JOURNAL OF SEMICONDUCTOR TECHNOLOGY AND SCIENCE, VOL. 23, NO. 4, AUGUST, 2023 ISSN(Print) 1598-1657
https://doi.org/10.5573/JSTS.2023.23.4.243 ISSN(Online) 2233-4866

A Lightweight Scan Architecture against the Scan-based Side-channel Attack

Xiangqi Wang[1], Xingxing Gong[1,2,*], Xianmin Pan[3], and Weizheng Wang[2,3]

Abstract—**The demand for cryptographic chips is growing rapidly in the market nowadays. Chips must undergo rigorous testing in order to promote quality. Scan-based design for testability (DFT) is widely used to improve the quality of testing. However, scan chain technology also provides illegal users with convenience. They can steal sensitive information of circuit under test (CUT) during testing, which seriously threatens the security of IP cores. Currently, researchers have proposed many secure strategies, but most of them affect the test quality or cause larger hardware overhead. In this paper, we propose a lightweight scan architecture against the scan-based side-channel attack. In this method, a number of logic gates, a linear feedback shift register (LFSR) and two corresponding counters are integrated into the design in order to ensure the security of the design. The normal scan operation can be performed only if users enter the correct scan input key at the *K* clock cycles. Otherwise, the scheme will incur scan obfuscation. Therefore, illegal users can only observe some incorrect responses from the scan output port. It is known from simulation results and theoretical analysis that the scheme is able to successfully defend against the scan-based side-channel attack while having extremely low overhead and high testability.**

Index Terms—**Cryptographic chips, DFT, scan-based attack, scan obfuscation**

I. INTRODUCTION

In recent years, while some new Internet technologies such as wireless sensor networks [1-3], big data [4, 5], Internet of Things [6, 7] and wireless communication [8, 9] have brought convenience to human life, they also expose various secure issues. For instance, personal information can be stolen by hackers for criminal activities and private electronic products can be maliciously controlled. Therefore, more and more people pay attention to personal privacy protection. At the same time, many researchers protect personal information from the underlying hardware [10].

With the expansion of application scenarios and market, the demand for semiconductor chips has grown substantially [11]. This also puts forward higher requirements for the integration and quality of the chip. Therefore, researchers have proposed the design for testability that implants the scan chain to IP cores at the design stage in order to improve the quality of chips, which makes manufacturing test and in-field testing easier. However, while providing controllability and observability, the scan design also provide convenience for attackers. An attacker can steal sensitive information inside the chip by the scan chain to take illegal control of the chip. The scan-based attack is an attack that probes the internal logic without removing the circuit package. This attack doesn't rely on any expensive equipment, so the attacker can execute the attack at a very low cost.

The purpose of attacking the chip is to obtain confidential information in the chip. The objectives of

Manuscript received Mar. 14, 2023; reviewed Jul. 24, 2023; accepted Aug. 1, 2023
[1]School of Mathematics and Statistics, Hunan First Normal University, Changsha 410138, China.
[2]School of Computer and Communication Engineering, Changsha University of Science & Technology, Changsha 410114, China
[3]College of Information Science and Engineering, Hunan Women's University, Changsha 410004, China
E-mail : xxG157610@163.com

the attack are as follows: 1) steal the key of the cryptographic chip]; 2) perform reverse analysis to extract the internal structure and function of the chip; 3) the attacker damages and controls the chip by shifting illegal data.

There are two main types of the scan-based side-channel attack: 1) the mode switching attacks; 2) the test-mode-only attack. The main process of recovering the key from the cryptographic chips through the scan chain is as follows: first, the attacker enters some known plaintexts, then the CUT will output some intermediate encryption results to the scan flip-flops (SFFs); the attacker gets some sensitive information by shifting these encryption results; finally, the attacker recovers the key by analyzing sensitive information.

Researchers have proposed many security measures to target this type of attacks. [12] proposed to protect the scan chain dynamically by adopting state-dependent scan flip-flop, but the design reduces the fault coverage of the test. The scan obfuscation structure was first proposed in [13], however, the structure induces routing overhead. The security of the scan architecture was improved by dividing the scan chain into smaller subchains evenly in [14]. This idea was also adopted by the authors in [15], who first divided a scan chain into several subchains, then used a controller to control the connection order of the subchains. However, Cui et al. [16] demonstrated that this design has security vulnerabilities and is vulnerable to the signature attack [17]. A partially secure scan architecture was proposed in [18], but this design makes it difficult for testers to observe and control the internal state of the CUT. To address this problem, Chen et al. [19] proposed a more advanced architecture that improves security mainly by removing the SFF containing sensitive information. Yang et al. [20] divided the CUT operation into secure mode and insecure mode. In secure mode, the encryption module can't enter the insecure mode to start the test, but it can operate normally. In insecure mode, the chips can be tested but can't move the key into the register. Hely et al. [21] protected the test mode by inserting a test controller into CUT. Although this countermeasure successfully prevents the mode-switching attack, they are vulnerable to the test-only mode attack. [22] introduces a dynamic scan chain reconfiguration technique that allows the recombination of scan chain connections during the testing process. This dynamic reconfiguration prevents attackers from deducing sensitive information based on observed scan chain connections. In [23], scan patterns/responses are decrypted/encrypted with highly efficient and secure block cipher at each scan port. Recently, secure schemes [24] based on physical unclonable function (PUF) [25-28] are widely researched.

In this paper, a lightweight scan design against the scan-based side-channel attack is proposed which provides high security and low overhead in order to protect the cryptographic chip from illegal attacks. In this approach, we introduce some logic gates, the LFSR and two counters to improve the security of the design. The scan input key determines whether the scheme can be executed properly during the test mode. If the user enters the incorrect scan input key, the scan design can't perform the normal test. The two counters are mainly utilized to control the whole implementation flow of scan design. The rest of this paper is as follows. Section II describes the proposed scan architecture in detail. Experimental results and theoretical analysis are presented in Section III. Finally, the paper is summarized in Section IV.

II. PROPOSED SECURE SCAN METHODOLOGY

1. Basic Idea of Proposed Secure Scan Design

The proposed secure scan architecture is shown in Fig. 1. Upon power-on, the whole circuitry is initialized to 0. Once the circuit is switched to the test mode (i.e., *SE* is set high), the user should shift the scan input key, In this scheme, the private key is not stored in the hardware, It is determined by the connection style (Q or $\overline{Q}$) between the scan chain and the LFSR. The SFFs associated with the key are randomly distributed in the scan chain. If the scan input key entered by the user is exactly correct, the LFSR which is controlled by the key can keep zero state and the scan chain is able to perform the scan operation normally. Otherwise, at the K^{th} cycle, the wrong scan input key will perturb the LFSR. If at least one LFSR cell receive 1 at the K^{th} cycle, some interference values will be generated in the LFSR from this moment on. Finally, these values are fed back to the scan chain. If the feedback value is 1, the scan chain will be obfuscated and can only perform the abnormal test. Therefore, the

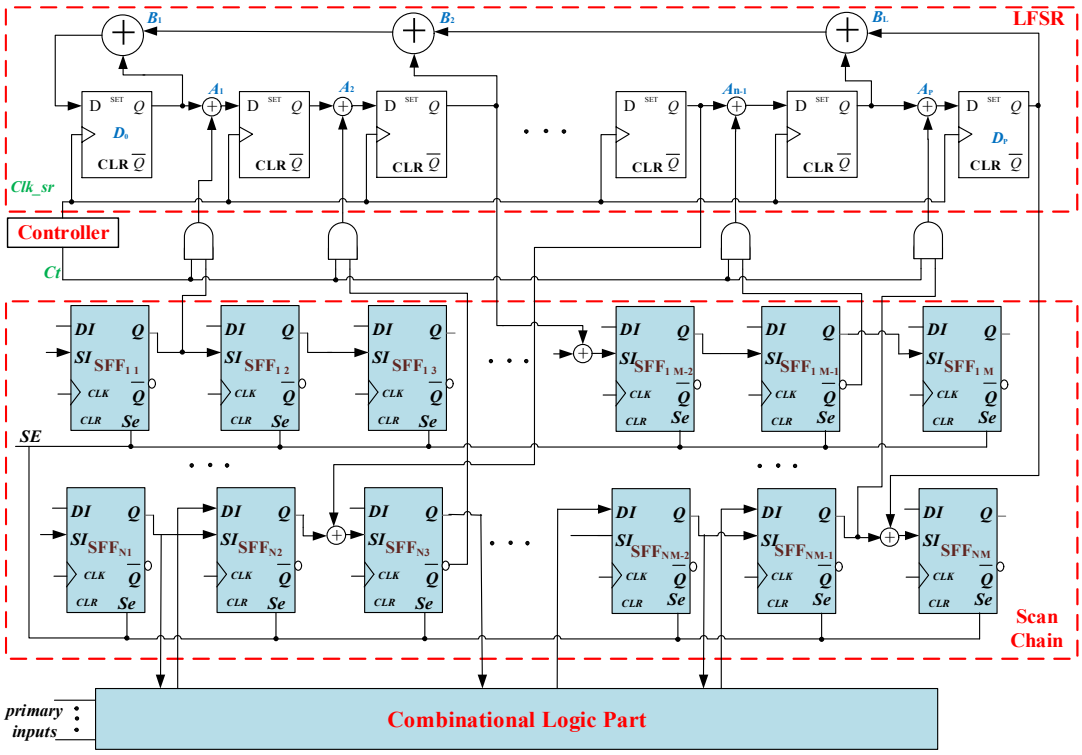

Fig. 1. Proposed secure scan scheme.

attacker can only observe the obfuscated data from the output port. Therefore, the secure scan design proposed in this paper is highly secure and has no impact on the testability of the chip. The secure scan architecture proposed in the next subsection will be discussed in detail.

2. Proposed Scan Scheme

Fig. 1 presents a security scan scheme, which is made up of some logic gates, LFSR and the Controller, with multiple scan chains as an example.

The data flip-flops in the circuit are replaced by the SFFs. In this paper, there are N rows and M columns of the SFFs in the scan chain. We select P SFFs from the scan chain as key storage cells. It is assumed that these P cells are randomly distributed from column 1 to column K ($1 \le K \le M$). Some XOR gates are randomly inserted between the SFFs. one input of XOR gates is connected to the Q or $\overline{Q}$ of previous SFF, the other input of which comes from the output of the D flip-flop in the LFSR. The LFSR is composed of some XOR gates and D flip-flops whose clock signal is controlled by the output *Clk_sr* of the Controller. The controller is formed by two counters and some logic gates. When the chip is switched to test mode, the counters start counting from 0. The output of the selected SFFs does not affect the LFSR for the first K-1 cycles because the output *Clk_sr* of the OR gate G3 locks the LFSR. In the K^{th} cycle, *Clk_sr* activates the LFSR and *Ct* also activates the selected SFFs. At this moment, if scan input key entered by the user is incorrect, the outputs of the selected SFFs interfere with the LFSR. *Ct* turns low and the effect of the selected SFFs on the LFSR is masked after the $(K+1)^{th}$ cycle, as shown in Fig. 2. One input of OR gate G3 in the Controller is connected to the system clock *CLK*. The output $\overline{Cout_1}$ of counter Counter1 is not only connected to the other input of OR gate G3, but also controls AND gate G1. The other input of G1 is controlled by the scan enable signal *SE*, and the enable signal EN_1 of Counter1 is driven by the output of AND gate G1. The XOR gate A_p is randomly inserted between the D flip-flops, one of its inputs comes from the output of the previous D flip-flop, the other input is connected to the output of the AND gate controlled by the *Ct* signal and output of the SFF together, the output of the XOR

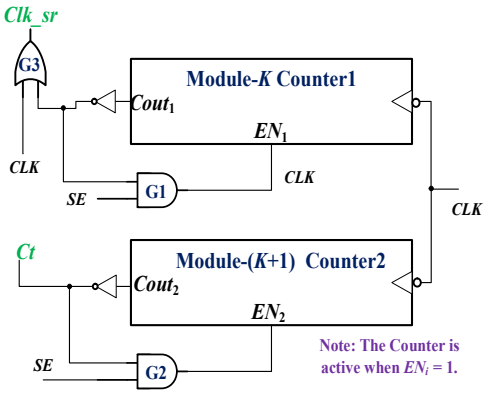

Fig. 2. The structure of the controller.

gate A_n is connected to the input port of the following D flip-flop. The signal *Ct* comes from the output $\overline{Cout_2}$ of counter Counter2. $\overline{Cout_2}$ and *SE* jointly control AND gate G2, and the output of G2 drives the enable signal EN_2 of Counter2. The clock signals of counters Counter1 and Counter2 are connected to the system clock *CLK*. As shown in Fig. 1, the XOR gate B_L ($L \geq 1$) is inserted in the external feedback path of the LFSR, one input of the remaining XOR gates $\{B_1.....B_{L-1}\}$ comes from the output of the D flip-flop and the other input is connected to the output of the following XOR gate except for the last XOR gate in the external feedback path. The XOR gate B_L is not randomly implanted but inserted according to the exponent of the characteristic polynomial:

$$G(x) = g_n x^n + g_{n-1} x^{n-1} + ... + g_3 x^3 + g_1 x^1 + g_0 .$$

Suppose $G(x) = x^4 + x^3 + x^1 + 1$, then a XOR gate will be inserted in the external feedback path of the first and the third D flip-flop.

Upon the system power on, the entire circuit is initialized to 0. First, *SE* are set to 1, so the circuit enters the test mode. The outputs of counters Counter1 and Counter2 enable signals EN_1 and EN_2, so both counters start counting from 0 and the user starts entering the scan input key, while the output of counter Counter1 causes the output *Clk_sr* of OR gate G3 to remain 1 for the first *K*-1 cycles and the output of counter2 causes *Ct* to remain 1 for the first k cycles. Counter Counter1 reaches its maximum value and the output *Clk_sr* of OR gate G3 is 0 at the K^{th} cycle, at the same time, Counter1 is disabled. At the $(K+1)^{th}$ cycle counter Counter2 reaches its maximum value and signal *Ct* is 0, at this time, Counter2 is disabled. In the first *K*-1 cycles, LFSR will be locked by signal *Clk_sr* and the value stored in the D flip-flop in LFSR will be 0. Therefore, the output of the AND gate will not disturb the value in the D flip-flop in LFSR. At the K^{th} cycle, the value stored in the D flip-flop from the LFSR starts to shift dynamically, however, *Ct* is still 1 at this time, then the output of the AND gate will be driven by the output of the SFF. If the entered scan input key is exactly correct, the low output of the selected SFFs causes the output of AND gate to be 0. Therefore, the selected SFFs can't affect the LFSR and this architecture can perform normal test. Otherwise, the output of some AND gates will be 1. It is assumed that the output *Q* of $SFF_{N,M-1}$ are 1, the output of the XOR gate A_p will be 1. The value 1 will be stored in D_p flip-flop at this moment. Then the output 1 of D_p is fed back to the XOR gates between the SFFs. The feedback value 1 will cause that $SFF_{N,M}$ receives the opposite value of the output of the previous SFF. At the $(K+1)^{th}$ cycle, the scan input key is completely shifted into the SFFs. Then, *SE* are set to 0, this scheme performs the encryption operation and the cryptographic key is returned to the SFFs. Finally, *SE* are set to 1, the cryptographic key is shifted out from the scan-out port.

The preceding analysis indicates that if the scan input key exists some error, the output of the SFFs will affect the values stored in the LFSR at the K^{th} cycle. These values affect the XOR gates between the SFFs at the corresponding time. Therefore, this architecture can perform the normal scan operation only if users enter the correct scan input key, otherwise, the illegal users can only observe some obfuscation values from the scan-out port.

3. Timing Analysis of Proposed Scheme

To describe more visually the operation flow of this design, Fig. 3 illustrates the timing analysis of the main signals in the proposed scheme. When the system is powered on and *RST* is 1, the whole circuitry is initialized to 0. When *RST* and *SE* are switched to 0, the circuitry enters the function mode. The counters are disabled since the outputs of two counters are 0 in functional mode. Therefore the additional circuitry does not work in the functional mode. When *SE* is 1, the

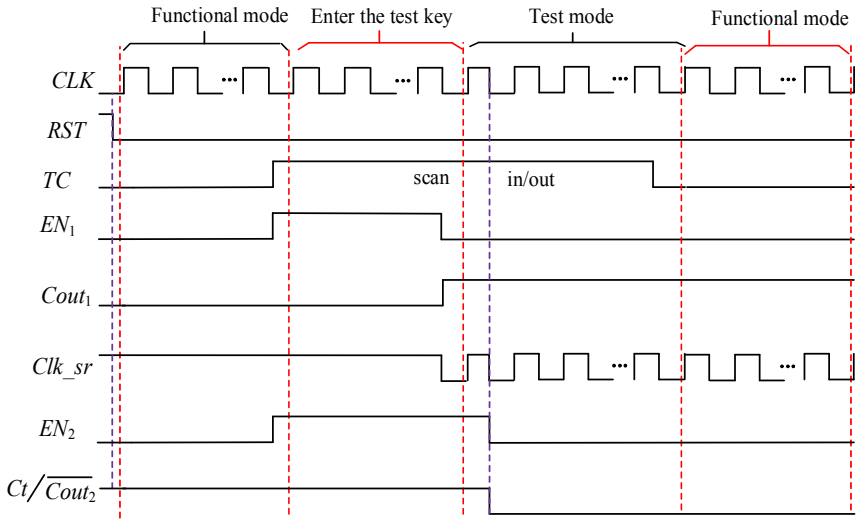

Fig. 3. Timing analysis of proposed scheme.

circuitry enters the test mode, both counters start counting and the user starts shifting the scan input key. *Clk_sr* remains 1 for the first *K*-1 cycles. *Clk_sr* is consistent with the system clock signal *CLK* until the K^{th} cycle. *Ct* remains 1 for the first *K* cycles. Counter2 reaches its maximum value until the $(K+1)^{th}$ cycle, at which point *Ct* remains 0. As long as the user enters the incorrect scan input key, the wrong key stored in the selected SFFs are loaded into the LFSR in the K^{th} cycle. At the meantime, these values are fed back to the scan chain. Therefore, it is impossible for illegal users to crack the internal logic of the chip.

III. Experiment Results and Analysis

We will evaluate our proposed scheme in terms of testability, security and performance overhead in this section.

1. Testability Analysis

In the proposed secure scan design, the insertion of some logic gates, counters and the LFSR does not affect the testability of the original circuitry. If some undetectable faults occur in this scheme, we can introduce BIST to test the inserted circuitry, so as to ensure a high fault coverage. The normal scan operation can be performed during the test as long as the engineer enters the correct scan input key.

2. Security Analysis

1) Brute force attack: In this scheme, the success rate of the brute force attack is associated with the scan input key. If the attacker does not enter correct key, thereby these values will affect the LFSR. The values in the LFSR influence the scan chain indirectly. Assuming that there are 10 D flip-flops in the LFSR, the LFSR can generate 1023 sets of responses. For an attacker, the probability of guessing the *L*-bit key is $(1/2)^L$. When the length *L* of the scan input key is 64, the probability of guessing the correct scan input key is only $5.4e^{-20}$. Therefore it is also difficult for an attacker to crack the scan input key.

2) Test mode only attack: Test mode only attack requires the attacker to load the pre-computed plaintexts, then all-0 or special test key are utilized to shift out the intermediate state in the scan chain to identify the SFFs. Due to the existence of some randomly inserted XOR gates between the SFFs, it is impossible to identify the SFFs through special test key. Therefore, the proposed scheme has good security against test mode only attack.

3. Overhead Analysis

To analyze the overhead, this paper use tsmc90nm technology to verify several benchmark circuits which includes AES-Pipelined, AES-Iterative, Vga-Lcd. We employed Synopsys Design Compiler and Synopsys DFT

Table 1. Synthesis results for the scan design and the secure design

Circuit Name	#SFF	Area (μm^2)		Power (μW)	
		Scan	Secure	Scan	Secure
Vga-Lcd	17071	922617	923692	198165	198619
AES-Iterative	1048	299267	300342	292655	293109
AES-Pipelined	10776	1977833	1978908	112225	112679

Table 2. The percentage of area and power overhead

Circuit Name	Area overhead (μm^2)	ΔA (%)	Power overhead (μW)	ΔP (%)
Vga-Lcd	1075	0.12	454	0.23
AES-Iterative	1075	0.36	454	0.15
AES-Pipelined	1075	0.05	454	0.40

Table 3. Comparison of different secure solutions

Design	Area overhead(%)	Security		Impact on testability	Impact on test time
		Vulnerability	Probability of brute attack		
Proposed	0.05	None	2^{-k}	Nil	k clock cycles before testing
MKR [20]	0.15	None	NA	Limited by inability to test secret-key registers	NA
Mode reset [21]	≈10	Test mode only attack	NA	Nil	NA
DFFs [22]	0.25	Bit-role identification attack	$C_{K_b}^{S_L * \# SC} * 2^{k_b}$	Nil	Multiple clock cycles before testing
Scan Chain Encryption [23]	2.92	Memory attack	2^{-k}	Nil	Multiple clocks for key decryption

Notes: k means the length of scan input key.

Compiler to synthesize the IP cores with the scan chain inserted and the IP cores with protection circuits inserted. As shown in Table 1, the first column represents three benchmark circuits, the second column shows the number of timing cells in each circuitry. Scan and Secure indicate the IP cores with multi-scan chains inserted and protection circuitry added, respectively. Table 2 presents the area and power overhead of the added protection circuitry and the percentage of the area and power overhead. The LFSR with the fixed size of 16 D flip-flops and the two counters with the size of 5 bits are implemented in this experiment respectively.

Table 3 compares proposed scheme with other schemes which include MKR [20], Mode reset [21], DFFs [22] and Scan Chain Encryption [23]. Compared to other secure schemes, the proposed secure scan design has a lower area overhead and improves security without affecting the functionality of the original circuitry. MKR [20] uses a secure test controller to manage the circuit, which has the following advantages: no test preparation time and high security. However, it can't test the secret key registers. Mode reset [21] causes high overhead and is vulnerable to the test mode only attack. The hardware overhead of DFFs [22] is more desirable, but which is vulnerable to bit-role identification attack. Scan chain encryption [23] has a high hardware overhead and is vulnerable to memory attack.

From the above analysis, it can be seen that this design has high security and low overhead without affecting the testability of the chip.

IV. CONCLUSIONS

In this paper, a lightweight scan architecture against the scan-based side-channel attack is proposed to protect the IP cores without sacrificing the testability. If the attackers enter the wrong scan input key, they can only acquire some obfuscation values from the scan-out port. Therefore, it is very difficult for them to decipher this architecture. Finally, the proposed scheme is verified on AES-Pipelined, AES-Iterative, Vga-Lcd and compared with other security countermeasures. The experimental results indicate that this design has a very low hardware overhead and this scheme is known to be highly security and testability from theoretical analysis.

ACKNOWLEDGMENTS

This work was supported in part by the Scientific Research Fund of Hunan Provincial Education Department under Grant no. 22A0686, and in part by the Natural Science Foundation of Hunan Province under Grant no. 2023JJ30316.

REFERENCES

[1] J. Wang, W. Chen, L. Wang et al., "Data secure storage mechanism of sensor networks based on blockchain," *Computers, Materials & Continua,* vol. 65, no. 3, pp. 2365-2384, 2020.

[2] J. Wang, Y. Gao, C. Zhou et al., "Optimal coverage multi-path scheduling scheme with multiple mobile sinks for wsns," *Computers, Materials & Continua,* vol. 62, no. 2, pp. 695-711, 2020.

[3] 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.

[4] J. Wang, Y. Yang, T. Wang et al., "Big data service architecture: a survey," *Journal of Internet Technology,* vol. 21, no. 2, pp. 393-405, 2020.

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

[6] 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.

[7] J. Zhang and G. Qu, "Physical Unclonable Function-Based Key Sharing via Machine Learning for IoT Security," in *IEEE Transactions on Industrial Electronics*, vol. 67, no. 8, pp. 7025-7033, Aug. 2020.

[8] F. Yu, L. Liu, L. Xiao, K. Li and S. Cai, "A robust and fixed-time zeroing neural dynamics for computing time-variant nonlinear equation using a novel nonlinear activation function," *Neuro-computing,* vol. 350, pp. 108-116, 2019.

[9] F. Yu, L. Gao, L. Liu, S. Qian, S. Cai et al., "A 1V, 0.53ns, 59μW current comparator using standard 0.18μm CMOS technology," *Wireless Personal Communications,* vol. 111, pp. 843-851, 2020.

[10] W. Z. Wang, Y. Chen, S. Cai and Y. Peng, "Preventing scan-based side-channel attacks by scan obfuscating with a configurable shift register," *Security and Communication Networks,* vol. 2021, no. 5222670, pp. 1-9, 2021.

[11] Shuo Cai, Yan Wen, Caicai Xie et al., "Low-power and high-speed SRAM cells for double-node-upset recovery," *Integration*, Vol. 91, pp. 1-9, 2023.

[12] 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.

[13] D. Hely, M. Flottes, F. Bancel et al., "Scan design and secure chip," in *Proc. Int. Line Test. Symp. (IOLTS)*, 2004, pp. 219-224.

[14] 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. 2007.

[15] Y. Atobe, Y. Shi, M. Yanagisawa et al., "Secure scan design with dynamically configurable connection," in *Proc. IEEE 19th Pacific Rim Int. Symp. Dependable Comput.*, Dec. 2013, pp. 256-262.

[16] 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.

[17] R. Nara, K. Satoh, M. Yanagisawa et al., "Scan-based side-channel attack against RSA cryptosystems using scan signatures," *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, vol. E93A, no. 12, pp. 2481-2489, 2010.

[18] M. Inoue, T. Y oneda, M. Hasegawa et al., "Partial scan approach for secret information protection," in *Proc. 14th IEEE Eur . Test Symp.*, May 2009, pp. 143-148.

[19] 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.

[20] 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.

[21] D. Hely, F. Bancel, M. L. Flottes et al., "Securing scan control in crypto chips," *Journal of Electronic Testing Theory & Applications*, vol. 23, no. 5, pp. 457-464, 2007.

[22] J. Lee, M. Tebranipoor, and J. Plusquellic, "A low-cost solution for protecting IPs against scan-based side-channel attacks," in *Proc. IEEE VLSI Test Symp. (VTS)*, Oct. 2006, p. 6-pp.

[23] M. Da Silva, M. l. Flottes, G. Di Natale et al., "Scan chain encryption for the test, diagnosis and debug of secure circuits," in *2017 22nd IEEE European Test Symposium*, Limassol, Cyprus, pp. 1-6, 2017.

[24] 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.

[25] J. Zhang, L. Ding, Z. Chen et al., "DA PUF: dual-state analog PUF," in *Proceedings of the 59th ACM/IEEE Design Automation Conference (DAC '22)*, New York, NY, USA, pp. 73-78, 2022.

[26] J. Shi, Y. Lu and J. Zhang, "Approximation Attacks on Strong PUFs," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 39, no. 10, pp. 2138-2151, Oct. 2020.

[27] J. Zhang, C. Shen, H. Su et al., "Voltage over-scaling-based lightweight authentication for IoT security," *IEEE Transactions on Computers*, vol.71, no. 2, pp. 323-336, 2021.

[28] Z. Chen, W. Lee, Q. Hong et al., "A Lightweight and Machine-Learning-Resistant PUF Using Obfuscation-Feedback-Shift-Register," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 69, no. 11, pp. 4543-4547, 2022.

Xiangqi Wang received the Ph.D. degree in Computational Mathematics from Hunan Normal University, Changsha, China in 2016. Since 2017, she has been an Assistant Professor with Hunan First Normal University, China. She was a visiting scholar at Peking University. Her current research interests include parallel computing, artificial intelligence security.

Xingxing Gong is a graduate student at College of Computer and Communication Engineering, Changsha University of Science & Technology. His research interests include design for testability and hardware security.

Xianmin Pan received the Master's degree in Electronic Technology from Zhongnan University of Economics and Law, Wuhan, China, in 2004. He is currently a Professor with the College of Information Science and Engineering, Hunan Women's University, Changsha, China. His research interests include artificial intelligence, data security.

Weizheng Wang received the B.S. degree in applied mathematics and the Ph.D. degree in computer application technology from Hunan University, Changsha, China, in 2005 and 2011, respectively. He is currently an Associate Professor with the School of Computer and Communication Engineering, Changsha University of Science & Technology, Changsha. His research interests include hardware security, artificial intelligence Security.