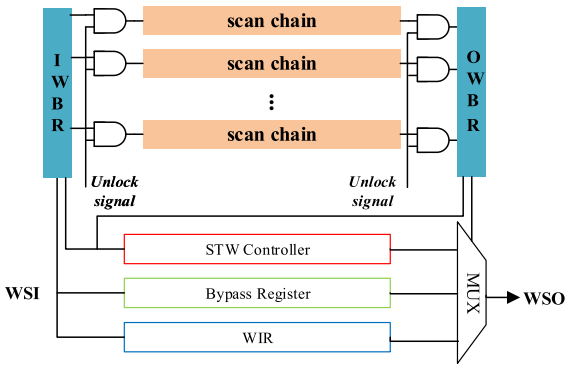

FIGURE 15. Secure test wrapper.

As illustrated in Figure 15, the main idea of this design is to protect the input and output of the scan chains by adding series of AND gates. An unlock signal is used to control these AND gates. The unlock signal is generated by the STW controller, which is used to compare the input from the user with the golden key (Secure Test Wrapper Key, STWK) generated by a LFSR. The LFSR reuses the same flip-flops of wrapper boundary scan cells to reduce hardware cost. If the input matches the STWK, the wrapper enters the unlock state. Otherwise, the wrapper is locked. In this way, the sensitive information in the scan chains is protected.

The testability and the test time are not affected if the right key is input. The hardware cost is less than the Bias PUF based scan since the secure test wrapper compares the input key with the golden key directly to determine the lock or unlock state.

L. SUMMARY

All the above secure scan designs are summarized in Table 2. In terms of security, simply inserting inverters or XOR gate in the scan path [24]–[26] without other dynamic protection units cannot provide enough security. Sub-chains based

TABLE 2. Summary and comparison of secure scan designs.

Secure Scan Designs		Key source	Security	Testability	Test time	Hardware overhead		
Strategies	Designs					Along scan chain	Outside scan chain	Estimation
Scan Chain Modification	Flipped scan [24]	×	×[25]	✓	✓	inverters		◆◇◇◇◇◇
	XOR scan [25]	×	×[26]	✓	✓	XOR gates		◆◆◇◇◇◇
	Double feedback XOR scan [26]	×	×[27]	✓	✓	XOR gates		◆◆◆◇◇◇
	rXOR scan [27]	PUF	✓	✓	✓	XOR gates, multiplexers	PUF	◆◆◆◆◇◇
	SDSFF based scan [28, 29]	×	✓	×[40,41]	✓	XOR gates, latches		◆◆◆◆◇◇
	DOS based scan [30, 31]	NVM	✓	✓	✓	XOR gates, extra chain	controller, LFSR	◆◆◆◆◆◆
	Test key integrated scan [32-35]	NVM	✓	✓	×	extra flip-flops	key checking unit, random generator	◆◆◆◆◆◇
	Sub-chains based Scan [36-39]	NVM	×[42]	✓	✓	multiplexers	controller, key checking unit, LFSR	◆◆◆◆◆◇
	SOSD based scan [40,41]	NVM	×[40,41]	✓	✓	OR gates	controller, shift registers	◆◆◆◆◇◇
	DOSD based scan [40,41]	NVM	✓	✓	✓	OR gates	controller, shift registers	◆◆◆◆◆◇
	Partial secure scan [42,43]	×	✓	✓	✓	extra flip-flops	controller, LFSR	◆◆◆◆◆◆
Scan I/O Restriction	Encryption based scan [44-47]	NVM	✓	✓	×		I/O cipher	◆◆◆◆◆◆
	Bias PUF based scan [48]	PUF	✓	✓	✓		Bias PUF, I/O mask	◆◆◆◆◇◇
	Secure test wrapper based scan [50]	NVM	✓	✓	✓		controller, I/O mask	◆◆◆◇◇◇

Key source: *Without secret key (×); Using NVM to store the secret key (NVM); Using PUF to generate the secret key (PUF).*
Security: *The design has been proven insecure (×); No published works claim cracking this design (✓).*
Testability: *Testability is compromised (×); No published works indicate the testability is impacted (✓).*
Test time: *The shift time of test is increased (×); Nearly no impact (✓).*
Estimation: *Lower hardware cost* (◇◇◇◇◇◇); *Higher hardware cost* (◆◆◆◆◆◆).

scan and SOSD based scan have also been proven insecure [41]–[43]. Among the rest of designs, the testability of the SDSFF based scan and the test time of the test key integrated scan and the encryption based scan are compromised. Finally, we find that the rXOR scan, the Bias PUF based scan, and the secure test wrapper based scan may have less hardware overhead than the DOS, the DOSD based scan, and the partial secure scan.

Among these three designs, the secure test wrapper based scan stores the secret key in the NVM, while other two designs leverage the PUF. In comparison with the NVM, the PUF leverages the process variation to generate inherent secret keys and can resist physical invasion attack, so provides higher security. The rXOR scan leverages the strong PUF with many CRPs to protect the data. The potential threat is that the strong PUF is vulnerable to machine learning attacks. Attackers may analyze the scan data to crack the PUF. The Bias PUF based scan proposes a new kind of PUF, whose responses are Bias to 0 or 1. Since machine learning attacks need to collect an effective training set, which contains both challenges with the response 0 and 1, the Bias PUF is naturally resistant to machine learning attacks.

In future works, there are several considerations. First, the security of above countermeasures is only analyzed toward existing attacks so far. Other attacks based on side channel, photon analysis, and so on may also need consideration. Second, the influence to test quality should be further assessed. Currently, only stuck at fault or transition fault is considered. The modification to scan chains may reduce the defect coverage of real chips, especially when scan compaction exists. Third, accroding to above analysis, Bias PUF based scan has certain advantages compared to other designs. However, its reliability may affect authentication, which needs further study.

IV. CONCLUSION

Because of the conflict between test and security, the attacks and defenses toward scan chain get more attention. This paper summarizes scan chain based attacks and countermeasures. The attack methods are classified respectively for the two steps of attack: scan data obtaining and scan data analysis. A full comparison of fourteen secure scan designs are presented in terms of security, testability, test time, and hardware overhead.

ACKNOWLEDGMENT

(Xiaowei Li and Wenjie Li contributed equally to this work.)

REFERENCES

[1] L. L. Wang, *Design For Testability*, 1st ed. Amsterdam, The Netherlands: Elsevier, 2012.
[2] B. Yang, K. Wu, and R. Karri, "Scan based side channel attack on dedicated hardware implementations of data encryption standard," in *Proc. Int. Conf. Test*, Oct. 2004, pp. 339–344.
[3] B. Yang, K. Wu, and R. Karri, "Secure scan: A design-for-test architecture for crypto chips," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 25, no. 10, pp. 2287–2293, Oct. 2006.
[4] Y. Liu, K. Wu, and R. Karri, "Scan-based attacks on linear feedback shift register based stream ciphers," *ACM Trans. Des. Automat. Electron. Syst.*, vol. 16, no. 2, Mar. 2011, Art. no. 20.
[5] A. A. Kamal and A. M. Youssef, "A scan-based side channel attack on the NTRUEncrypt cryptosystem," in *Proc. 7th Int. Conf. Availability, Rel. Secur.*, Aug. 2012, pp. 402–409.
[6] R. Nara, N. Togawa, M. Yanagisawa, and T. Ohtsuki, "A scan-based attack based on discriminators for AES cryptosystems," *IEICE Trans. Fundamentals Electron., Commun. Comput. Sci.*, vol. 92, no. 12, pp. 3229–3237, Dec. 2009.
[7] R. Nara, N. Togawa, M. Yanagisawa, and T. Ohtsuki, "Scan-based attack against elliptic curve cryptosystems," in *Proc. 15th Asia South Pacific Design Autom. Conf.*, pp. 407–412, Jan. 2010.
[8] R. Nara, K. Satoh, M. Yanagisawa, T. Ohtsuki, and N. Togawa, "Scan-based side-channel attack against RSA cryptosystems using scan signatures," *IEICE Trans. Fundamentals Electron., Commun. Comput. Sci.*, vol. 93, no. 12, pp. 2481–2489, Dec. 2010.
[9] J. DaRolt, G. Di Natale, M.-L. Flottes, and B. Rouzeyre, "Scan attacks and countermeasures in presence of scan response compactors," in *Proc. 6th IEEE Eur. Test Symp.*, May 2011, pp. 19–24.
[10] J. Da Rolt, G. Di Natale, M.-L. Flottes, and B. Rouzeyre, "New security threats against chips containing scan chain structures," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust*, Jun. 2011, p. 110.
[11] B. Ege, A. Das, S. Gosh, and I. Verbauwhede, "Differential scan attack on AES with X-tolerant and X-masked test response Compactor," in *Proc. 15th Euromicro Conf. Digit. Syst. Design*, Sep. 2012, pp. 545–552.
[12] H. Kodera, M. Yanagisawa, and N. Togawa, "Scan-based attack against DES cryptosystems using scan signatures," in *Proc. IEEE Asia–Pacific Conf. Circuits Syst.*, Dec. 2012, pp. 599–602.
[13] J. Da Rolt, A. Das, G. Di Natale, M.-L. Flottes, B. Rouzeyre, and I. Verbauwhede, "A new scan attack on RSA in presence of industrial countermeasures," in *Proc. Int. Workshop Constructive Side-Channel Anal. Secure Design*, May 2012, pp. 89–104.
[14] J. D. Rolt, G. Di Natale, M.-L. Flottes, and B. Rouzeyre, "Are advanced DfT structures sufficient for preventing scan-attacks?" in *Proc. IEEE 30th VLSI Test Symp.*, Apr. 2012, pp. 246–251.
[15] J. D. Rolt, G. Di Natale, M.-L. Flottes, and B. Rouzeyre, "A novel differential scan attack on advanced DFT structures," *ACM Trans. Des. Automat. Electron. Syst.*, vol. 18, no. 4, Oct. 2013, Art. no. 58.
[16] D. Hely, F. Bancel, M.-L. Flottes, and B. Rouzeyre, "Test control for secure scan designs," in *Proc. 10th IEEE Eur. Test Symp.*, Washington, DC, USA, May 2005, pp. 190–195.
[17] S. S. Ali, S. M. Saeed, O. Sinanoglu, and R. Karri, "Scan attack in presence of mode-reset countermeasure," in *Proc. IEEE 19th Int. On-Line Test. Symp. (IOLTS)*, Jul. 2013, pp. 230–231.
[18] S. S. Ali, O. Sinanoglu, S. M. Saeed, and R. Karri, "New scan-based attack using only the test mode," in *Proc. IFIP/IEEE 21st Int. Conf. Very Large Scale Integr.*, no. 1, Oct. 2013, pp. 234–239.
[19] S. S. Ali, O. Sinanoglu, and R. Karri, "Test-mode-only scan attack using the boundary scan chain," in *Proc. 19th IEEE Eur. Test Symp.*, May 2014, pp. 1–6.
[20] S. S. Ali, S. M. Saeed, R. Karri, and O. Sinanoglu, "New scan-based attack using only the test mode and an input corruption countermeasure," in *Proc. IFIP/IEEE Int. Conf. Very Large Scale Integr.-Syst. Chip*, vol. 1, Oct. 2013, pp. 48–68.
[21] S. S. Ali, S. M. Saeed, R. Karri, and O. Sinanoglu, "New scan attacks against state-of-the-art countermeasures and DFT," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust*, May 2014, pp. 142–147.
[22] S. M. Saeed, S. S. Ali, O. Sinanoglu, and R. Karri, "Test-mode-only scan attack and countermeasure for contemporary scan architectures," in *Proc. Int. Test Conf.*, Oct. 2014, pp. 1–8.
[23] S. S. Ali, S. M. Saeed, O. Sinanoglu, and R. Karri, "Novel test-mode-only scan attack and countermeasure for compression-based scan architectures," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 34, no. 5, pp. 808–821, May 2015.
[24] G. Sengar, D. Mukhopadhyay, and D. R. Chowdhury, "Secured flipped scan-chain model for crypto-architecture," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 26, no. 11, pp. 2080–2084, Nov. 2007.
[25] M. Agrawal, S. Karmakar, D. Saha, and D. Mukhopadhyay, "Scan based side channel attacks on stream ciphers and their counter-measures," in *Progress in Cryptology-INDOCRYPT*, Berlin, Germany: Springer, 2008, pp. 226–238.
[26] S. Banik and A. Chowdhury, "Improved scan-chain based attacks and related countermeasures," in *Progress in Cryptology-INDOCRYPT*, Cham, Switzerland: Springer, 2013, pp. 78–97.
[27] S. Banik, A. Chattopadhyay, and A. Chowdhury, "Cryptanalysis of the double-feedback XOR-chain scheme proposed in indocrypt 2013," in *Progress in Cryptology-INDOCRYPT*, Cham, Switzerland: Springer, 2014, pp. 179–196.
[28] Y. Atobe, Y. Shi, M. Yanagisawa, and N. Togawa, "Dynamically changeable secure scan architecture against scan-based side channel attack," in *Proc. Int. SoC Design Conf. (ISOCC)*, Nov. 2012, pp. 155–158.
[29] Y. Atobe, Y. Shi, M. Yanagisawa, and N. Togawa, "State dependent scan flip-flop with key-based configuration against scan-based side channel attack on RSA circuit," in *Proc. IEEE Asia–Pacific Conf. Circuits Syst.*, Dec. 2012, pp. 607–610.
[30] D. Zhang, M. He, X. Wang, and M. Tehranipoor, "Dynamically obfuscated scan for protecting IPs against scan-based attacks throughout supply chain," in *Proc. IEEE 35th VLSI Test Symp. (VTS)*, Apr. 2017, pp. 1–6.
[31] X. Wang, D. Zhang, M. He, D. Su, and M. Tehranipoor, "Secure scan and test using obfuscation throughout supply chain," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 37, no. 9, pp. 1867–1880, Sep. 2018.
[32] J. Lee, M. Tebranipoor, and J. Plusquellic, "A low-cost solution for protecting IPs against scan-based side-channel attacks," in *Proc. 24th IEEE VLSI Test Symp.*, Apr./May 2006, pp. 93–99.
[33] M. Tehranipoor and J. Lee, "Protecting IPs against scan-based side-channel attacks," in *Introduction to Hardware Security and Trust*, M. Tehranipoor and C. Wang, Eds. New York, NY, USA: Springer, 2012, pp. 411–427.
[34] U. Chandran and D. Zhao, "SS-KTC: A high-testability low-overhead scan architecture with multi-level security integration," in *Proc. 27th IEEE VLSI Test Symp.*, May 2009, pp. 321–326.
[35] M. A. Razzaq, V. Singh, and A. Singh, "SSTKR: Secure and testable scan design through test key randomization," in *Proc. Asian Test Symp.*, Nov. 2011, pp. 60–65.
[36] J. Lee, M. Tehranipoor, C. Patel, and J. Plusquellic, "Securing scan design using lock and key technique," in *Proc. 20th IEEE Int. Symp. Defect Fault Tolerance VLSI Syst.*, Oct. 2005, pp. 51–62.
[37] J. Lee, M. Tehranipoor, C. Patel, and J. Plusquellic, "Securing designs against scan-based side-channel attacks," *IEEE Trans. Dependable Secure Comput.*, vol. 4, no. 4, pp. 325–336, Oct./Dec. 2007.
[38] Y. Atobe, Y. Shi, M. Yanagisawa, and N. Togawa, "Secure scan design with dynamically configurable connection," in *Proc. IEEE 19th Pacific Rim Int. Symp. Dependable Comput.*, Dec. 2013, pp. 256–262.
[39] M. Oya, Y. Atobe, Y. Shi, M. Yanagisawa, and N. Togawa, "Secure scan design using improved random order and its evaluations," in *Proc. IEEE Asia–Pacific Conf. Circuits Syst. (APCCAS)*, Nov. 2014, pp. 555–558.
[40] A. Cui, Y. Luo, and C.-H. Chang, "Static and dynamic obfuscations of scan data against scan-based side-channel attacks," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 2, pp. 363–376, Feb. 2017.
[41] W. Zhou, A. Cui, H. Li, and G. Qu, "How to secure scan design against scan-based side-channel attacks?" in *Proc. IEEE 26th Asian Test Symp. (ATS)*, Nov. 2017, pp. 121–126.
[42] A. Cui, Y. Luo, H. Li, and G. Qu, "Why current secure scan designs fail and how to fix them?" *Integration*, vol. 56, pp. 105–114, Jan. 2017.
[43] M. Inoue, T. Yoneda, M. Hasegawa, and H. Fujiwara, "Partial scan approach for secret information protection," in *Proc. 14th IEEE Eur. Test Symp.*, May 2009, pp. 143–148.
[44] X. Chen, Z. Lu, G. Qu, and A. Cui, "Partial scan design against scan-based side channel attacks," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Aug. 2018, pp. 1484–1489.
[45] M. D. Silva, M.-L. Flottes, G. Di Natale, and B. Rouzeyre, "Experimentations on scan chain encryption with PRESENT," in *Proc. IEEE 2nd Int. Verification Secur. Workshop (IVSW)*, Jul. 2017, pp. 45–50.

[46] M. D. Silva, M.-L. Flottes, G. Di Natale, B. Rouzeyre, P. Prinetto, and M. Restifo, "Scan chain encryption for the test, diagnosis and debug of secure circuits," in *Proc. 22nd IEEE Eur. Test Symp. (ETS)*, May 2017, pp. 1–6.
[47] M. D. Silva, M.-L. Flottes, G. Di Natale, and B. Rouzeyre, "Preventing scan attacks on secure circuits through scan chain encryption," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 38, no. 3, pp. 538–550, May 2019.
[48] M. D. Silva, E. Valea, M.-L. Flottes, S. Dupuis, G. Di Natale, and B. Rouzeyre, "A new secure stream cipher for scan chain encryption," in *Proc. IEEE 3rd Int. Verification Secur. Workshop (IVSW)*, Jul. 2018, pp. 68–73.
[49] W. Li, J. Ye, X. Li, H. Li, and Y. Hu, "Bias PUF based secure scan chain design," in *Proc. Asian Hardw. Oriented Secur. Trust Symp. (AsianHOST)*, Dec. 2018, pp. 31–36.
[50] *IEEE Standard Testability Method for Embedded Core-Based Integrated Circuits*, IEEE Standard 1500-2005, 2011.
[51] G.-M. Chiu and J. C.-M. Li, "A secure test wrapper design against internal and boundary scan attacks for embedded cores," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 20, no. 1, pp. 126–134, Jan. 2012.
[52] G. Di Natale, M.-L. Flottes, B. Rouzeyre, and P.-H. Pugliesi-Conti, "Manufacturing testing and security countermeasures," in *Hardware Security and Trust*. Cham, Switzerland: Springer, 2017.
[53] S. M. Saeed, S. S. Ali, and O. Sinanoglu, "Scan design: Basics, advancements, and vulnerabilities," in *Hardware Security and Trust*. Cham, Switzerland: Springer, 2017.
[54] M. T. Rahman, D. Forte, and M. M. Tehranipoor, "Protection of assets from scan chain vulnerabilities through obfuscation," in *Hardware Protection Through Obfuscation*. Cham, Switzerland: Springer, 2017.

XIAOWEI LI (SM'04) received the B.Eng. and M.Eng. degrees in computer science from the Hefei University of Technology, Hefei, China, in 1985 and 1988, respectively, and the Ph.D. degree in computer science from the Institute of Computing Technology (ICT), Chinese Academy of Sciences (CAS), Beijing, China, in 1991. He was an Associate Professor with the Department of Computer Science and Technology, Peking University, Beijing, from 1991 to 2000. In 2000, he joined ICT, CAS, as a Professor, where he is currently the Deputy Director of the State Key Laboratory of Computer Architecture. He has authored or coauthored more than 300 papers in journals and international conferences, holds 66 patents and 50 software copyrights. His current research interests include VLSI testing, design for testability, dependable computing, hardware security, and wireless sensor networks.

Dr. Li has been serving as a member for the Steering Committee of ITC-Asia, since 2018. He is on the Technical Program Committee of several IEEE and ACM conferences, including ITC, VTS, and DATE. He was the Chair of the Technical Committee on Fault Tolerant Computing, the China Computer Federation, from 2008 to 2012, and the Steering Committee Chair of the IEEE Asian Test Symposium, from 2011 to 2013. He has been the Vice Chair of the IEEE Asia and Pacific Regional TTTC, since 2004. He currently serves as a Vice Chair for IEEE TTTC (2018–2019). He serves as an Associate Editor for JCST, JOLPE, JETTA, and the IEEE TCAD.

WENJIE LI received the B.S. degree in computer science and technology from the Taiyuan University of Technology, Taiyuan, China. He is currently pursuing the M.S. degree with the State Key Laboratory of Computer Architecture, Institute of Computing Technology (ICT), Chinese Academy of Sciences (CAS), Beijing. His current research interests include hardware security, AI security, and physical unclonable function.

JING YE received the B.S. degree in electronics engineering and computer science from Peking University, in 2008, and the Ph.D. degree from ICT, CAS, in 2014. He is currently an Associate Professor with the State Key Laboratory of Computer Architecture, Institute of Computing Technology (ICT), Chinese Academy of Sciences (CAS), and an Assistant Secretary-General of Technical Committee on Fault Tolerant Computing, China Computer Federation. He has published more than 50 papers and holds seven patents. His current research interests include VLSI test and security, and AI security. He received the IEEE TTTC's E. J. McCluskey Doctoral Thesis Award Semi-Final (Asia region) Second Place, and the Second Prize of the Beijing Science and Technology Award. He has been the Founder of the Annual Workshop on Hardware Security in China, since 2016.

HUAWEI LI (M'00–SM'09) received the B.S. degree in computer science from Xiangtan University, Xiangtan, China, in 1996, and the M.S. and Ph.D. degrees from the Institute of Computing Technology (ICT), Chinese Academy of Sciences (CAS), Beijing, China, in 1999 and 2001, respectively. She has been a Professor at ICT, CAS, since 2008. She visited the University of California at Santa Barbara, Santa Barbara, from 2009 to 2010. She has published more than 200 technical papers, and holds 27 Chinese patents. Her current research interests include testing of VLSI/SOC circuits, design verification, design for reliability, fault tolerance, and approximate computing. She was a recipient of the 2012 National Technology Invention Award of China.

Prof. Li was the Technical Program Co-Chair of the IEEE Asian Test Symposium (ATS), in 2007 and 2018, and the General Co-Chair, in 2014. She was the Technical Program Co-Chair of the IEEE International Test Conference in Asia, in 2018. She has served as the Steering Committee Chair of the IEEE Workshop on RTL and High Level Testing (2014–2016), served as the Steering Committee Vice Chair for ATS, from 2017 to 2019, served as the Chair for the China Computer Federation Technical Committee on Fault-Tolerant Computing, and served on the technical program committees for several IEEE conferences. She has served as an Associate Editor for the IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION, and served on the editorial boards for two Chinese journals: the *Journal of Computer-Aided Design and Computer Graphics* and the *Journal of Computer Research and Development*.

YU HU (M'06) received the B.S., M.S., and Ph.D. degrees in electrical engineering from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 1997, 1999, and 2003, respectively. She is currently a Professor with the Institute of Computing Technology, Chinese Academy of Sciences, Beijing, China. Her current research interests include autonomous driving, deep learning, and algorithm acceleration. She is a member of the Association for Computing Machinery (ACM), the Institute of Electronics, Information and Communication Engineers (IEICE), and China Computer Federation (CCF).