Hindawi
Security and Communication Networks
Volume 2021, Article ID 5222670, 9 pages
https://doi.org/10.1155/2021/5222670

Research Article

Preventing Scan-Based Side-Channel Attacks by Scan Obfuscating with a Configurable Shift Register

Weizheng Wang, Yin Chen, Shuo Cai, and Yan Peng

School of Computer and Communication Engineering, Changsha University of Science and Technology, Changsha 410114, China

Correspondence should be addressed to Weizheng Wang; peakexpe@csust.edu.cn

Received 26 July 2021; Revised 12 October 2021; Accepted 23 October 2021; Published 5 November 2021

Academic Editor: Jie Cui

Scan test is widely used in integrated circuit test. However, the excellent observability and controllability provided by the scan test gives attackers an opportunity to obtain sensitive information by using scan design to threaten circuit security. Hence, the primary motivation of this paper is to improve the existing DFT technique, i.e., to enhance the chip security on the premise of guaranteeing test quality. In this paper, we propose a new scan design method against scan-based side-channel attack. In the proposed method, the encryption structure is adopted, which requires the correct test authorization code to carry out normal test operation. Without the correct test authorization, the attackers cannot obtain the desired scan data, preventing the scan-based side-channel attacks. Furthermore, the test authorization code is determined by the nonvolatile memory built into the chip to realize the inconsistency of the test authorization code for each chip.

1. Introduction

In recent years, several technologies, such as sensor networks [1–4], wireless communication [5–8], smart grid [9, 10], big data [11, 12], and internet of things [13, 14], have been developed rapidly and their security has been widely researched [15]. At the same time, the researcher has been paying more and more attention to the security issue of the underlying hardware [16–18].

In the manufacturing process of integrated circuit, defects are inevitable. When system intrinsic faults and faults in the integrated circuit occur simultaneously [19–21], fault detection will become more difficult [22–24]. In order to detect the faults of integrated circuit, testing is becoming an indispensable step and occupies an important position. Based on this, the design of scan chain to facilitate testing is proposed and widely used. Scan chain design can provide high controllability and observability during testing. However, the design of the scan chain gives attackers an open door while providing convenience. In [25], Yang et al. first proposed the scan-based side-channel attack. If the scan chain is not encrypted, sensitive information such as intellectual property (IP) or secret keys [26, 27] could be exposed to attackers. Therefore, it is necessary to use a feasible solution to protect integrated circuits (ICs) from scan-based side-channel attacks [28].

In recent years, many scan-based attacks have been proposed to protect encryption systems. The scan-based side-channel attacks are mainly carried out through the acquisition and analysis of scan data. Currently, on-chip implementation of private key algorithms have been facing scan-based side-channel attacks, like Data Encryption Standard (DES) [29], Advanced Encryption Standard (AES) [30], Rivest-Shamire-Adleman (RSA) [31], Elliptic Curve Cryptography (ECC) [32], NtrueTrypt [33], and Stream Cryptography based on Linear Feedback Shift Register (LFSR) [34].

Based on this, many countermeasures are put forward to counter the scan-based attacks [35–44]. Previously, the existing advanced DFT architecture includes test response compactor, X-masker [45, 46], and X-tolerance [47, 48]. They were regarded as a powerful countermeasure of resisting scan-based attacks. This DFT architecture makes it difficult to apply plaintext input and obtain intermediate data from the scan chain, which provides a high level of security. However, recent research has shown that this strategy is also vulnerable. After inserting the test controller into the circuit under test, the state of the scan chain is cleared if the CUT is switched from functional mode to test mode [49]. This countermeasure is effective against mode-switching attacks, but they are not available against test-mode-only attacks. In [50], the technique keeps the password apart from the key module in test mode. It prevents an attacker from switching between test mode and functional mode. Another kind of methods obfuscate the scan output by changing the structure of the scan chain [51–56]. However, even without information about the scan cells, a skilled adversary can still carry out a signature attack [57, 58]. In [59], a solution is proposed, which is based on the lock and key of physical unclonable function, but this design method has a particularly high hardware overhead. Some methods resist scan-based attacks by reordering scan chains [60–69].

In order to protect the encryption chip from scan-based side-channel attacks, in this paper, we propose a new scan design method. In this method, only the user with the correct test authorization code can perform a normal scan. When a user without test authorization code tries to perform a scan test, the scan input/output data will be obfuscated. The test authorization code is determined by the values of the nonvolatile memory and the way the *D* flip-flops in a nonlinear shift register (NSR) connect with scan flip-flops. This means that the test authorization code for each encryption chip can be set differently. The main contributions of this paper are as follows:

(1) A novel scan design scheme based on test authorization is presented to overcome scan attacks. By embedding a small management circuit, the enhanced DFT scheme improves significantly the security of chip. Furthermore, the proposed scheme does not incur significant performance penalties, for example, without decreasing the testability of the chip and increasing any timing delay.

(2) The test authorization code can be changed when altering the configuration bits for the nonlinear shift register. Hence, the test authorization code can be different for two chips with the same design. This reduces substantially the risk of test authorization code disclosure. Even if one test authorization code is leaked, it will not affect all chips.

The rest of this paper is organized as follows. Section 2 describes the basic ideas, scan structure, and timing analysis of the proposed structure. Section 3 provides testability analysis, security analysis, and experimental results. Section 4 is the conclusion of this paper.

2. Proposed Secure Scan Design

2.1. Basic Idea of Proposed Secure Scan Design. In the proposed secure scan design, the test authorization code is used to manage scan operation. Only entering the correct test authorization code can enable the normal scan operation. When the test authorization code is wrong, the scan-in stimulus and scan-out response are randomly XORed with the value of the node inside the combinational logic unit. At the same time, the wrong key will cyclically shift in the NSR, making data obfuscation elusory. Since the scan data is obfuscated, attackers will be misled into inferring incorrect results.

After power-on, the circuit is reset first. The operation mode of the circuit is controlled by the shift enable signal *SE*. When *SE* is set to low (“0”), the circuit enters in functional mode. When *SE* changes from “0” to “1,” enter the test authorization code from the first clock cycle of the scan test, and the *N*-bit test authorization code should be entered in *N* clock cycles. If the test authorization code is correct, normal scan operations can be carried out and the scan data will not be affected. If not, the circuit cannot perform the normal scan operation and the scan data will be obfuscated. The attacker will mistakenly believe that is the correct scan data and infer incorrect results. In order to strengthen the security of the encryption chip, the nonvolatile memory is used to control the test authorization code of each chip to be different. The test authorization code is determined by both the values of the nonvolatile memory and the output port (Q or $\overline{\text{Q}}$) of the *D* flip-flops in the NSR used to control the scan chain.

The proposed scan design method is a new architecture. In the following introduction, we first introduce the secure scan design and then show how to perform the test operation on a protected chip.

2.2. Scan Architecture of Proposed Secure Scan Design. As shown in Figure 1, the proposed secure scan structure is mainly composed of nonvolatile memory, nonlinear shift register (NSR), scan chain, and some control logic. The scan chain, made up of scan flip-flops (SFFs) marked in blue, is the intrinsic component in the standard scan design. The configurable NSR is used to store the test authorization code. If the test authorization code is *N* bits, an *N*-bit vector is needed to prestore in the nonvolatile memory to configure the NSR. The NSR contains *N D* flip-flops, each of which is preceded by a 2-to-1 Multiplexer. The multiplexer has two data inputs, which are connected with the output *Q* and $\overline{Q}$ of the front *D* flip-flop, respectively. The address input driven by a configuration bit in the nonvolatile memory is used to determine which data input is selected. Therefore, if the bit in the nonvolatile memory is “0,” it indicates that the output $\overline{Q}$ of the front *D* flip-flop derives the next *D* flip-flop. Instead, if the bit is “1,” it implies the output *Q* of the front *D* flip-flop derives the next *D* flip-flop. It should be pointed out that the *D* input to the first *D* flip-flop is controlled by an additional 2-to-1 multiplexer. The two data inputs of the multiplexer are, respectively, connected to the last *D* flip-flop and the test authorization code input pin.

In the proposed structure, the scan chain is modified; that is, some XNOR gates are inserted between scan flip-flops. The output of a NAND gate serves as one of the inputs to the XNOR gate between scan flip-flops. The output *Q* (or its complement $\overline{Q}$) of a *D* flip-flop in NSR is connected with one input of the NAND gate, and the other input is driven by

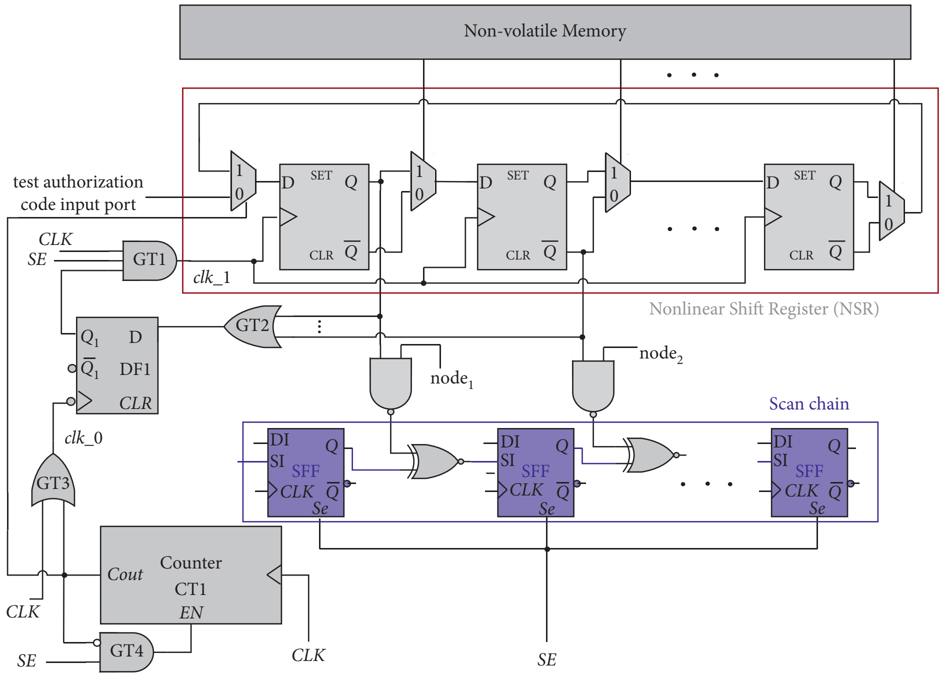

Figure 1: Proposed secure scan structure.

a combinational logic node selected randomly from CUT. On the assumption of *Q* connection, if the output *Q* of a NSR cell is 0, the NAND gate generates "1," and the output of the XNOR gate is decided by the preceding scan flip-flop. Otherwise, if the output *Q* of a NSR cell is "1," the output of the NAND gate is decided by the combinational logic node. When the combinational logic node is also "1," the low level output of the NAND gate will make the succeeding scan flip-flop receive the opposite value of the preceding scan flip-flop. By this way, the logic obfuscation in the scan chain is achieved. Due to the uncertainty about the value of the combinational logic node, the logic obfuscation is haphazard and thus difficult to analyze. It is not difficult to see that if the *Q* output of a NSR cell is used to hardwire to the NAND gate, to enable the normal scan operation the state of the NSR cell should be 0. On the contrary, if it is the complement output $\overline{Q}$, the state of the NSR cell should be 1. We define the expected NSR state enabling the normal scan operation as the scan key. Meanwhile, the vector, which is loaded into NSR and used to generate the scan key, is defined as the test authorization code.

Besides being connected to the NAND gate, the *Q* output (or its complement $\overline{Q}$) of each NSR cell is also connected with an OR gate GT2. After the test authorization code is entered into the NSR completely, the output of the OR gate G2 can be latched into the *D* flip-flop DF1. The clock signal *clk*_0 of DF1 is driven by the OR gate GT3, which is controlled by the system clock *CLK*. The other input of GT3 is connected to the carry output *Cout* of a module-*N* counter CT1. The clock signal *clk*_1 of the *D* flip-flop in NSR is driven by the output Q1 of DF1 and the system clock *CLK* through the AND gate GT1. The enable signal of CT1 is marked as *EN*, which is connected to the complement of the carry output signal *cout* through an AND gate GT4.

After the system reset or power-on, the module-*N* counter CT1 and DF1 will be initialized to zeros. The NSR is also initialized to all-zeros state.

In the test mode (*SE* = 1), when the output of the AND gate GT4 is high-level, *EN* port becomes high, and the module-*N* counter will be enabled. The module-*N* counter will start counting from zero. During this mode, test authorization code should be delivered first. When the correct test authorization code is entered completely, all the inputs of OR gate GT2 are "1" and the output of OR gate GT2 is "0," so *clk*_1 will be "0." Simultaneously, the counter reaches the maximum value of counting, so the carry output signal of CT1 becomes "1." Due to the "1" value of carry output signal, the *EN* input of CT1 turns low, leading CT1 into the hold mode. The *D* flip-flop DF1 is locked because *clk*_0 is equal to "1" consistently. During this period, Q1 = 0 and the output signal *clk*_1 of GT1 remains "0." At this time, the *D* flip-flop in the NSR is locked by the clock *clk*_1 and the correct test authorization code is stored in the NSR until it is initialized. Because one input of the XNOR gate between SFFs is "1," the scan data will not be affected and normal scan operations can be performed.

When the test authorization code is incorrect, that is, at least one bit is incorrect, the scan key will also be wrong. In this case, the output of the OR gate GT2 will be "1" after the module-*N* counter reaches the maximum value of counting. The "1" output of GT2 will be latched into DF1, the clock *clk*_0 of DF1 is disabled, and Q1 remains "1." Thus, the output clock *clk*_1 of GT1 will be active; that is, the shift operation in the NSR is enabled. The incorrect scan key will be shifted cyclically in NSR during the execution of the test operation. The shifted scan key will obfuscate the output of the scan chain through the XOR gate between SFFs. As a result, the attacker gets incorrect scan output, making the scan attack invalid.

As mentioned earlier, the test authorization code is determined by the combination of the values in the nonvolatile memory and the connection style between NSR and the scan chain. The following is an example of inferring the test authorization code. Take a 5-bit test authorization code as an example. Assume that the value in nonvolatile memory is 01101, and the initial state in NSR after initialization is 00000. The test authorization code X_5, X_4, X_3, X_2, X_1 is delivered in five clock cycle from right to left. As can be seen from Table 1, after one cycle, the state of NSR becomes $X_1$1001. Eventually, after five cycles, the state of NSR is X_5, $\overline{X_4}$, $\overline{X_3}$, $\overline{X_2}$, X_1. The connection style between the *D* flip-flops in the NSR and the inserted NAND gates is shown in Figure 2. Thus, the expected scan key should be 11001. That is, X_5, $\overline{X_4}$, $\overline{X_3}$, $\overline{X_2}$, X_1 should be consistent with 11001. The right test authorization code can be solved, i.e., X_5, X_4, X_3, X_2, $X_1 = 10111$.

2.3. Timing Analysis of Proposed Secure Scan Design. Assume that the state of the circuit before reset is unknown. The circuit is reset when the reset signal *RST* of the circuit changes from low to high. That is, all storage units are cleared to zero. In functional mode, *RST* is invalid and *SE* is low. In functional mode, NSR will not affect any operation of the circuit. Because the *clk*_1 is low, the NSR is disabled and the initial value of the NSR will not change. Low-level *SE* causes *EN* to be low. Based on this, the counter CT1 will not start counting, and the carry signal *cout* remains “0.” In summary, additional circuits will not work in functional mode.

In order to perform the test operation, *SE* should be set to “1,” while *clk*_1 is activated. The *N*-bit test authorization code can be entered serially into the NSR input port. At this point, the *EN* port of CT1 is activated and the counter starts counting from “00.” When the test authorization code is completely entered, the carry signal *cout* of CT1 turns “1.” The high value of *cout* makes the enable signal *EN* of CT1 turn to “0,” causing CT1 to be disabled. As described in Section 3, if the incorrect test authorization code is entered, the output Q1 of DF1 will be high due to the high output of GT2. The clock signal *clk*_1 of NSR is always consistent with CLK during test mode. The timing diagrams are illustrated in Figure 3. In this condition, incorrect test authorization code will shift bit by bit in the *D* flip-flop of NSR. That is, the scan data is the obfuscated data instead of the output data under scan test with correct test authorization code.

If the test authorization code entered is correct, the input of DF1 connected to the output of GT2 will be low. Because one input of GT1 is “0,” the clock signal *clk*_1 of the *D* flip-flop in the NSR will be disabled, and the correct test authorization code is stored in the NSR. The timing diagrams are illustrated in Figure 4. In this condition, the scan test can be implemented normally.

3. Results and Performance Analysis

3.1. Testability Analysis. The insertion of security design does not affect the original testability of the circuit. All commonly used testing techniques like stuck-at, and delay test can be applied. As long as the test authorization code is entered correctly, the normal scan operation can be performed, and the scan-out data will not be obfuscated.

Targeting at the stuck-at fault model, we do experiments on several big ITC′99 benchmark circuits including B17, B18, B19, B20, and B22. The results show, the fault coverage does not reduce for all these benchmark circuits with the same test set when the proposed secure scan design is integrated into them.

Since the added security design only adds logic gates, counters, and triggers, the faults occurring in the security scan design can be easily detected. When faults occur, although the test authorization code entered is correct, the output data will be still obfuscated. Then, the circuit will be treated as faulty one. Therefore, this does not affect the testability of the circuit.

3.2. Security Analysis. This section provides a detailed analysis of the security of the proposed structure by means of the following attack models.

3.2.1. Brute Force Attack. Since the test authorization code of the circuit is determined by the values in the nonvolatile memory and the way the NSR is connected with the scan chain, it is difficult to guess the test authorization code by brute force without obtaining specific design information about the circuit. The probability of randomly speculating the *L*-bit test authorization code to perform the scan test correctly is $(1/2)^L$. For $L = 64$, the probability of guessing the test authorization code is only 5.4×10^{-20}. In this case, it is impossible to obtain the test authorization code through brute force attack. In engineering applications, the attack probability and hardware overhead within the controllable range determine the value of *L*.

3.2.2. Differential Attack. Differential attack means that the attacker first runs in functional mode for several cycles and then switches to test mode to obtain an intermediate state [32]. Even if the attacker can dominate the scan chain through the primary input pins, the output data of scan chain will be obfuscated without the correct test authorization code. Therefore, the proposed secure scan structure can resist differential attack.

3.2.3. Test-Mode-Only Attack. Test-mode-only differential attack requires attackers to scan specific test vector pairs to obtain valuable information. However, in the proposed secure scan structure, these data will not be properly loaded into the scan chain due to the protection of obfuscation logic. In addition, incorrect keys can be cyclically shifted in the NSR during testing. Therefore, this leaves the obfuscated bits in an indeterminate state for each clock cycle while the scan operation is being performed. Therefore, the secure design proposed in this paper has the ability to resist test-mode-only attack.

Table 1: The state of example NSR.

0^{th}	0	0	0	0	0
1^{st}	X_1	1	0	0	1
2^{nd}	X_2	$\overline{X_1}$	1	0	1
3^{rd}	X_3	$\overline{X_2}$	$\overline{X_1}$	1	1
4^{th}	X_4	$\overline{X_3}$	$\overline{X_2}$	$\overline{X_1}$	0
5^{th}	X_5	$\overline{X_4}$	$\overline{X_3}$	$\overline{X_2}$	X_1
	1	1	0	0	1

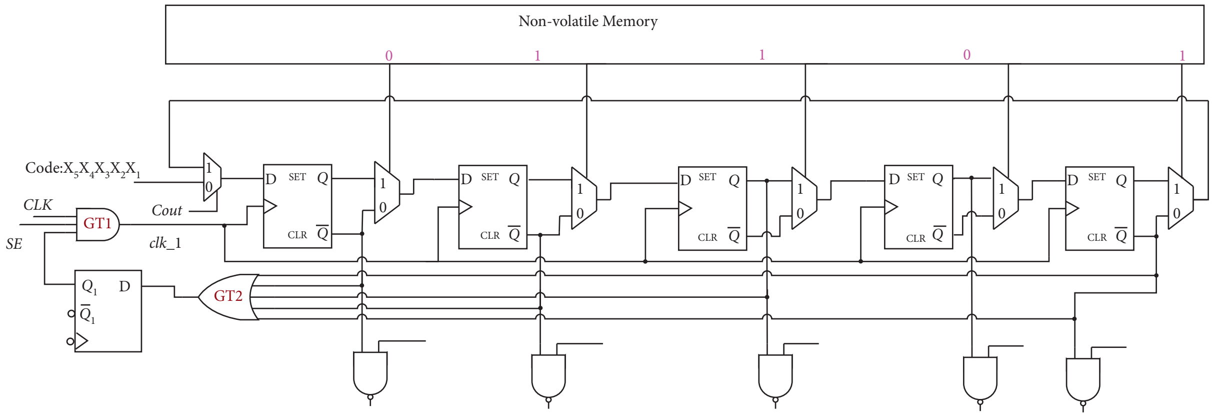

Figure 2: An example of inferring test authorization code.

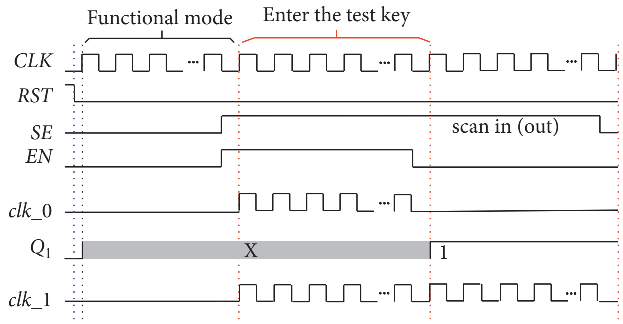

Figure 3: Timing diagram when the test authorization code is incorrect.

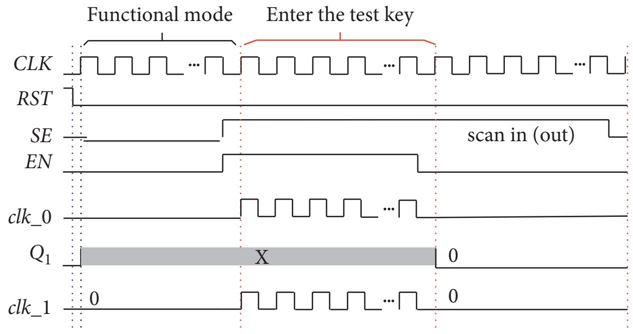

Figure 4: Timing diagram when the test authorization code is correct.

3.2.4. Resetting Attack. Resetting attack requires the attacker first resets the CUT, at which the state of all scan flip-flops is initialized to all-zeros. Then, the initial state is scanned with the given test authorization code. Finally, the attacker analyses the data from the scan-out result and determines whether the test authorization code is correct. However, the secure scan design proposed in this paper has obfuscation characteristics. When the test authorization code is not correct, the wrong scan key shifted in the NSR, and the scan-out data will also be obfuscated. Hence, inferring the test authorization code bit by

Table 2: Area without inserting security design.

Area categories	Area
Combinational area	288499.656516
Buf/Inv area	82048.231581
Noncombinational area	63713.608595
Macro/black box area	0.000000
Net interconnect area	1611937.031250
Total cell area	352213.265112
Total area	1964150.296362

Table 3: Power consumption without inserting encryption design.

Internal power	Switching power	Leakage power	Total power
288.8334 uw	9.4736e+04 uw	8.9739e+06 nw	1.0400e+05 uw

Table 4: Area overhead with inserting encryption design.

Area categories	Area
Combinational area	288683.274511
Buf/Inv area	82261.829572
Noncombinational area	63958.268591
Macro/black box area	0.000000
Net interconnect area	1615052.812500
Total cell area	352641.543102
Total area	1967694.355602

Table 5: Power consumption with inserting encryption design.

Internal power	Switching power	Leakage power	Total power
311.7226 uw	1.0020e+05 uw	8.9633e+06 nw	1.0948e+05 uw

Table 6: Comparison of different secure scan design. Note: LOC denotes "launch-on-capture."

Design	Area overhead (%)	Vulnerability	Probability of brute force	Test application
Proposed (64 bit authorization code)	0.18	None	2^{-64}(64 is the length of test authorization code)	All types of tests can be applied
MKR [30]	0.19	None	Brute force is inapplicable	Online testing cannot be applied
Mode reset [49]	~10	Test-mode-only attacks	Brute force is inapplicable	Online testing cannot be applied
Scan chain encryption [40]	2.92	Memory attack	2^{-m}(m is the length of test password)	All types of tests can be applied
FTSL-64 [59]	3.09	None	2^{-64}	Loc delay testing cannot be applied

bit from the scan-out data does not work. The proposed secure scan design can effectively resist the attacker using resetting attack to threaten the security of the circuit.

3.3. Overhead Analysis. In order to analyze area overhead, we perform experiments on AES circuit with Synopsys Design Compiler and Synopsys DFT Compiler. The area without the security design is shown in Table 2, and the power consumption is shown in Table 3.

The area and power consumption after inserting the proposed secure scan design with 64-bit test authorization code are shown in Tables 4 and 5. By comparing the total area and total power consumption, it can be seen that the overhead and power consumption after inserting encryption design are well within the acceptable range.

Through the above analysis, the proposed secure scan design has high security and testability, as well as low area overhead and power consumption.

3.4. Overheads and Performance Comparison of Different Countermeasures. The area overhead and performance of the proposed secure scan design are compared with other countermeasures, MKR [30], Mode reset [49], scan chain encryption [40], and so on. The characteristics of these countermeasures are shown in Table 6. It can be seen from the comparison that the proposed secure scan design has many advantages, such as low area overhead, unscathed testing applications, and high security.

4. Conclusion

In this paper, a secure scan design is proposed to defeat the scan-based side-channel attacks. The proposed design adopts encryption structure, which requires the correct test authorization code to carry out normal test operation. The test authorization code needs to be inferred from both the configuration bit of a nonlinear shift register and the connection style between the nonlinear shift register and the scan chain. The configuration bits are stored in a nonvolatile memory, which can be configured arbitrarily by IP owner and are inaccessible for users and attackers. The proposed structure performs well in testability and security, and its overhead and power consumption are within acceptable range.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by the Natural Science Foundation of Hunan Province under Grant nos. 2020JJ5604 and 2020JJ4622, the National Natural Science Foundation of China under Grant no. 61702052, and the Scientific Research Fund of Hunan Provincial Education Department under Grant no. 18A137.

References

[1] J. Wang, Y. Gao, W. Liu, A. K. Sangaiah, and H.-J. Kim, "An intelligent data gathering schema with data fusion supported for mobile sink in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 15, no. 3, 2019.

[2] B. Yin, S. Zhou, S. Zhang, K. Gu, and F. Yu, "On efficient processing of continuous reverse skyline queries in wireless sensor networks," *Ksii Transactions on Internet & Information Systems*, vol. 11, no. 4, pp. 1931–1953, 2017.

[3] J. Wang, Y. Gao, X. Yin, F. Li, and H. Kim, "An enhanced PEGASIS algorithm with mobile sink support for wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 9472075, 2018.

[4] 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.

[5] Y. Fei, 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, pp. 108–116, 2019.

[6] M. Long, Y. Chen, and F. Peng, "Simple and accurate analysis of BER performance for DCSK chaotic communication," *IEEE Communications Letters*, vol. 15, no. 11, pp. 1175–1177, 2011.

[7] Y. Fei, L. Gao, L. Liu, S. Qian, S. Cai, and Y. Song, "A 1 V, 0.53 ns, 59 μW current comparator using standard 0.18 μm CMOS technology," *Wireless Personal Communications*, vol. 111, pp. 843–851, 2020.

[8] Y. Fei, Q. Tang, W. Wang, and H. Wu, "A 2.7 GHz low-phase-noise LC-QVCO using the gate-modulated coupling technique," *Wireless Personal Communications*, vol. 86, no. 2, pp. 671–681, 2016.

[9] Q. Tang, K. Yang, D. Zhou, Y. Luo, and F. Yu, "A real-time dynamic pricing algorithm for smart grid with unstable energy providers and malicious users," *IEEE Internet of Things Journal*, vol. 3, no. 4, pp. 554–562, 2016.

[10] T. Qiang, M. Xie, K. Yang, Y. Luo, D. Zhou, and Y. Song, "A decision function based smart charging and discharging strategy for electric vehicle in smart grid," *Mobile Networks and Applications*, vol. 24, pp. 1722–1731, 2019.

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

[12] J. Wang, Y. Yang, J. Zhang, X. Yu, O. Alfarraj, and A. Tolba, "A data-aware remote procedure call method for big data systems," *Computer Systems Science and Engineering*, vol. 35, no. 6, pp. 523–532, 2020.

[13] 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.

[14] 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.

[15] M. Long, F. Peng, and H.-y. Li, "Separable reversible data hiding and encryption for HEVC video," *Journal of Real-Time Image Processing*, vol. 14, no. 1, pp. 171–182, 2018.

[16] 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*, pp. 1–14, 2021.

[17] W. Wang, X. Wang, J. Wang, N. N. Xiong, S. Cai, and P. Liu, "Ensuring Cryptography chips security by preventing scan-based side-channel attacks with improved DFT architecture," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, pp. 1–15, 2021.

[18] 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.

[19] X. He, Z. Wang, L. Qin, and D. Zhou, "Active fault-tolerant control for an Internet-based networked three-tank system," *IEEE Transactions on Control Systems Technology*, vol. 24, no. 6, pp. 2150–2157, 2016.

[20] Y.-Y. Wang, Y. Sun, C.-F. Chang, and Y. Hu, "Model-based fault detection and fault-tolerant control of SCR urea injection systems," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 6, pp. 4645–4654, 2016.

[21] H. Badihi, Y. Youmin Zhang, and H. Hong, "Wind turbine fault diagnosis and fault-tolerant torque load control against actuator faults," *IEEE Transactions on Control Systems Technology*, vol. 23, no. 4, pp. 1351–1372, 2015.

[22] I. Pomeranz, "On the computation of common test data for broadside and skewed-load tests," *IEEE Transactions on Computers*, vol. 61, no. 4, pp. 578–583, 2012.

[23] I. Pomeranz, "Multicycle tests with constant primary input vectors for increased fault coverage," *IEEE Trans. CAD Integrated Circuit Systtem*, vol. 31, no. 9, pp. 1428–1438, 2018.

[24] S. Zhang, K. R. Pattipati, Z. Hu, and X. Wen, "Optimal selection of imperfect tests for fault detection and isolation," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 43, no. 6, pp. 1370–1384, 2013.

[25] B. Yang, K. Wu, and R. Karri, "Scan based side channel attack on dedicated hardware implementations of data encryption standard," in *Proceedings of the International Test Conference*, pp. 339–344, Charlotte, NC, USA, October 2004.

[26] S. S. Ali, O. Sinanoglu, and R. Karri, "Test-mode-only scan attack using the boundary scan chain," in *Proceedings of the 19th IEEE Europe Test Symposium (ETS)*, pp. 1–6, Paderborn, Germany, May 2014.

[27] M. Tehranipoor and C. Wang, *Introduction to Hardware Security and Trust*, Springer, New York, NY, USA, 2011.

[28] J. Dworak and A. Crouch, "A call to action: securing IEEE 1687 and the need for an IEEE test security standard," in *Proceedings of the IEEE 33rd VLSI Test Symposium (VTS)*, pp. 1–4, Napa, CA, USA, April 2015.

[29] B. Yang, K. Wu, and R. Karri, "Scan based side channel attack on dedicated hardware implementations of data encryption standard," in *Proceedings of the International Conference Test*, pp. 339–344, Boston, MA, USA, October 2004.

[30] 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.

[31] R. Nara, K. Satoh, M. Yanagisawa, T. Ohtsuki, and N. Togawa, "Scan-based side-channel attack against RSA cryptosystems using scan signatures," *IEICE - Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E93-A, no. 12, pp. 2481–2489, 2010.

[32] J. D. Rolt, G. Di 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, 2013.

[33] A. A. Kamal and A. M. Youssef, "A scan-based side channel attack on the NTRUEncrypt cryptosystem," in *Proceedings of the 7th International Conference Availability, Reliability Security*, pp. 402–409, Prague, Czech Republic, August 2012.

[34] Y. Liu, K. Wu, and R. Karri, "Scan-based attacks on linear feedback shift register based stream ciphers," *ACM Transactions on Design Automation of Electronic Systems*, vol. 16, no. 2, 2011.

[35] J. Da Rolt, A. Das, G. Di Natale, M. L. Flottes, B. Rouzeyre, and I. Verbauwhede, "A scan-based attack on elliptic curve cryptosystems in presence of industrial design-for-testability structures," in *Proceedings of the IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems*, pp. 43–48, Austin, TX, USA, October 2012.

[36] J. Da Rolt, G. Di Natale, M. Flottes, and B. Rouzeyre, "New security threats against chips containing scan chain structures," in *Proceedings of the 2011 IEEE International Symposium on Hardware-Oriented Security and Trust*, p. 110, San Diego, CA, USA, June 2011.

[37] J. Da Rolt, G. Di Natale, M. Flottes, and B. Rouzeyre, "Are advanced DfT structures sufficient for preventing scan-attacks?" in *Proceedings of the 2012 IEEE 30th VLSI Test Symposium (VTS)*, pp. 246–251, Hyatt Maui, HI, USA, April 2012.

[38] 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 Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 34, no. 5, pp. 808–821, 2015.

[39] G.-M. Chiu and J. C.-M. Li, "A secure test wrapper design against internal and boundary scan attacks for embedded cores," *IEEE Transactions on Very Large Scale Integration Systems*, vol. 20, no. 1, pp. 126–134, 2012.

[40] M. Da Silva, M.-L. Flottes, G. Di Natale, and B. Rouzeyre, "Preventing scan attacks on secure circuits through scan chain encryption," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 38, no. 3, pp. 538–550, 2019.

[41] M. Da 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 *Proceedings of the 2017 22nd IEEE European Test Symposium (ETS)*, pp. 1–6, Limassol, Cyprus, May 2017.

[42] M. Da Silva, E. Valea, M. L. Flottes, S. Dupuis, G. Di Natale, and B. Rouzeyre, "A new secure stream cipher for scan chain encryption," in *Proceedings of the 2018 IEEE 3nd International Verification and Security Workshop (IVSW)*, Platja d'Aro, Spain, October 2018.

[43] P. Raiola, M. Kochte, A. Atteya et al., "Detecting and ResolvingSecurity violations in reconfigurable scan networks," in *Proceedings of the 2018 24th IEEE International Symposium on On-Line Testing and Robust Design (IOLTS)*, Platja d'Aro, Spain, October 2018.

[44] G. Sengar, D. Mukhopadhyay, and D. R. Chowdhury, "Secured flipped scan-chain model for crypto-architecture," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 26, no. 11, pp. 2080–2084, 2007.

[45] O. Novak, J. Jenicek, and M. Rozkovec, "Sequential test decompressors with fast variable wide spreading," in *Proceedings of the 19th IEEE Design Diagnostics Electron. Circuits System Symposium*, pp. 132–137, Kosice, Slovakia, April 2016.

[46] J.-H. Kang, N. A. Touba, and J.-S. Yang, "Reducing control bit overhead for X-masking/X-canceling hybrid architecture via pattern partitioning," in *Proceedings of the 53nd Design Automation Conference*, pp. 344–349, Austin, TX, USA, June 2016.

[47] J. Da Rolt, G. Di Natale, M.-L. Flottes, and B. Rouzeyre, "Scan attacks and countermeasures in presence of scan response compactors," in *Proceedings of the 16th IEEE European Test Symposium (ETS)*, pp. 19–24, Trondheim, Norway, May 2011.

[48] A. Das, B. Ege, S. Ghosh, L. Batina, and I. Verbauwhede, "Security analysis of industrial test compression schemes," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 32, no. 12, pp. 1966–1977, 2013.

[49] D. Hély, F. Bancel, M.-L. Flottes, and B. Rouzeyre, "Securing scan control in crypto chips," *Journal of Electronic Testing*, vol. 23, no. 5, pp. 457–464, 2007.

[50] W. Wang, J. 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.

[51] 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.

[52] Y. Atobe, Y. Shi, M. Yanagisawa, and N. Togawa, "Secure scan design with dynamically configurable connection," in *Proceedings of the 19th IEEE Pacific Rim International Symposium Dependable Computing (PRDC)*, pp. 256–262, Vancouver, Canada, December 2013.

[53] 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.

[54] Y. Atobe, Y. Shi, M. Yanagisawa, and N. Togawa, "Dynamically changeable secure scan architecture against scan-based side channel attack," in *Proceedings of the International SoC Design Conference*, pp. 155–158, Jeju Island, South Korea, November 2012.

[55] D. Zhang, M. He, X. Wang, and M. Tehranipoor, "Dynamically obfuscated scan for protecting IPs against scan-based attacks throughout supply chain," in *Proceedings of the 35th IEEE VLSI Test Symposium*, pp. 141–146, Las Vegas, NV, USA, April 2017.

[56] 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.

[57] H. Kodera, M. Yanagisawa, and N. Togawa, "Scan-based attack against DES cryptosystems using scan signatures," in *Proceedings of the IEEE Asia Pacific Conference Circuits System*, pp. 599–602, Kaohsiung, Taiwan, December 2012.

[58] 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. 12, no. 12, pp. 3229–3237, 2009.

[59] 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.

[60] U. Chandran and D. Zhao, "SSKTC a high-testability low-overhead scan architecture with multi-level security integration," in *Proceedings of the 27th IEEE VLSI Test Symposium (VTS)*, pp. 321–326, Santa Cruz, CA, USA, May 2009.

[61] M. A. Razzaq, V. Singh, and A. Singh, "SSTKR secure and testable scan design through test key randomization," in *Proceedings of the 20th IEEE Asian Test Symp. (ATS)*, pp. 60–65, New Delhi, India, November 2011.

[62] S. Paul, R. S. Chakraborty, and S. Bhunia, "VIm-scan: a low overhead scan design approach for protection of secret key in scan-based secure chips," in *Proceedings of the 25th IEEE VLSI Test Symposium*, pp. 455–460, Berkeley, CA, USA, May 2007.

[63] Y. Luo, A. Cui, G. Qu, and H. Li, "A new countermeasure against scan-based side-channel attacks," in *Proceedings of the IEEE International Symposium Circuits System (ISCAS)*, pp. 1722–1725, Montreal, Canada, May 2016.

[64] G. Sengar, D. Mukhopadhyay, and D. R. Chowdhury, "An efficient approach to develop secure scan tree for crypto-hardware," in *Proceedings of the International Conference Advanced Computer Communication (ADCOM)*, pp. 21–26, Guwahati, India, January 2007.

[65] Y. Atobe, S. Youhua, M. Yanagisawa, and N. Togawa, "State dependent scan flip-flop with key-based configuration against scan-based side-channel attack on RSA circuit," in *Proceedings of the Asia Pacific Conference Circuits System*, pp. 607–610, Kaohsiung, Taiwan, December 2012.

[66] S. Paul, R. S. Chakraborty, and S. Bhunia, "VIm-scan: a low overhead scan design approach for protection of secret key in scan-based secure chips," in *Proceedings of the 25th IEEE VLSI Test Symposium (VTS'07)VTS*, pp. 455–460, Berkeley, CA, USA, May 2007.

[67] L. Pierce and S. Tragoudas, "Enhanced secure architecture for joint action test group systems," *IEEE Transactions on Very Large Scale Integration Systems*, vol. 21, no. 7, pp. 1342–1345, 2013.

[68] R. Nara, N. Togawa, M. Yanagisawa, and T. Ohtsuki, "Scan-based attack against elliptic curve cryptosystems," in *Proceedings of the Asia South Pacific Design Automation Conference (ASP-DAC)*, pp. 407–412, Taipei, Taiwan, January 2010.

[69] M. Fujishiro, M. Yanagisawa, and N. Togawa, "Scan-based attack against Trivium stream cipher independent of scan structure," in *Proceedings of the IEEE 10th International Conference ASIC (ASICON)*, pp. 1–4, Shenzhen, China, October 2013.