JOURNAL OF SEMICONDUCTOR TECHNOLOGY AND SCIENCE, VOL. 21, NO. 4, AUGUST, 2021 ISSN(Print) 1598-1657
https://doi.org/10.5573/JSTS.2021.21.4.247 ISSN(Online) 2233-4866

A Low-overhead Solution for Obfuscating Scan Data Against Scan-based Side-channel Attacks

Xiong Zheng[1], Zuoting Ning[2], Weizheng Wang[1,*], and Yan Peng[1]

***Abstract*—Scan-based design has been used normally to simplify the manufacturing test. However, the convenience brought by the design also becomes the weakness that increases the vulnerability of crypto chips. Many attacks have been proved effective to steal secret information stored inside chips through this structure. In this paper, we will propose a secure scan design with very low overhead and high security. The proposed scheme chooses some scan cells in the front part of the original scan chain to store the test key. The output of these scan cells will be transmitted to a multiple-input AND gate to realize authentication. If the input test key is incorrect, the data of the sub-chain in the front part of the scan chain will be shifted circularly and the values of those scan cells used to store the test key will be dynamically transmitted to the latter part of the scan chain to realize dynamic data obfuscation. The scheme excellently resists existing scan attacks.**

***Index Terms*—Scan design, noninvasive attack, crypto chips, low overhead**

I. INTRODUCTION

Some emerging technologies, such as wireless sensor networks and internet of things [1-5], have been developed quickly in recent years and their security has been seriously concerned. Simultaneously, the security issue of the underlying hardware has also received more and more attentions [6-9]. Scan-based design is one of the commonly used Design-for-Testability (DFT), which has significantly simplified the process of manufacturing test. However, due to its high controllability and observability, secret information inside chips may be stolen through this structure. Recently, the scan-based side-channel attacks have shown that attackers can analyze intermediate data to get important information inside chips through the scan design [10, 11]. Studies in [12-15] have shown that keys stored in chips with Advanced Encryption Standard (AES), RSA, Elliptic Curve Crypto systems (ECC) and Data Encryption Standard (DES) have been cracked successfully. To eliminate this potential crisis, many methods have been proposed.

A thorough way to defend against scan-based attacks is to cut off the polysilicon fuses after the test of the chip has been finished, which makes further access unavailable [16]. However, this significantly compromises the testability because the scan chain is also used to connect to an external five-pin joint test action group (JTAG) interface which makes it capable to debug infield [17]. BIST proposed in [18, 19] does not need users' test data and thus prevents attackers from accessing the secret key, but the fault coverage got compromised compared with the levels of scan test and ATPG.

Mirror Key Registers proposed in [14] is to isolate the key to an additional register to prevent it from entering the scan chain under test mode. Although simple and effective, the scheme considerably influences the test procedure. The method needs a separate test procedure in

Manuscript received Apr. 5, 2021; reviewed Jun. 20, 2021; accepted Jun. 23, 2021
[1]School of Computer and Communication Engineering, Changsha University of Science and Technology, Changsha 410114, China
[2]Department of Information Technology, Hunan Police Academy, Changsha 410138, China
E-mail : greaquer_w@yeah.net

which the large part related to the key is tested in secure mode while another small part independent of the key is tested in insecure mode. The large test cost in secure mode adversely affects the test time and coverage. Advanced industrial DFT structures, like decompressors and X-masking in [21] which are considered firmly secure against scan-based attacks [22], still have been attacked shown in [23].

Instead of directly preventing from accessing the key information, Virtually Impervious Scan (VIm-Scan) [20] uses an additional test key to realize the authentication before the data can be scanned out. It introduces a "pattern matching block" which stores a set of *M N*-bit test keys. Users must firstly input correct keys, otherwise the output will be all zeros. The main overhead of the scheme is dependent on the length and number of random test keys. The security of the scan design provided by this scheme relies on the probability of matching *M N*-bit test keys with input patterns loaded into the scan chain. The scheme can provide high security when *M*N* is enough large, but the scan-out data being all zeros when all test keys have not been matched may give attackers an obvious signal and there is no input restriction that allows attackers to wildly input. This may increase the possibility to crack the test keys.

In [25], the authors propose a solution of obfuscating scan data to prevent attackers from analyzing the output data. The unauthenticated users should also firstly input an *N*-bit additional test key. After the *N*-bit test key has been loaded into SR (an additional chain designed to store the test key), the input of SR will be locked. When the test key is not correct, *N* scan flip-flops (SFFs) of scan chain randomly selected will dynamically change their mode between normal and test, which may fail attackers to analyze from the output data. The overhead of the scheme will increase with the increase of the length of the test key. When the length of test key is short, the time used to crack the test key will also be short. The similar schemes based on data obfuscation are also presented in [24, 25, 32].

In this paper, we will propose a new solution for obfuscating scan data with higher security and lower overhead. The rest of the paper is organized as follows. In Section II, we present the proposed technique. In Section III, experimental results are presented to analyze the proposed scheme. In Section IV, we will discuss an improved scheme against certain attacks. We conclude in Section V.

II. Proposed Low-overhead Solution Against Scan Attacks

The proposed secure scan design uses test authorization mechanism to protect the chip. It makes full use of the scan chain itself to store the test authorization key, i.e, some scan cells in the scan chain are chosen to serve as test authorization key storage units. If the users can not load the correct test authorization key at the beginning of testing, then the test input data can no longer enter the scan chain while the test output data will also be confused. The proposed secure scan design requires very low overhead, which is the most significant advantage compared with the existing similar schemes.

The proposed secure scan design is shown in Fig. 1. It separates the scan chain into three parts. The first part is used to store test authorization key, the third part is used to obfuscate scan data and the second part is used to generate the end flag while completely inputting the test authorization key. The secure scan design introduces *N* NAND gates which are hard-wired with the Q or $\overline{Q}$ output of *N* randomly chosen scan flip-flops (marked as test key cells key[*i*]) among the first part of the scan chain. All the output of the *N* NAND gates are connected to a multiple-input AND gate G1, and the output of G1 is used as the clock signal of D1 which can lock the control signal *EN* to high level with a rising edge. The inverse of *EN* (i.e. $\overline{EN}$) is also wired to an input of each NAND gate. The value of key[*i*] ($1 \le i \le N$) is decided by the connection style, i.e, key[*i*]=0/1 if the Q /$\overline{Q}$ output is connected to the NAND gate. When the circuit is reset, *EN*=0 and $\overline{EN}$ =1. After the right test key is loaded, *EN* should become '1'. Otherwise, *EN* keeps zero. The output of *N* NAND gates are also connected to some AND gates randomly inserted among the third part of the chain to obfuscate scan data when the inputted test key is incorrect.

The *End_Flag* signal, which is the $\overline{Q}$ output of an SFF (named flag scan flip-flop) randomly selected among the second part of the chain, is used to judge whether the test key has been delivered completely.

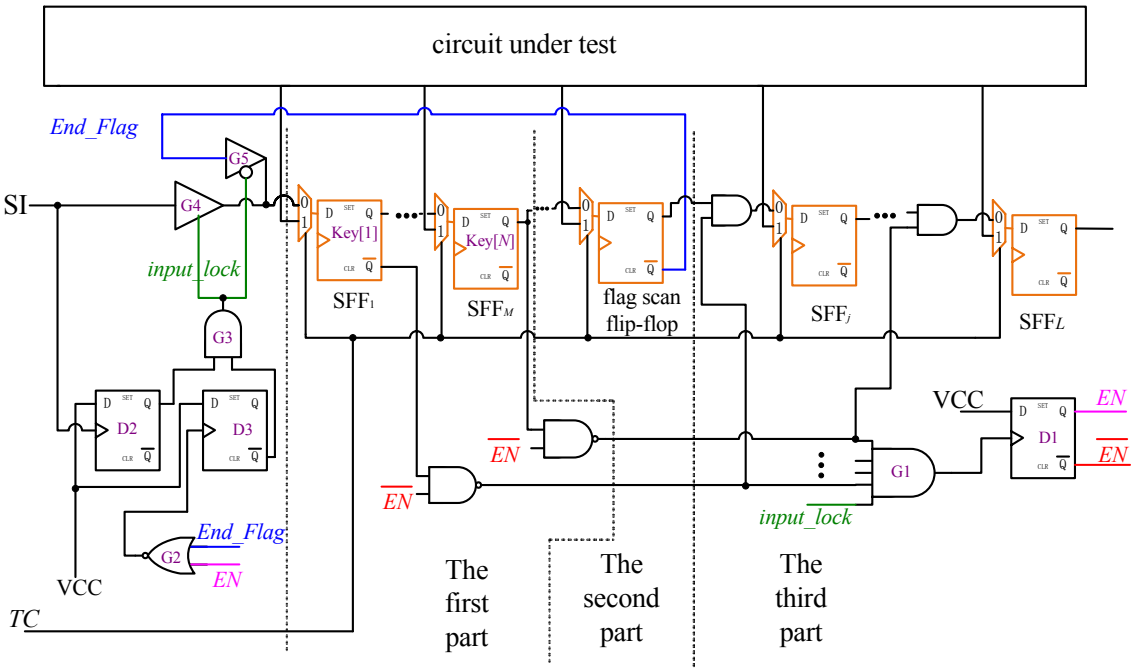


Fig. 1. Proposed scan design with low overhead for obfuscating scan data.

When the circuit is reset, *End_Flag*=1. Once the scan test starts, a transition from low level (‘0’) to high level must be sent via SI as Start Signal. As SI transitions from ‘0’ to ‘1’, the *Q* output of rising-edge flip-flop D2 becomes ‘1’. At this situation, *input_lock* signal (the output of AND gate G3) becomes ‘1’ since the $\overline{Q}$ output of D3 is 1 at the beginning. The tri-state buffer G4 is enabled, so the test key can be delivered. The test key should pass through the first part of the scan chain in which the authentication is performed.

When the Start Signal arrives in the flag scan flip-flop, *End_Flag* changes to low level (‘0’) which means the loading of the test key has been finished. Then the low-level value of *End_Flag* will be transmitted to the input restriction circuit between SI and the first SFF of the scan chain. If the loaded key is right, *EN* should be changed from ‘0’ to ‘1’ before the Start Signal has been transmitted to the flag scan flip-flop. In this case, the output of NOR gate G2 will remain low level (‘0’) although the value of End_Flag changes later. So, the clock of D3 will never be activated, and *input_lock* will keep ‘1’. Then the scan chain will always work normally. If the loaded test key is wrong, *EN* is still in low level (‘0’) when *End_Flag* changes to low level (‘0’). In this case, the output of NOR gate G2 will generate a transition from ‘0’ to ‘1’. So, the clock of D3 is activated, ‘1’ will be locked into D3, and *input_lock* will become ‘0’. The test data cannot be delivered from SI. The data of the first part of the chain will be shifted circularly to dynamically obfuscate the scan out data in the third part of the chain. Because the big AND gate G1 is also driven by *input_lock,* the test authorization key can be no longer checked for match after *input_lock* changes to ‘0’.

The timing diagrams of the signals during authentication process are shown in Fig. 2. *M* and *P* are the length of the first part of the scan chain and the location of flag SFF, respectively. In the figure we can see that *End_Flag*, *input_lock* and *EN* are initialized to ‘1’, ‘0’, and ‘0’, respectively. The first “0→1” transition inputted from SI causes *input_lock* signal becoming high level to enable the input from SI. After *M* clocks, if the inputted test key is right, the *EN* signal will change to high level and the *input_lock* will remain in high level. When the inputted test key is incorrect, the *EN* signal will remain in low level and the *input_lock* signal will change to low level to switch the input of the scan chain from SI to *End_Flag*.

Users who want to correctly input the test key should firstly send a high level to enable the tri-state gate G4 connected with SI, which will also finally become the end flag signal outputted from the flag scan flip-flop

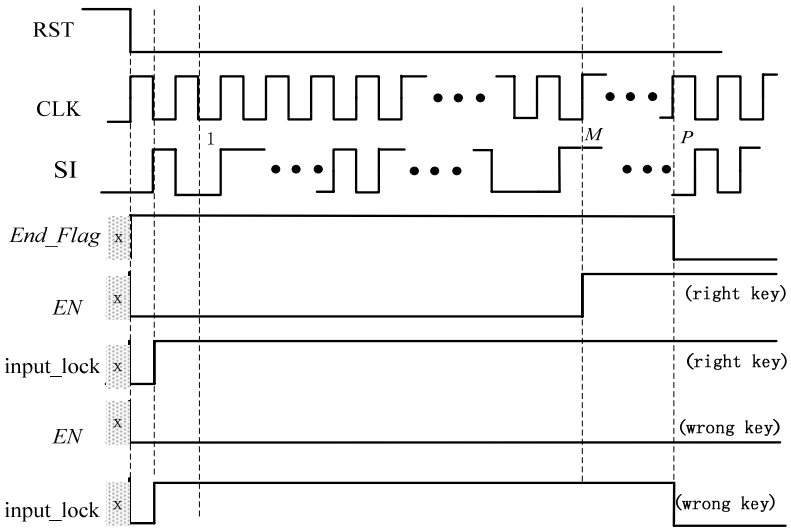


Fig. 2. Timing diagram of the signals in authentication operation.

mentioned above. Before *End_Flag* changes to low level, the right test key should be inputted. Otherwise, the SI of the chain will be locked and the data in the first part of the scan chain will be shifted circularly clock by clock. One input of the AND gate inserted in the third part of the chain is fed by a test key cell via a NAND gate. If the input is 0, the adjacent SFF can only receive zero. The scan-out obfuscation arises if the real value is '1'.

The proposed scheme just introduces the input restraint circuitry, a multiple-input AND gate and some NAND gates which brings slight impact on the chip implementation flow. Details will be discussed as follows. Because we just use some outputs of scan cells among the first part of the scan chain as signals to realize authentication, and insert some AND gates on scan path in the third part, there will be no impact to the design and layout of the original design. After the secure scan design insertion and placement, the tests will be performed by fab, assembly and other testers in supply chain. These authorized testers just need to input test patterns generated before and analyze the responses.

In addition, the proposed scheme can also be used to strengthen the security of the scan-tree in [33]. We can randomly choose a scan path in the tree to serve as the scan chain in Fig. 1. Once the test key is wrong, the input of the root node will be disabled and the data obfascation will occur at leaf nodes of the tree.

III. ANALYSIS AND RESULTS

In this section, We will analyze the testability, security and overhead of the proposed design. Then we will compare our design with some other countermeasures.

1. Analysis of Testability

Once the test key has been input correctly, the *EN* signal will be locked to "1" forever. The output of NAND gates of the first part of the scan chain will be all high levels and the obfuscation function of the third part of the chain will be no longer in force. The input of the scan chain will be stuck at SI forever. The scan chain will finally work normally which means test vectors and test responses will finally be inputted and outputted normally.

The circuitry introduced by the proposed design can not be tested and should not be testable. But it is easy to judge the correctness of this part of the circuitry by just loading the correct test key to see if the scan chain is working normally. If the output of the scan chain is incorrect when the correct test key has been inputted, the circuitry is wrong, otherwise the circuitry is correct.

2. Analysis of Security

Supposing that the length of the first part of the scan chain is M and the length of the test key is N(N <=

M),adversaries who know the exact number and position of the *N*-bit test keys should have $1/2^N$ probability to input the correct test key. However, if they don't know the details of the test key, the probability should be less than $1/2^N$ because the test key is randomly distributed in a longer scan chain. When N = 100 and M = 200, the probability will be less than 7.89e-31 and should be closer to 6.22e-61 depending on the randomness of the distribution of the test key. For the data in the scan chain having been shifted circularly in the first part and obfuscated in the third part, it should not be able to analyze the positions of certain SFFs through the output of the scan chain. As the input is blocked in the middle and the output will be changed in an unknown way before the correct test key has been inputted, any malicious data will finally be obfuscated into an unpredicted state and adversaries should not be able to build association between the input and output. Based on the advantages mentioned above, the scheme can excellently resist such attacks like differential attack [23], reset attack and test mode only differential attack [31], etc.

3. Analysis of Overhead

The proposed scheme, called LOOS (Low-Overhead Obfuscating Scan) for convenience, costs a very low overhead. The experiment is conducted on scan designs for pipelined [26] and iterative AES circuits with Key scheduling(KS) [27] and the result is shown in Table 1. The suffix 64 and 128 in column two are the length of the test key implemented. In column three, there are four sub-columns which respectively show the area cost of the original design, scan design, proposed security scan design and the increment of the proposed scheme compared to the scan design. We implemented the netlists of the original designs with Synopsys Design Compiler and added the scan chain by using Synopsys DFT Compiler. After that, we inserted the proposed part of the circuit into the netlists and then synthesized them with Synopsys Design Compiler. The costs of the area are represented by square micrometers (μm^2).

The additional part of the circuit is inserted in the scan path, rather than the functional path. Consequently, no timing overhead will be caused in the functional mode.

What's more, the proposed scheme is also compared with some other countermeasures which include MKR [14], mode-reset [28], SOSD [29], DOSD [25], DOS [32], PUF [24] and SDSFF [30] and the results are shown in Table 2. The test key of the proposed scheme can be placed in the first set of the test stimuli used in the normal test so there will be no extra time overhead used to realize authentication. While other countermeasures like SOSD [29] and DOSD [25] shown in the last column of Table 2 need extra time to input the test key before the normal test. In addition, the online test of MKR [14] scheme is not available though it is secure. In this case, the proposed scheme should be better. The area overhead is calculated by the standard as same as what is used in Table 1, typified by the pipelined AES core. We can see that the proposed scheme cost relatively low compared to other countermeasures in Table 2. The mode reset [28] countermeasure costs a lot but still being incapable to resist test-mode-only attacks. Although secure, SDSFF [30] is not practical for its inevitable defects. The scheme can't maintain the original fault coverage when any fault occurs in the circuit under test.

Table 1. Area overhead of the proposed scheme

AES	Scheme	Area(μm^2)				ΔA (%)
		original	scan	secure	ΔA	
Pipelined	LOOS-64	112332.9	116022.3	116116.0	93.7	0.08
	LOOS-128			116202.2	179.9	0.15
Iterative	LOOS-64	15856.3	16596.0	16689.8	93.8	0.56
	LOOS-128			16775.9	179.9	1.07

What's more, there are also some other ways to realize the protection, such as the secure JTAG proposed in [34]. However, the protection circuit in the proposed scheme is inside the chip, and it can achieve higher security because attackers can never bypass the protection circuit.

As mentioned above, the proposed scheme is better not only because it incurs low time and area overhead but also because it should be more secure than many existing countermeasures.

IV. An Improved Scheme Against Certain Attack

In some situations, adversaries may know the exact positions of critical registers in the scan chain. With the information of these positions, they can construct a specific set of sequences and analyze from the primary

Table 2. Comparison with some other countermeasures

design	area overhead (%)	Security		testability influence	test time influence
		vulnerability	key cracking probability		
LOOS-128	0.15	NONE	≤$1/2^{128}$, related to the key distribution range	NONE	NONE
MKR [14]	0.19	NONE	inapplicable	can not test secret key registers in test mode	Online test is not available
Mode reset [28]	~10	Test-mode-only attack	negligible	NONE	NA
SOSD-128 [29]	0.34	TMOSA	$1/2^{128}$	Nil	needing N clocks to input test key before normal test
DOSD-128 [25]	0.47	NONE	$1/2^{128}$	Nil	
PUF-128 [24]	3.80	NONE	$1/2^{128}$	Nil	
DOS [32]	2.01	memory attack	$1/2^{m*n}$	Nil	NA
SDSFF-100 [30]	0.25	NONE	$1/2^{5}$	Influenced by existing faults in the circuit under test	NA

Notes: *m* and *n* denotes the number of and the length of scan chains in [32].

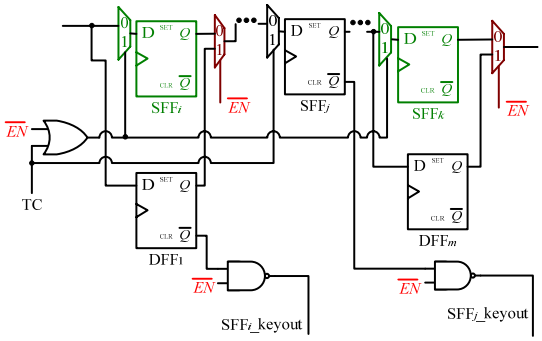


Fig. 3. Improved secure scan design against certain attack.

output response to steal secret information. As such attack is based on the knowledge of the positions of critical registers in the scan chain, with our design, such attack will take effect only when these critical registers are all distributed among the first part of the scan chain. To eliminate such potential crisis, we can use the structure shown in Fig. 3 in some critical registers to resist such attack. We use an OR gate with input of the inverse of *EN* and *TC* to lock some critical registers' mode to normal mode. When *EN* is in low level, the output of the OR gate should always be in high level. The inputs of these registers are bypassed by additional registers which can also be used as test key registers. When *EN* changes to high level, the output of these 2-to-1 multiplexers controlled by *EN* will change to the original SFFs' output and the scan chain will work normally.

These 2-to-1 multiplexers are located in the scan path. When the circuit is working normally, the additional logic will keep inactive because the signal will no longer go through these 2-to-1 multiplexers. Thus, no extra timing overhead is increased in the normal mode.

V. CONCLUSIONS

In this paper, we have illustrated a simple and effective scheme with very low overhead and enough security for obfuscating scan data against scan-based side-channel attacks in cypher chips. The method provides security by restricting the input and dynamically obfuscating scan-out data to prevent attackers from wildly inputting data and analyzing secret information from the output data. The proposed solution costs significantly low overhead compared to existing schemes and can easily improve the security by adding test key length with just some NAND gates.

ACKNOWLEDGEMENT

This work was supported in part by the Open Research Fund of Hunan Provincial Key Laboratory of Network Investigational Technology under Grant No. 2018WLZC002, the Natural Science Foundation of Hunan Province under Grant No. 2020JJ5604 and 2020JJ4622, the National Natural Science Foundation of China under grant No. 61702052, adn the Scientific Research Fund of Hunan Provincial Education Department under grant No.18A137.

REFERENCES

[1] 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, April 2019.

[2] J. Wang, Y. Gao, W. Liu,et al. "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, pp. 1-9, 2019.

[3] J. Wang, Y. Gao, X. Yin, et al., "An Enhanced PEGASIS Algorithm with Mobile Sink Support for Wireless Sensor Networks," *Wirel. Commun. Mob. Comput.*, vol. 2018, Article ID 9472075, 2018.

[4] W. Li, Z. Chen, X. Gao, et al. Multi-Model Framework for Indoor Localization under Mobile Edge Computing Environment. IEEE Internet Things J. 2019, 6, 4844-4853.

[5] J. Wang, Y. Gao,W. Liu, W. Wu, S.-J. Lim. "An Asynchronous Clustering and Mobile Data Gathering Schema based on Timer Mechanism in Wireless Sensor Networks," *CMC Comput. Mater. Contin*. 2019, 58, 711-725.

[6] J. L. Zhang, C. Shen, H. Su, M. T. Arafin, G. Qu, "Voltage Over-scaling-based Lightweight Authentication for IoT Security," *IEEE Transactions on Computers*, 2021, DOI: 10.1109/ TC.2021.3049543.

[7] 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 Cybernetics-Systems, 2020, doi: 10.1109/TSMC.2020.3036879.

[8] J. L. Zhang, W. Z. Wang, X. W. Wang, and Z. H. Xia, "Enhancing security of FPGA-based embedded systems with combinational logic binding," *J. Comput. Sci. Technol.*, vol. 32, no. 2, pp. 329-339, Mar. 2017.

[9] J. Zhang, 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, Aug. 2020.

[10] 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*. (*ETS*), Paderborn, Germany, 2014, pp. 1-6.

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

[12] B. Yang, K. Wu, and R. Karri, "Scan-based side-channel attack on dedicated hardware implementations of data encryption standard," *in Proc. Int. Test Conf.* (*ITC*), Washington, DC, USA, Oct. 2004, pp. 339-344.

[13] R. Nara, N. Togawa, M. Yanagisawa, and T. Ohtsuki, "Scan-based attack against elliptic curve cryptosystems," *in Proc. Asia South Pacific Design. Autom. Conf.* (*ASPDAC*), Taipei, Taiwan, Jan. 2010, pp. 407-412.

[14] B. Yang, K. Wu, and R. Karri, "Secure scan: A design-for-test architecture for Crypto chips," *IEEE Trans. Comput.-Aided Design Integr.*, vol. 25, no. 10, pp. 2287-2293, Oct. 2006.

[15] R. Nara, K. Satoh, M. Yanagisawa, and N. Togawa, "Scan-based side-channel attack against RSA cryptosystems using scan signatures," *IEICE Trans. Fundam. Electron., Commun. Comput. Sci*., vol. E93-A, no. 12, pp. 2481-2489, Dec. 2010.

[16] O. Kömmerling and M. G. Kuhn, "Design principles for tamper-resistant smartcard processors," *in Proc. USENIX Workshop Smartcard Technology*, Chicago, IL, May 1999, pp. 9-20.

[17] D. Josephson and S. Poehhnan, "Debug methodology for the McKinley processor," *in Proc. Int. Test Conf*., Baltimore, MD, 2001, pp. 451-460.

[18] Hafner et al, "Design and test of an integrated cryptochip," *IEEE Design and Test of Computers*, pp. 6-17, 1991.

[19] Zimmermann et al, "A 177 Mbit/s VLSI Implementation of the International data Encryption System," *IEEE Journal of Solid-State Circuits*, vol. 29, no. 3, Mar. 1994.

[20] 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 Proc. 25th IEEE VLSI Test Symp*., Berkeley, CA, USA, May 2007, pp. 455-460.

[21] T. Yu, A. Cui, M. Li, and A. Ivanov, "A new decompressor with ordered parallel scan design for reduction of test data and test time," *in Proc. IEEE Int. Symp. Circuits Syst.* (*ISCAS*), Lisbon, Portugal,

May 2015, pp. 641-644.

[22] C. Liu and Y. Huang, “Effects of embedded decompression and compaction architectures on side-channel attack resistance,” *in Proc. 25th IEEE VLSI Test Symp.* (*VTS*), Berkeley, CA, USA, May 2007, pp. 461-468.

[23] J. Da Rolt, G. Di Natale, M.-L. Flottes, and B. Rouzeyre, “A novel differential scan attack on advanced DFT structures,” *ACM Trans. Design. Autom. Electron. Syst.*, vol. 18, no. 4, Oct. 2013, Art. no. 58.

[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,* doi: 10.1109/TETC.2019.2903387.

[25] A. Cui, Y. Luo and C. 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, Feb. 2017, doi: 10.1109/TIFS.2016.2613847.

[26] (Oct. 2014). AES: Overview. [Online]. Available: http://opencores.org/project,tiny_aes

[27] I. Verbauwhede, P. Schaumont, and H. Kuo, “Design and performance testing of a 2.29-GB/s Rijndael processor,” *IEEE J. Solid-State Circuits*, vol. 38, no. 3, pp. 569-572, Mar. 2003.

[28] D. Hely, F. Bancel, M.-L. Flottes, and B. Rouzeyre, “Test control for secure scan designs,” *in Proc. Eur. Test Symp.* (ETS), Tallinn, Estonia, May 2005, pp. 190-195.

[29] Y. Luo, A. Cui, G. Qu and H. Li, “A new countermeasure against scan┐based side-channel attacks,” *in Proc. 2016 IEEE Int. Symp. Cir. Syst.*, Montreal, Canada, May 2016, pp. 1722-1725.

[30] 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. Circuit. Syst.* (*APCCAS*), Kaohsiung, Taiwan, Dec. 2012, pp. 607-610.

[31] 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.* (*VLSI SoC*), 2013, pp. 234-239.

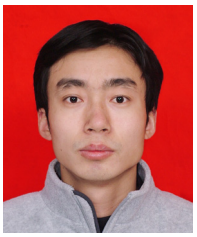
[32] X. Wang, D. Zhang, M. He, D. Su and M. Tehranipoor, "Secure Scan and Test Using Obfuscation Throughout Supply Chain," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 37, no. 9, pp. 1867-1880, Sept. 2018.

[33] D. Xiang, K. Li, J. Sun and H. Fujiwara, "Reconfigured Scan Forest for Test Application Cost, Test Data Volume, and Test Power Reduction," *IEEE Transactions on Computers*, 2007, vol. 56, no. 4, pp. 557-562.

[34] Park, K., Yoo, S.G., Kim, T. et al. “JTAG Security System Based on Credentials,” *Journal of Electronic Testing*, 2010, vol. 26, no. 5, pp. 549-557.

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

Zuoting Ning received the Ph.D. degree of computer science from Hunan University in 2017, He is a lecturer in Hunan Police Academy. His research inerests include machine learning, network security and hardware security.



Weizheng Wang received the Ph.D. degree in computer application technology from Hunan University in 2011. He is currently an associate professor in Changsha University of Science and Technology, Changsha. His research interests include hardware security, design for testability, and artificial intelligence security.

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