Indian Journal of Science and Technology, *Vol 8(13), 61856, July 2015*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Rectifying Various Scan-based Attacks on Secure IC'S

C. Ramya[1*] and S. Saravanan[2]

[1]VLSI Design, SASTRA University, Thanjavur-613401, Tamil Nadu, India; ramyaabi2491@gmail.com
[2]School of Computing, SASTRA University, Thanjavur-613401, Tamil Nadu, India; saran@core.sastra.edu

Abstract

Designing of confidential ICs must satisfy many design rules in order to rectify the various attacks and to protect the secret data. Based on the concept of withholding information, on-chip comparisons for actual and expected response have already been proposed. From the security point of view, few limitations of existing method limit the security level. Some countermeasures have been proposed in order to secure the scan technique and on-chip comparison. In this paper, an additional inverter is introduced within the scan chain architecture. The introduction of flipped scan chain increases the switching of scan output and increases the complexity to retrieve the secret data. On comparing with Traditional scan chain, proposed method results in only negligible area overhead with high security level. This result shows that possible trials will be more than $2^{\#SFF}$ to hack the data. The proposed method can be applied for all scan testing.

Keywords: Flipped Scan Chain, On-Chip Comparison, Scan Chain

1. Introduction

Scan-based test scheme is the powerful design for hardware testability for sequential circuits at production time and debugged infield. High fault coverage is obtained by scan-test fault diagnosis[5]. Testability designs may allow required fault diagnosis by directly accessing the internal state of the circuit under test. The diagnosis of faulty devices is mandatory to understand the defects at the production time so that it can improve the production yield[1]. Many aspects of our applications rely on electronic data exchange Encryption algorithms are used to guarantee the confidentiality, integrity, and authenticity of these applications. These algorithms are implemented on dedicated hardware for performance optimization and to add confidential information, which must be kept secret from unauthorized users[9–13,19]. Imperfect production process of devices needs manufacturing testing to find the defective one among all the circuits. Such defects may allow some possibilities to observe the circuit's internal state which is related with confidential information.

Various countermeasures have been proposed to rectify the scan attacks which are mentioned earlier. A common industrial practice is to unbound the scan chain after production testing which is done by blowing the fuses at the ends of scan chain[11]. However, Design for Test flow is same in this method. But still controllability and Observability features of scan chain can be weak from the cryptographic point of view. In brief, a new design-For-Testability architecture was described on the concept of withholding information within the chip[8]. This eliminates the need of scan chain disconnection from the chip. This approach is mainly to avoid scanning out the data and interface to test equipment for further analysis. Method for on-chip comparison was already been proposed in [1] and [8]. The test procedure consists in providing both test inputs and expected test responses to the Device-Under-Test (DUT), comparison between the actual and the expected responses being done on-chip. It offers the possibilities to observe the secret key of encrypted data which occupies the register since continuous bitwise observation of the comparison result.

Another approach to overcome this drawback as mentioned above, comparing the whole test vector instead

*Author for correspondence

comparing bit by bit. After applying the whole test vector, only the pass/fail information is read out from the DUT. A limitation in this technique is predicting expected response for test vector with unknown value is no longer possible. Some countermeasures are proposed for such limitations and summary of the most relevant design-for-testability and security proposals as mentioned in the literature, and discuss their drawbacks which in brief are organized as follows.

Several countermeasures have been proposed to rectify possibilities of scan attacks. One of the methods is scan-chain scrambling technique[10] in which the flip-flops are dynamically rearranged in a scan chain to protect the confidential data. This scrambling technique provides both security and testability for crypto chips. However, information which is scanned out from the chip can still determine the secret key with increased power consumption and area overhead. Secure-scan DFT architecture with additional mirror key register was proposed to overcome the above mentioned limitations. It utilizes the additional register (MKR) for storing secret information instead of using data path & control path for scan chain[12]. This solution will result in limited fault coverage and usage of additional register increases the area overhead in the architecture.

Two classes of solutions were found in literature such as dedicated secure test wrappers[6], and the hidden functions to obfuscate the actual contents of the scan chains. Secure test wrappers basically implement an FSM with two states: mission mode and test mode. In mission mode, the circuit handles confidential data and the Scan chain cannot be accessed. In test mode, scan chain is enabled because confidential data no more processed in the circuit in this mode. Switching from mission to test mode is usually implemented by resorting to an authentication protocol. To enable the test mode, test controller must receive the secret wrapper key before it switches. However, secured authentication method requires the implementation of crypto functions into the wrapper and thus area overhead considerably increases[7]. In paper [16], it explains how to overcome hackers attack by finding from CRO I/O. It also shows performance of crypto function without an external power source embedded capacitance power supply method is used to integrate group of capacitor with power supply.

In paper [17], proposed modified scan path architecture through extra electronic component to protect secure key against threat with modified elliptic curve crypto scan architecture in HDL. In paper [19], Control of X-distribution in scan path propagated to comparator and X align block to achieve modified scan cell. It improves observability of scan path and reduces the size of test vector. Other architectures have been explored for rectifying scan-based attacks by maintaining the secret function within the chip. Method of On-chip evaluation, compensation and storage of diagnosed fault avoids possibility to observe through the scan-out data. In [14], securing scan chain lock and key method is proposed. In [4], Scan flip flop is altered as flipped scan flip flop by inserting invertors in the scan chain randomly, providing bit flipping while data are scanned out. Previously, thwarting method was proposed for on-chip comparison. This architecture includes secure comparator along with Device Under Test (DUT) for on-chip comparison instead of scanning out the data. Test procedures processed by providing scan-in input and expected response for comparison. The actual response which is scanned out from the scan chain is given as one of the input to the secure comparator where actual response and expected response is compared. In paper [8] it reduces the complexity of brute force attack and describes the countermeasures to rectify the above mentioned scan attacks.

2. Proposed Solution

All scan chain attacks discussed in the literatures [2,3,6] rely on the possibility to hack the secured information through the scan chain. Therefore, countermeasures have proposed for making the scan out nonexploitable. The proposed approach in this paper is based on comparing the actual responses with the expected responses within the chip area instead of scanning-out and comparing the response within the ATE. In standard scan-based scheme, FF's is replaced with scan flip flops (i.e. flip flop with a multiplexer). These are connected serially to behave as long shift register in test mode. The input of FF is directly connected to input pin (scan-in) and the output of the FF is directly connected to scan-out (output pin). An additional pin (scan enable) is accessed to select whether the SFFs behave as normally or as a shift register. The output of one SFF is connected to the input of next SFF.

When the scan chain is introduced for hardware testing, additional scan enable pin is needed to enable the test mode from normal mode. Insertion of scan-chains while testing the hardware requires a few multiplexed pins to

the standard inputs/outputs to behave as the scan-enable, scan-inputs and scan-outputs. A scan DUT with additional mux is shown in the Figure 1.

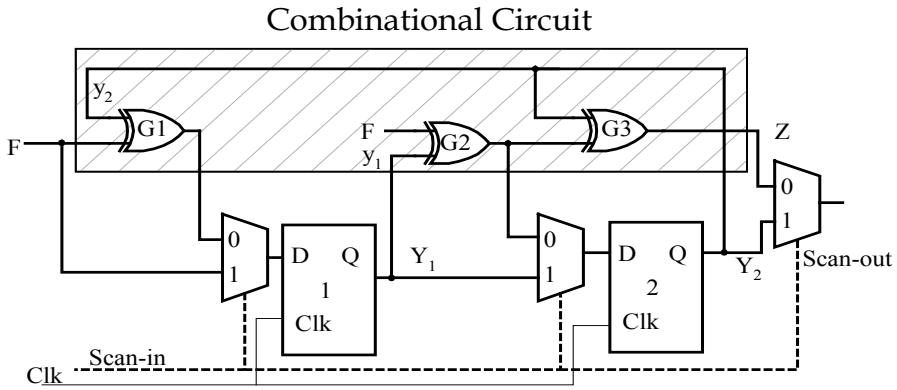

Figure 1. Combinational circuit with scan flip flop.

Introduction of scan chain will reduce the additional circuitry for testing. When the FFs behave as a shift register, the device undergoes for testing the logic. While scanning out the data for comparing it with the original data, attackers can be able to hack the secure information. In order to make it securable, SFFs is replaced with flipped scan chain flip flops (FSFFs). An additional inverter is added along with the scan chain (i.e. Flipped scan chain). When the inverter is randomly arranged before the scan chain, the scan out data of random SFF will be flipped (inverted)[15]. Flipped Scan chain aimed at protecting the scan data form being analyzed through the intermediate states of the device. Moreover, this FSFF does not impact on the normal functionality of the device. An introduction of inverter with the scan FF is showed in Figure 2.

Flipped scan chain increase the complexity of brute force attack to observe the intermediate signals exactly. Further, random arrangement of NOT gate inverts the test output randomly and goes for comparison with the same flipped expected response. Based on the approach of on-chip comparison, this paper in brief is to compare the actual response with the expected response for whole test vector and even no more unknown values in the test data make it easy to provide expected response after testing the data with flipped scan chain. When the scan chain is enabling, need to provide both expected and test input to the design. But predicting the expected response for unknown values in the test input is no longer possible. In such case, this comparison will no more confidential and effective. To overcome this limitation, the proposed approach is to compress the input test data by code based scheme. Data compaction method will reduce the unknown values by making it compatible within the test patterns.

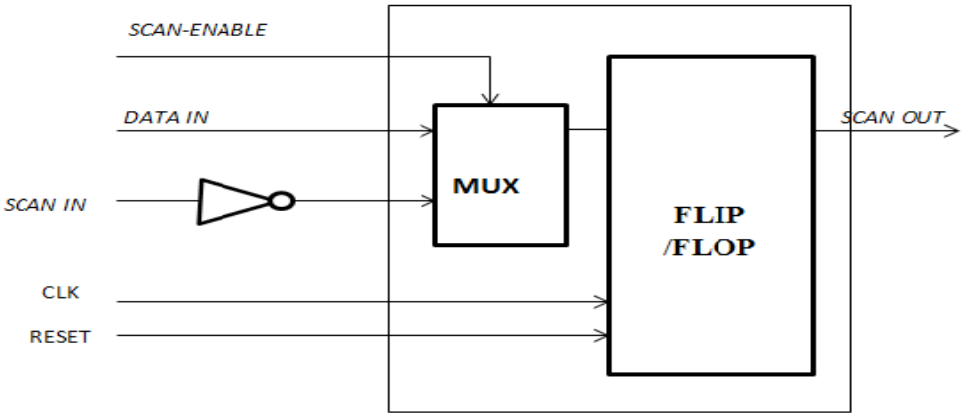

Figure 2. Flipped scan chain flip flop.

The general scheme of the proposed Secure Comparator is shown in Figure 3. Instead of neither ignoring the comparison result for unknown values nor providing the additional mask to avoid the unknown values in the comparison, these unknown values are filled by using the compression technique from the flipped scan chain. Once the data is compressed with known values, ATE also provides expected response for those compressed test inputs. Instead of scanning out the data, on-chip comparison is done by secure comparator. The Secure Comparator is composed of three parts: the Sticky Comparator, output enabler and I/O buffer. Sticky comparator compares the scan out result with the expected response the help of a flag. Initially the flag is reset, the flag set to '1' when the comparison fails. The value of the flag designates whether it is equal or not. The output enabler triggers the Test Res after applying the whole test vector. It consists of down counter with parallel load to load the #SFF when scan chain is enabling. I/O buffer (bidirectional buffer) permits the sharing of same pin for both Test Res and Sin.

This flipped scan chain would increases the complexity of brute force attack to retrieve the data. example to illustrate operation of flipped scan chain is shown in Figure 2 where the original SFFs (random) is replaced by an FSFF. Here, scan chain with eight SFF is considered. For shift operation, data that passes FSFF would be inverted.

Let us assume test vector

$V = (V_{n-1}, \ldots V_2, V_1, V_0)$ and the expected response is $r = (r_{n-1}, \ldots r_2, r_1, r_0)$.The scan-input is $S_{in} = (Si_{n-1}, \ldots, Si_2, Si_1, Si_0)$ and the output from the scan chain is $S_{out} = (So_{n-1}, \ldots, So_2, So_1, So_0)$ The random positions of SFF are replaced by FSSF like the Figure 2. Thus scan out and the test vector can be expressed in terms of r and S_{in}, respectively.

Based on the above equation, for the pair of test vector and expected response (V, r) is processed with unique sequence of scan-in and scan-out. Thus, output data is almost switched from the input as shown in Figure 2.

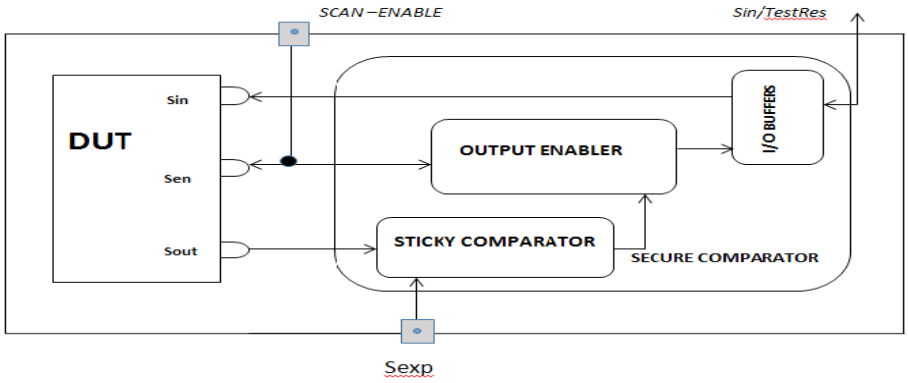

Figure 3. Secure comparator.

3. Security and Comparison Result

3.1 Security Analysis

The proposed scheme of Flipped scan chain with comparator further reduces the possibility to hack the secured information. Insertion of comparator along with the traditional scan chain still permits the attackers to observe through the intermediate state of FFs. In the proposed method of Flipped scan chain along with secure comparator, intermediate bit streams are flipped randomly with help of the inverter. Brute Force attack is only the feasible solution to retrieve the secret key. It requires 2 ^ #SFF possible trial for #SFF scan chains.

$$v_i = \begin{cases} si_i, if\,(i < k) \\ \overline{si_i}, if\,(i = k) \\ si_i, if\,(i > k) \end{cases} \quad so_i = \begin{cases} r_k, if\,(i < k) \\ \overline{r_k}, if\,(i = k) \\ \overline{r_k} + r_k, if\,(i > k) \end{cases}$$

Thus for hackers, there is a possibility to predict the counting's of inverter in the scan chain by sending unknown patterns for feasible times but the position of inverter is unpredictable. This proposed module does not impact the design flow. Even though this solution increases the area overhead, implementation needs only small part of the designs.

3.2 Comparison Result

Synthesis of proposed method implies that parameters like area, power etc. vary from the existing one. Table 1 shows the comparison result of area overhead.

Table 1. Result comparison of area overhead

Circuits	DFF	SFF	FSFF	FSFF with Comparator
S5378	4421	5907	6324	6731
S9234	3504	4841	5238	5610
S13207	10493	14639	14677	17687
S15850	12984	21647	25892	29436

Table 2. Hardware comparisons with FSFF

Implementation	Logic per insertion	Number of insertion
Xor-chain	Xor x1	n/2
RSS	Xor x1 Inv x1	K
Flipped-scan	Inv x1	n + x

Even if the area is high, it is negligible when compared to other existing solutions. Table 2 shows the comparison hardware overhead among few methods. In the security point of view, this method would increase the complexity of the feasible solution to hack such information from the DUT. Flipped scan chain method supports at-speed testing and moreover no impact on fault coverage. Where 'x' is the number of inverter depends on the combinational logic in the circuit, 'n' is the total number of scan chain flip-flops and x is less than n, i.e., $x < n$.

4. Conclusion

In this proposed scheme, a new approach of flipped on-chip comparison is described for security issues. Based on the concept of holding the confidential information within the chip, proposed method is more secure than other countermeasures with less controllability to unknown users. It compares both the input response and the expected response without relying on the cost of the design. Flipped scan chain increases with negligible area overhead and design changes. This method has also been accessed in order to reduce the possible unknown values in the test procedure. On comparing with the standard scan test, this design does not impact on the quality of the test and the diagnosis of fault.

The new method can be implemented after the synthesis of DUT and achieves high security against the scan attacks with proper protection.

5. References

1. Poehl F, Beck M, Arnold R, Rzeha J, Rabenalt T, Goessel M. On-chip evaluation, compensation and storage of scan diagnosis data. IET Computers & Digital Techniques. 2007: 1(3):207–12.
2. Yang B, Wu K, Karri R. Secure scan: a design-for-test architecture for crypto chips. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. 2006 Oct; 25(10):2287–93.
3. Yang B, Wu K, Karri R. Scan based side channel attack on dedicated hardware implementations of data encryption standard. Proceedings of IEEE International Test Conference. 2004 Oct. p. 339–44.
4. Sengar G, Mukhopadhyay D, Chowdhury DR. Secured flipped scan-chain model for crypto-architecture. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. 2007 Nov; 26(11):2080–4.
5. Hely D, Bancel F, Berard N, Flottes ML, Rouzeyre B. Test control for secure scan designs. Proceedings of the IEEE European Test Symposium; 2005 May. p. 190–5.
6. Chiu G–M, Li JCM. A secure test wrapper design against internal and boundary scan attacks for embedded cores. IEEE Transactions on Very Large Scale Integration (VLSI) Systems. 2012 Jan; 20(1):126–34.
7. Agrawal M, Karmakar S, Saha D, Mukhopadhyay D. Scan based side channel attacks on stream ciphers and their counter-measures. Proceedings of 9th International Conference on Cryptology in India; Kharagpur: LNCS; 2008. p. 226–38.
8. Da Rolt J, Di Natale G, Flottes ML, Rouzeyre B. Thwarting scan-based attacks on secure-ICs with on-chip comparison. IEEE Transactions on Very Large Scale Integration (VLSI) Systems. 2014 Apr; 22(4):947–51.

9. Da Rolt J, Di Natale G, Flottes ML, Rouzeyre B. New security threats against chips containing scan chain structures. IEEE International Symposium; Hardware-Oriented Security Trust; 2011 Jun. p. 110–5.
10. Hely D, Bancel F, Flottes M, Rouzeyre B, Renovell M, Berard N. Scan design and secure chip. Proceedings of the IEEE International On-Line Testing Symposium; Funchal, Portugal: 2004. p. 219–26.
11. Easter RJ, Chencinski EW, D'Avignon EJ, Greenspan SR, Merz WA, Norberg CD. S/390 parallel enterprise server CMOS cryptographic coprocessor. IBM Journal of Research and Development. 1999 Sep-Nov; 43(5/6):761–76.
12. Josephson D, Poehhnan S. Debug methodology for the McKinley processor. Proceedings of International Test Conference; Baltimore, MD: 2001. p. 451–60.
13. Mukhopadhyay D, Banerjee S, Chowdhury DR, Bhattacharya B. Cryptoscan: Secured scan chain architecture. Proceedings of 14th IEEE Asian Test Symposium; 2005. p. 348–53.
14. Lee J, Tehranipoor M, Patel C, Plusquellic J. Securing scan design using lock and key technique. Proceedings of the 20th IEEE International Symposium of Defect and Fault Tolerance in VLSI Systems; 2005. p. 51–62.
15. Shi Y, Togawa N, Yanagisawa M, Ohtsuki T. Robust secure scan design against scan-based differential cryptanalysis. IEEE Transactions on Very Large Scale Integration (VLSI) Systems. 2012; 20(1):176–81.
16. Sridhar KP, Saravanan S, Sai RV. Countermeasure against side channel power attacks in cryptography devices. Indian Journal of Science and Technology. 2014 Apr; 7(S4):15–20.
17. Sridhar KP, Raguram M, Prakash B, Koushighan S, Saravanan S. Secured elliptic curve cryptosystems for scan based VLSI architecture. ICICE2014-IEEE explorer; Chennai: 2014. p. 1–5.
18. Saravanan S, Charaphani K, Silambamuthan R. Design and implementation of hardware based entropy analysis. Research Journal of Applied Sciences, Engineering and Technology. 2012; 4(14):2082–6.
19. Narmatha D, Saravanan S. Improved observability of test pattern using X-alignment technique. International Journal of Applied Engineering Research. 2014; 9(11):1711–9.
20. Sridhar KP, Muralidharan D. Optimal hamming distance model for crypto cores against side channel threats. Indian Journal of Science and Technology. 2014 Apr; 7(4S):28–33.
21. Baek S-S, Won Y-S, Han D-G, Ryou J-C. The effect of eight-shuffling AES implementations techniques against side channel analysis. Indian Journal of Science and Technology. 2015 Mar; 8(S5):91–7.
22. Sasi SB, Sivanandam N. A survey on cryptography using optimization algorithms in WSNs. Indian Journal of Science and Technology. 2015 Feb; 8(3):216–21.