Shatterproof Secure Scan Design against Scan-Based Side Channel Attacks

Basil Varghese and Meera Thampy

Abstract*— *Scan test is a powerful and popular test technique because it can control and observe the internal states. However, scan path would be used to discover the internals of crypto hardware, which presents a significant security risk of information leakage. An interesting robust secure scan design technique by inserting inverter and XOR gates into the internal scan path to complicate the scan structure has been recently presented. Unfortunately, it still carries the potential of being attacked through differential cryptanalysis of the information scanned out from chips. Therefore, in this paper we propose secure scan architecture, called SSS design. By using the SSS design into the chip, testing and accessing scan chains are guaranteed to be allowed only by an authorized user. The proposed technique has a negligible area overhead, has no negative impact on chip performance and places several levels of security over the scan chain protecting it from potential attacks. The modified scan design makes it more difficult to discover the internal scan architecture.

Keywords*— *Shatter Proof Secure Scan Flip-Flop (SSSF), Shatter proof Secure Scan (SSS), Scan Based Side Channel Attack (SSCA), Scan Flip-Flop (SSF), Robust Secure Scan Flip-Flop (RSSF)

I. INTRODUCTION

SCAN based test is a double edged sword. On one hand, it is a powerful test technique. On the other hand, it is an equally powerfu1 attack tool. In the modern era, security of crypto-chips is a major concern. Currently, all communication, networking, database management systems and financial application use cryptographic methods. The possibility of scan-based side-channel attacks adds to an already growing customer concern of hardware security. Fundamentally, the problem lies on the inherent contradiction between testability and security for digital circuits. Hence, there's a need for an efficient solution such that both testability and security are satisfied.Scan chains are one of the most popular methods to test hardware's. In this scheme all flip flops (FFs) are connected in a chain and the state of the FFs can be scanned out through the chain. Scan testing equips a user with two very powerful features namely controllability and observability. Controllability refers to the fact that the user can set the FFs to a desired state, while observability refers to the power to observe the content of the FFs. These two features used as a means to breach chip security**.**

Scan test has been widely adopted as a default testing technique among most VLSI designs, including crypto cores. Unfortunately, these scan chains might be used as a side channel to recover the secret keys from the hardware implementations of cryptographic algorithms, for example scan-based attacks on Data Encryption Standard(DES), Advanced Encryption Standard (AES), and Elliptic Curve Cryptography (ECC) have been illustrated in [2]–[4], respectively. In general, the existing scan-based side channel attacks (SSCA) could be viewed as one kind of differential cryptanalysis by using scan chains of crypto cores. Unlike other known side channel attacks, SSCA is much easier. It is because that in SSCA, in addition to the primary outputs of the crypto cores, a hacker could use scan chain to shift out the intermediate contents during a cryptographic operation. It was illustrated in [3] that on average overall only 544 plaintexts are required to discover the AES key by using SSCA, which clearly shows the great potential threat of scan-based side channel attack.

Scan chain based attacks are a kind of side channel attack, which targets one of the most important features of today's hardware - the test circuitry. In cryptography, a side channel attack is any attack based on information gained from the physical implementation of a cryptosystem, rather than brute force or theoretical weaknesses in the algorithms. For example, power consumption, timing information, electromagnetic leaks or even sound can provide an extra source of information which can be exploited to break the system. The existing scan-based attacks could be viewed as one kind of differential cryptanalysis, which takes advantages of scan chains to observe the bit changes between pairs of chosen plaintexts so as to identify the secret keys.

A robust secure scan (RSS) is proposed in previous paper is shown in Fig. 1, in which a new kind of scan flip-flop, called robust secure scan flip-flop (RSSF)[1], is introduced from a security aspect. The basic idea of the RSS design is to encrypt the contents in scan chains during scan operation, so as to reduce the controllability and observability of unintended users. By including such RSSFs into crypto cores, all the advantages and simplicity of traditional scan test are preserved, and the security is significantly improved with ignorable design and test overhead.

Basil Varghese, M.Tech, VLSI & Embedded Systems, Sree Narayana Gurukulam College of Engineering, Kadayiruppu, Kolenchery. E-mail: basilbss@gmail.com

Meera Thampy, Asst.Professor, Department of Electronics and Communication, Sree Narayana Gurukulam College of Engineering, Kadayiruppu, Kolenchery. E-mail: meera9584@gmail.com

ISBN 978-93-82338-83-3 © 2013 Bonfring

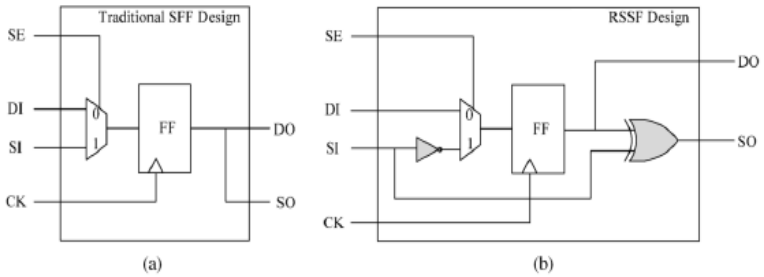

Fig: 1: RSSF versus traditional SFF. (a) Traditional SFF. (b) RSSF

The RSSF scan structure still has the security threat on reset based attack, which is because the proposed test method works like a static scan structure when the CUT is reset. It might be possible for hackers to discover the scan structure so as to infer the RSSF positions by iterating the operations as reset apply plaintext/ scan-in and scan out. To address such a design/test challenge, this paper proposes a shatterproof secure scan structure design for crypto cores as a countermeasure against scan-based attacks to maintain high security without compromising the testability with ignorable design and test overhead.

The rest of this paper is organized as follows. Section II presents the proposed Shatterproof Secure Scan Design. In Section III, detailed analysis on implementation overhead and security performance are given. Section IV concludes this paper.

II. SHATTER PROOF SECURE SCAN DESIGN

Due to the security and testability requirements as mentioned above, a novel shatterproof secure scan-based test approach is proposed as a countermeasure against scan-based side channel attack.

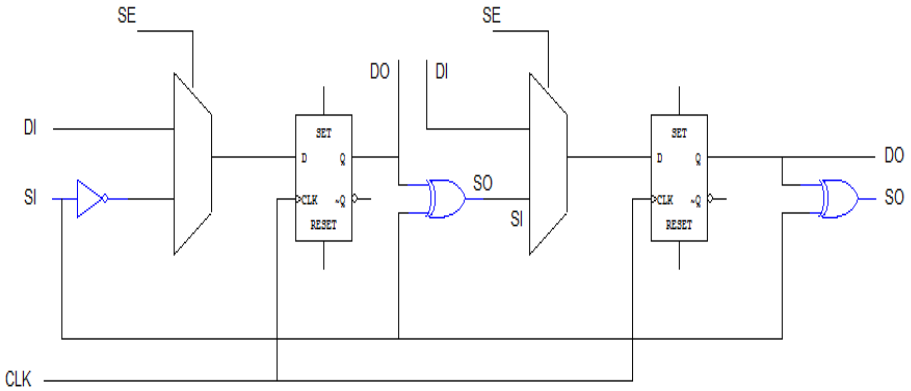

Fig. 2: Proposed SSSF design

A. *SSS Design*

The proposed shatterproof secure scan design is used in two scanning block of a combinational circuit have one SSSF. Conventional scanning flip flops are used in single block and it quit easy to identifying the output of the block then hackers have trace out the internal structure and functions of that block but in the SSSF it very hard and somewhat impossible. During the scanning process basically, all FFs in the design are replaced with scan type FFs. It makes all FFs in the design controllable and observable by chaining them together and shifting test data in and out. Scan type FF contains a MUX to select either a normal mode data DI or a scan data SI. SE is a control input. The first step is to put a circuit into a scan mode. The whole chip is divided into parts (scan chains). Serial data is applied to the input of every chain and getting shifted between FFs to the outputs. Every scan chain output is tested for the proper data coming out.

The basic idea of the proposed SSS design is to encrypt the contents in scan chains during scan operation, so as to reduce the controllability and observability of unintended users. By doing this, it becomes more complicated for hackers to identify the bit differences between pairs of related plaintexts when they are encrypted under the same key. One kind of the proposed SSS design is shown in Fig.2, in which the contents of two neighboring SFFs [6], [7] are encoded during scan operation from a security aspect. When compared with the traditional SFF, an extra inverter and an XOR gate are introduced in the SSS design. This simple logic could be used for encryption during scan operations. The additional inverter and the XOR gate are inserted along the scan path; they do not affect the timing of the design. Thus in function mode, SSSF works like a traditional scan flip-flop. Observe that the proposed shatterproof secure scan flip-flop (SSSF) has identical pin outs when compared with the traditional scan flip-flop as shown in Fig.2, and is therefore fully compatible with industry standard design tools from a design perspective,

ISBN 978-93-82338-83-3 © 2013 Bonfring

when integrated into current design flows it only requires the SSSF added into the cell library.

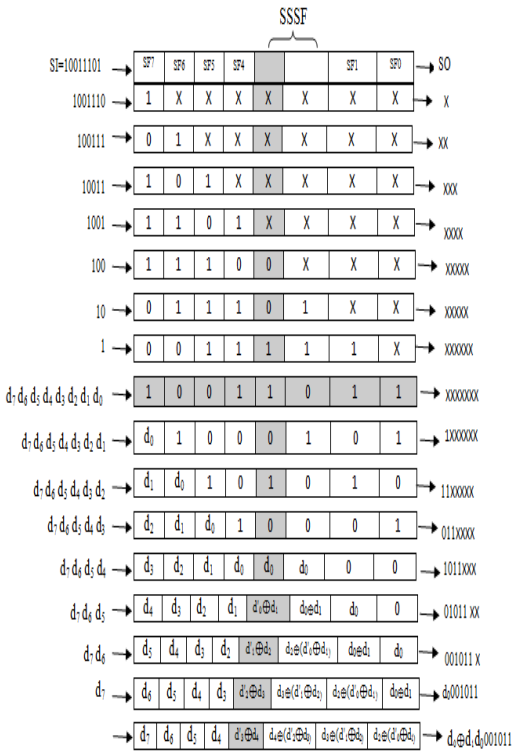

Fig. 3: Operation of SSSF

An example to illustrate the operations of SSSF is shown in Fig.3, where the original SFF (SFF3 and SFF4) is replaced by an SSSF and the scan chain contains eight scan flip-flops. As a result, during scan in/out, the data that passes SSSF would be encoded. Thus for hackers, it becomes extremely complicated to identify the relationship between the captured response and the scan-out.

The procedure for circuit testing:

1. Set c =1 to switch the circuit to shift register mode
2. Check operation as a shift register by using scan-in inputs, scan-out output and the clock
3. Set the initial state of the shift register
4. Set c = 0 to return to normal mode
5. Apply test input pattern to the combinational logic
6. Set c=1 to return to shift register mode
7. Shift out the final state while setting the starting state for the next test
8. Go to step 4.

In order to carry out scan-based attacks on crypto hardware implementations, one needs to ascertain the internal scan structure. Using the proposed RSSF design, the task of determining the scan structure becomes computationally infeasible. Simply consider that a scan chain has *n* SFFs and one SFF is replaced by SSSF, so according to (1) and (2), the probability to guess the correct structure by an attacker is $1/2^{n+2}$, which is because the final observable scan-outs depend not only on the contents in the *n* SFFs but also on the first scan-in.

III. Implementation and Analysis Security

In this section, security analysis and implementation overhead are discussed to show the advantages of the proposed secure test technique over existing methods.

A. Implementation Analysis

One of the reasons to replace the original SFF with the proposed SSSF is that scan data should be encrypted to prevent secret leakage so that:

1) The applied test vector from external should not be the same as the real test vector and

2) The real captured response must be different from the data that is scanned out and could be observed at external.

The second reason is that, for pairs of responses, the Hamming distances between the scan-outs should not always be the same as those between the original responses. In traditional scan, the Hamming distances for responses and scan-outs are always the same, which might be used by the hacker to guess the secret key. It is because due to the avalanche effect of cryptographic algorithms, by observing the scan-outs of some specific pairs of plaintexts it becomes possible to guess the secret key. Consider the case that there is a scan chain which contains two scan flip-flops (SFF1 and SFF0). Assume that the captured responses in these two SFFs are R1 and R0. Thus in traditional scan structure, R1 and R0 will be shifted out, and the Hamming distances between two responses could be observed and compared. In traditional scan, the Hamming distances for responses and scan-outs are always the same, which might be used by the hacker to guess the secret key. It is because due to the avalanche effect of cryptographic algorithms, by observing the scan-outs of some specific pairs of plaintexts it becomes possible to guess the secret key

Table I: Observable Hamming Distances between Pairs of Responses Using Tradition Scan Structure

Response				Scan Out			
R3	R2	R1	R0	R3	R2	R1	R0
0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	1
0	0	1	0	0	0	1	0
0	0	1	1	0	0	1	1
0	1	0	0	0	1	0	0
0	1	0	1	0	1	0	1
0	1	1	0	0	1	1	0
0	1	1	1	0	1	1	1
1	0	0	0	1	0	0	0
1	0	0	1	1	0	0	1
1	0	1	0	1	0	1	0
1	0	1	1	1	0	1	1
1	1	0	0	1	1	0	0
1	1	0	1	1	1	0	1
1	1	1	0	1	1	1	0
1	1	1	1	1	1	1	1

The proposed SSSF design could deal with such an issue to make it more complicate for the hackers to guess the key. Tables I and II show the observable Hamming distances between pairs of responses using the traditional scan and the proposed SSS structure, respectively, where we assume there is a scan chain that contains four SFFs and in SSS the last SFF (SFF1 and SSF0) is replaced by the proposed SSSF.

ISBN 978-93-82338-83-3 © 2013 Bonfring

Table II: Observable Hamming Distances between Pairs of Responses Using The Proposed SSS Structure

Response				Scan Out			
R3	R2	R1	R0	R3	R2	R1	R0
0	0	0	0	1	1	1	1
0	0	0	1	1	1	1	0
0	0	1	0	1	1	0	0
0	0	1	1	1	1	0	1
0	1	0	0	1	0	0	0
0	1	0	1	1	0	0	1
0	1	1	0	1	0	1	1
0	1	1	1	1	0	1	0
1	0	0	0	0	0	0	1
1	0	0	1	0	0	0	0
1	0	1	0	0	0	1	0
1	0	1	1	0	0	1	1
1	1	0	0	0	1	1	0
1	1	0	1	0	1	1	1
1	1	1	0	0	1	0	1
1	1	1	1	0	1	0	0

From the two tables, it could be observed that the Hamming distances of 80 out of 136 pairs are changed, and for the unchanged 56 pairs the positions of different bits are changed in 29 pairs. In other words, there are only 27 pairs in which the Hamming distances and the different bit positions are the same as those using the traditional scan structure. It should be mentioned that in this work the basic idea of SSS is to encrypt the scan data by considering the relationship of two neighbouring scan data. In general, two factors should be considered when designing such an SSSF:

1) It is desired that the resulted Hamming distances should be unpredictable when compared with those in normal scan and

2) The implementation of SSSF should not induce any test problems.

B. Security Analysis

Due to the avalanche effect of cryptographic algorithms, there exist two kinds of scan-based differential cryptanalysis, called as constant based (CBA) [5] and fixed-hamming-distance-based attack (FHDA) [2]. Here let us use AES as an example cryptographic algorithm to explain these two kinds of attacks.

CBA takes advantages of the fact that in encryption process, the contents of some special registers are independent on the inputted plaintext. For example, the round registers in AES, without special protection, for each normal inputs, in the first cycle they would be 0001, and then 0010, _ _ _, 1010. By using several different plaintext inputs and scanning out the contents at different times of the cryptographic operation, these registers could be easily identified. Then by setting the registers as 1010 (i.e., to indicate the round cycle is 10, the last round for 128-bitAES), which is because in AES the mix-column operation is bypassed in the last round, it became much easier to discover the secret keys. Such a kind of attack is called constant-based attack. FHDA is another kind of scan-based attack by counting the number of bit changes on relevant plaintexts so as to discover the secret key, and refer to for more details on FHDA.

In the following, the security robustness of our method will be analysed and show how the proposed design can protect crypto cores from the known scan-based side channel attacks: CBA and FHDA.

i. Constant-Based Attack

Constant-based attack takes advantages of the fact that in encryption process, the contents of some flip-flops are always the same in some specified cycles for different plaintext inputs. In traditional scan, by using several different plaintext inputs and scanning out the contents at different times of the cryptographic operation, these registers called constant flip-flops (CFFs) in our work could be easily identified. Then by setting these CFFs to specific state through scan operation, the complexity of secret key identification might be reduced to a low level. When using the proposed SSS, it can be easily configured that once the intermediate data of CFFs passing the replaced SSSFs, they would be encrypted and this makes it extremely difficult to identify the positions of CFFs in the scan chain from external. In addition, because the proposed SSSFs deals with the scan-in and scan-out as well, it is also difficult for hackers to set the CFFs to desired states with no detailed knowledge of the scan structure implementation. Therefore, it is obvious that the proposed SSS could be an effective countermeasure of such constant-based attacks.

ii. Fixed-Hamming-Distance-Based Attack

In FHDA, usually several pairs of relevant plaintexts are applied and then for each pair the number of different bits in the round output is counted. Here let us use the FHDA procedure introduced in to illustrate the robustness of our SSS structure in AES. In our work, first we rerun the FHDA on an AES [3] implementation, and confirmed that when the Hamming distance between the round results is 9, 12, 23, or 24, the corresponding occurring frequency is one, which could be used to uniquely determine the round key. Next we simply group the registers together in the scan chain for each block, replace the last SFF in the scan chain with SSSF, and then conduct FHDA. In the third step, we replace two SFFs with SSSFs, and run the attack again. Furthermore the occurring frequency for each Hamming distance in the above mentioned three cases is calculated and plotted. By observing the results, it could be seen that the number of combinations that might be used to uniquely determine the pair of plaintexts is reduced from 4 to 1 and 0 for the two SSS implementations respectively.

IV. RESULTS AND DISCUSSION

As for security, secure scan requires the redesign of the function/test mode control unit, thus it could limit the CUT to be switched from functional mode to test mode [9]. To run in scan test mode, all the internal registers should be reset and instead of the secret key a mirror key is loaded for scan test. However, it is not applicable in case that the secret key is hardware wired or stored in the secure memory and the reset operation cannot clear and should not clear them.

For design and test issues, secure scan does not support at-speed online testing due to the reset and key-reload operations, and would incur large area overhead (around 10% as indicated in) that is because additional registers, called mirror key registers (MKR) [8], are inserted to isolate any critical data

ISBN 978-93-82338-83-3 © 2013 Bonfring

from entering the scan chain when in test mode. Both the proposed SSS design and the flipped-scan can support at-speed testing. In our work, no negative effect on fault coverage, test patterns and ATPG time is observed. Due to the total number of insertion is quite flexible depending on the required security margin, and according to our experience typically the required insertion (K) is at least less than half of the total number of SFFs (n), which clearly shows that the proposed SSS design provides a low cost but flexible secure test solution for cryptocores, and also removes the back-loop problem of XOR-chain for better testability.

As for security, secure scan requires the redesign of the function/test mode control unit, thus it could limit the CUT to be switched from functional mode to test mode. To run in scan test mode, all the internal registers should be reset and instead of the secret key a mirror key is loaded for scan test. However, it is not applicable in case that the secret key is hardware wired or stored in the secure memory and the reset operation cannot clear and should not clear them. For flipped-scan, it still has the security threat on FHDA because the Hamming distance between the observable scan-outs and the real response is fixed. To run in scan test mode, all the internal registers should be reset and instead of the secret key a mirror key is loaded for scan test.

V. SIMULATED OUTPUT OF VHDL CODING

The output taken from an example,Fig.4 shows the outputof proposed scanning stricture SSSF is used to scan a 4bit full adder. In normal mode get the actual result and in the scanning mode we can get encrypted output.

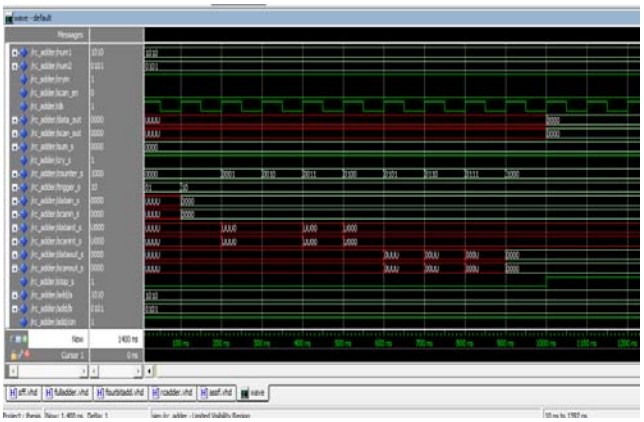

Fig. 5: VHDL output of SSSF using 4bit full adder

The objectives of this proposed architecture to design Shatterproof Secure Scan Design countermeasure Against Scan-Based Differential Cryptanalysis for compatible with the state-of-the-art design flow. The output waveform of SSSF Scan is shown in fig4 and here the security is significantly improved with ignorable design and test overhead.

VI. CONCLUSION

In this paper, a new shatterproof secure scan technique is introduced as an effective countermeasure against scan-based differential cryptanalysis. Thus to develop secure test techniques for these crypto cores becomes an emergent task so as to guarantee the security as well as the quality. In the literature, some interesting secure test methods have been proposed to protect crypto cores against SSCA. A function/test mode control method was proposed in which the basic idea is to limit the crypto cores being switched between normal function mode and scan test mode. However it is not applicable in case that the secret key is hardware wired or stored in the secure memory and the reset operation cannot clear and should not clear them.

The proposed scheme can be used to protect the intellectual property of a chip, which is easily compromised using conventional scan chains. The security of the flipped scan chain against scan-based attacks depends on the fact that the attacker is unable to ascertain the structure of the scan chain due to the presence of inverters in the chain. Moreover, it doesn‘t support at-speed online testing, and incurs large area overhead. It could be fully compatible with the state-of-the-art design flow and all the advantages and simplicity of traditional scan test are preserved, therefore it is desirable in modern crypto designs as a secure test solution with ignorable design/test overhead.

ACKNOWLEDGMENT

The authors would like to thank the Department of Electronics and communication, SNGCE Kadayirippu for their support. We would also like to thank friends and resource persons who give technical support, valuable advice and encouragement throughout the project.

REFERENCES

[1] Youhua Shi ; Togawa, N. ; Yanagisawa, M. ; Ohtsuki, T.Very Large Scale Integration (VLSI) Systems, IEEE Transactions on “Robust Secure Scan Design Against Scan-Based Differential Cryptanalysis” VOL. 20, NO. 1, JANUARY 2012.

[2] B. Yang, K.Wu, and R. Karri, “Scan based side channel attack on dedicatedhardware implementation of data encryption standard,” in *Proc.Int. Test Conf.*, 2004, pp. 339–344.

[3] B. Yang, K.Wu, and R. Karri, “Secure scan: A design-for-test architecture for crypto chips,” *IEEE Trans. Comput.-Aided Des. Integr. CircuitsSyst.*, vol. 25, no. 10, pp. 2287–2293, Oct. 2006.

[4] R. Nara, N. Togawa, M. Yanagisawa, and T. Ohtsuki, “Scan-based attack against elliptic curve cryptosystems,” in *Proc. IEEE ASP-DAC*, 2010, pp. 407–412.

[5] G. Sengar, D.Mukhopadhyay, and D.R. Chowdhury, “Secured flipped scan-chain model for crypto-architecture,” *IEEE Trans. Comput.-Aided Des.Integr. Circuits Syst.*, vol. 26, no. 11, pp. 2080–2084, Nov. 2007.

[6] M. Agrawal, S. Karmakar, D. Saha, and D. Mukhopadhyay, “Scan based side channel attacks on stream ciphers and their counter-measures,”in*Proc. Int. Conf. Cryptology India (INDOCRYPT)*, 2008, pp. 226–238.

[7] H. Atobe, R. Nara, Y. Shi, N. Togawa,M. Yanagisawa, and T. Ohtsuki, “Dynamically variable secure scan architecture against scan-based sidechannel attack on cryptography LSIs,” IEICE Tech. Rep., Nov. 2008, vol. 108, pp. 55–59.

[8] Y. Shi, N. Togawa, M. Yanagisawa, and T. Ohtsuki, “Design-for-secure-test for crypto cores,” in *Proc. IEEE Int. Test Conf.*, 2009, pp. 1–1,Poster-11.

[9] D. Hely, M. Flottes, F. Bancel, B. Rouzeyre, and N. Bérard, “Scandesign and secure chip,” in *Proc. Int. On-Line Test. Symp.*, 2004, pp. 219–224.