iJETRM
International Journal of Engineering Technology Research & Management

REVIEW ON EXISTING COUNTER MEASURES AGAINST SCAN BASED SIDE CHANNEL ATTACKS

Karthik Maiya*[1]
Deepika P[2]
*[1]Karthik Maiya (Department of Electronics and Communication Engineering, RVCE, India)
[2]Deepika P (Department of Electronics and Communication Engineering, RVCE, India)

ABSTRACT

Scan-based design-for-testability (DFT) structure has been widely adopted in core based designs as it enables high testability for design under test (DUT). However, security concerns are caused in the form of side channel attack. For a cryptographic core or module, unauthorized people can use scan chain as a side channel to collect sensitive information about the keys used in the core or the design itself. This poses a high threat for the fields where the cryptographic chips are applied. Effective countermeasures should be explored to solve this problem. In this paper, we have reviewed the existing work on secure scan designs and highlight their merits and weaknesses. All these work are compared in terms of the area overhead, security and impact on testability.
.

Keywords:
Design for Testability, Data Encryption Standard, Side channel attack

INTRODUCTION

Manufacture or structural Testing is a part of every ICs design cycle. Even very advanced fabrication processes produce defective ICs. These ICs can be prevented from reaching the market only by testing them thoroughly after they are manufactured. Testing is therefore essential to sort out faulty and good circuits and thus ensure the quality of the product. However, as the design complexity of an IC grows, the cost of its testing increases and as a result the overall price of IC in the market increases. To reduce the test cost, special design modifications at early stages of design cycle has been adopted throughout the IC manufacturing industry generally known as Design-For-Testability (DFT). The main purpose of introducing DFT to an IC is to improve testability (mainly the capacity to detect the presence of faults), diagnostics, test time and reducing the number of required test pins [1].

The most common DFT technique is scan insertion which increases the observability and the controllability of the circuit's internal nodes, thereby increasing the testability. But however it has been proven to be prone to side channel attack (SCA) which might leak details of ICs to unauthorized parties. These attacks are serious threats to highly complex ICs such as SOCs as most SOCs have dedicated crypto cores. Crypto cores are sequential circuits which run algorithms such as AES, DES or TDRE [2]. These algorithms are based on special keys which are used to encrypt and decrypt data. The main threat to such cores is corruption of these keys or hacking the keys. In this paper only scan based SCA and its mitigation using recently found advanced techniques is discussed [3].

SCAN BASED SCA

The insertion of scan chains involves replacement of the flip flops (FFs) in the design by scan flip-flops (SFFs) and connecting these SFFs in form of a shift-register, called as scan chain. The scan chain is bound to an input pin (scan-in) and to an output pin (scan-out). The most popular scan design style is the multiplexer based scan flop style. For this style an extra pin called scan-enable should be added to control the functionality of the scan chain.

If the scan-enable pin is set to 0, the SFFs are connected to the circuit and behave as normal flip flops (functional mode). When the scan-enable is set to 1 the SFFs are connected to the scan chain and the bit-stream at the scan-in is shifted in while the data stored in the SFFs is shifted out through the scan-out pin. A complex design such as a SOC may contain multiple cores with each core having multiple scan chains [1]. By controlling the scan-in and scan-enable inputs and observing the scan-out pin, the attacker can observe the confidential data or can corrupt the internal states of the crypto circuits.

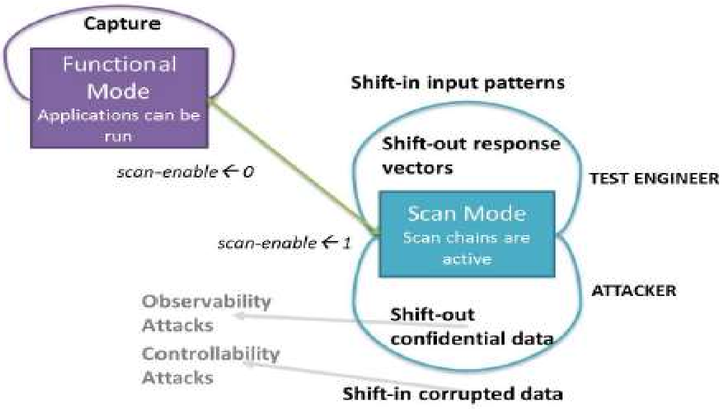

Fig. 1: A flow diagram representing behavior of test engineer and an attacker [1]

Fig. 1 illustrates the duality between test and security. The above loop during the scan mode in the figure shows the approach of a test engineer where the job is to shift patterns into the scan chain and shift-out the responses. The very same scan chain is used by the attacker to dump corrupted data into the scan chain (controllability attack) or can steal the confidential data (observability attack). Sometimes scan chains might also be used to get design information of hard IPs [1].

TECHNIQUES PROPOSED TO MITIGATE SCAN BASED SCA IN RECENT TIMES

State dependent scan flip flop (SDSFF)

This method was proposed by Yuta Atobe et al. where multiplexer based scan flop is converted to a new architecture as shown in Fig. 2

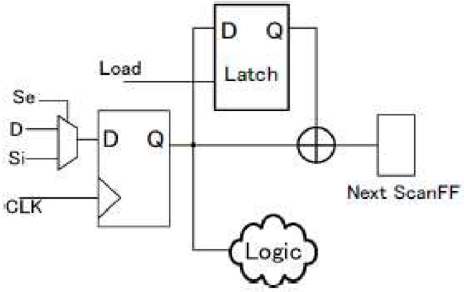

Fig. 2: SDSFF architecture [4]

In this architecture, the load signal of the D-latch, Si and D are the test inputs during testing. But the load to test signal is only made available to the test engineer. As a result attackers cannot shift the desired pattern into the chain to get confidential information. The authors have also proposed an improved variant of SDSFF as this design will automatically start loading load signal and the attacker can make use of it. The improved version of SDSFF updates the latch with different timing which is not available to a non test engineer. This can provide additional security to the scan flops.

Results of this paper were obtained for a circuit which performed RSA over 1024 bits. The RSA cryptography circuit contained 8507 flip-flops excluding the secret key registers in total and the length of scan chain was also 8507. The authors replaced normal scan FFs with 1, 2, 10, 20, 40, 60, 100 SDSFFs for security and overhead analysis. The main outcome of this analysis was that even with 100 SDSFFs the area overhead was found to be 0.6% in addition to a normal scan design and the possibility of an attacker successfully causing a scan attack is 3^{-n} where n is the total number of flops in the scan chain.

The key inference of this paper is that only with a few modifications to the scan flop it is possible to secure the crypto cores with only a small penalty in area. The main requirement to this technique is that length of the scan chain has to be sufficiently long so that the probability of successful attack is reduced [4].

Memristor retention loss based scan test

A memristor is an electrical component that limits the flow of electrical current in a circuit and remembers the amount of charge that had previously flowed through it. Memristors are non-volatile that is they retain memory without power. Memristor devices generally endure retention loss in the long term. Exploiting this retention loss, the authors Yanping Gong et al. have proposed a new secure scan chain scheme to address scan chain based attacks. A configurable refresh scheme is utilized to distinguish between the testing and non-authorized accesses. With a finite state machine based key verification process, only authorized testers will be able to receive correct scan outputs.

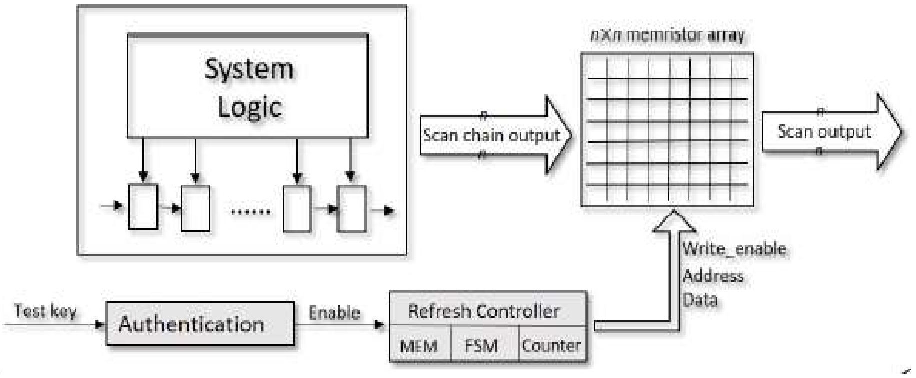

Fig. 3: Architecture of proposed scan test [5]

The proposed technique in Fig. 3 makes use of scan obfuscation where outputs of scan chains are multiplied with the memristor array as matrix multiplication. Due to retention loss and multiplication the values of memristor array changes and outputs become corrupted. Only authenticated testers with correct test key can access the refresh controller to refresh the memristor array and maintain constant values of the memristor array. Thus only proper test personnel can refresh memristor array and can get the correct scan outputs.

The proposed technique was verified for a scan architecture with 512 scan chains. The memristor array is 512 X 512. The authors have shown that time correlation of the memristor array decays exponentially with time without a refresh [5]. The key benefit of the design is that retention loss is completely random making this technique efficient in protecting the confidential information.

Key based scan test

This technique was proposed by Rahul Pandey et al. which uses a key to secure the scan chain outputs. Fig. 4 is the architecture proposed by the authors. The user has to input a particular key of n-bit length along with patterns. A reference key is stored in the memory which will be compared with the user input key. If the key matches, then the actual outputs from the scan chains are encoded and come out. If the key does not match then a random response is generated, encoded and comes out. Thus an observability scan attack can be avoided.

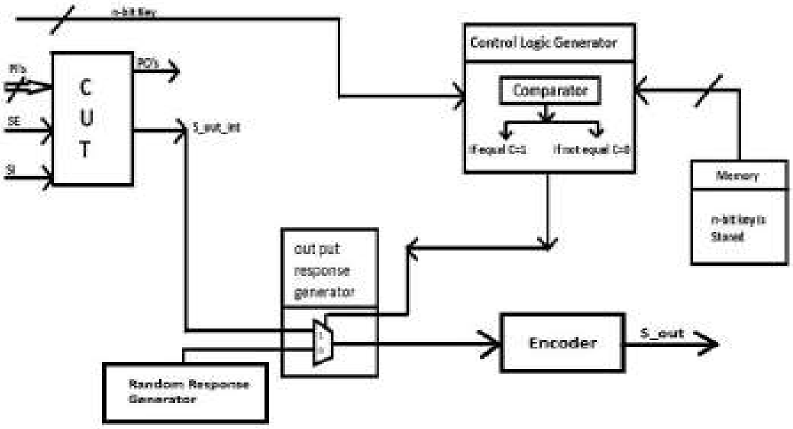

Fig. 4: Proposed architecture for testing [6]

This architecture was used on a cryptographic core which performs AES. The secret key used had a length of 128 bit. The ATPG for the core detected 287 test vectors with fault coverage of 99.98%. The area overhead is 0.14% of the scan design, while the power overhead is 0.008% [6]. This key advantage of this technique is that it requires very less hardware for a core to make it more secure from scan attacks but core will still be susceptible to corruption.

LFSR based secure scan test

The authors Samta D. Talatule et al. have proposed a LSFR based scheme for scan test. The LFSR is used to generate a key for every pattern.

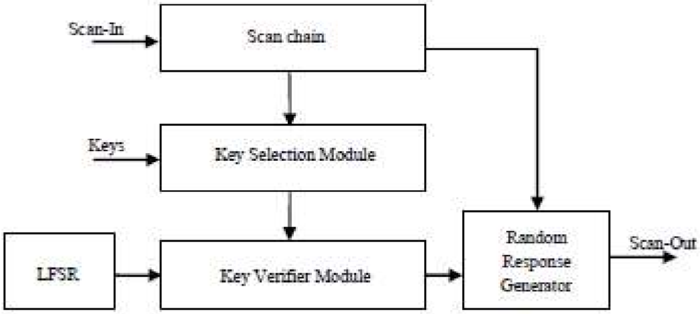

Fig. 5: Proposed architecture of the design [7]

Fig 5 shows the proposed architecture for scan test. The authors have used LFSR to generate keys. The patterns loaded to the scan chain most of the times have don’t care bits. The user has to embed the key in the position of don’t care bits. The position of don’t care bits is selected by the selection module which is a group of multiplexers. Once the position of don’t care bits are found, key verifier module compares these bits with the LFSR bits. The key verifier module is a simple combination of XNOR and AND gates. If the keys are matched correct output response appears at the output else a random response appears at the output. The experimental results of this paper were obtained for the s27 benchmark circuit. s27 is one of the sequential benchmark circuits proposed by the International Symposium on Circuits & Systems (ISCAS).

The area overhead of this technique is pretty large due to use of LFSR as it has to match the length of key and for a proper security length of a key should be large [7].

Lock and key scheme based scan architecture

This architecture was proposed by Yanhui Luo et al. where a shift register (SR) is used to verify the key and is used to control scan enable pin of the scan flops.

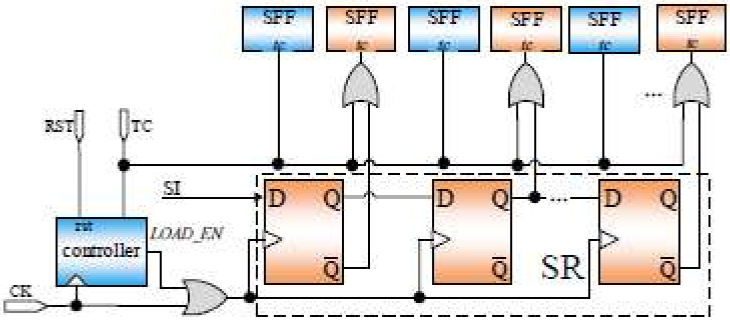

Fig. 6: Proposed architecture [8]

Fig 6 is the complete architecture of the lock and key scheme. In functional mode TC=1, hence the SFFs behave as normal functional flops. During test mode TC=0, and shift registers are configured such that only if proper values are shifted into the SR through SI, then TC of all scan flops will be enabled and patterns can be shifted into the scan chain. The pattern to the SI will be the key to the technique. If a different key is fed into shift register some scan flops will be in normal mode and pattern will not be shifted into the scan chain.

The implementation was verified for security, testability and area overhead on 64 and 128 bit AES core. The probability of scan attack was found to be 2^{-N} where N is the length of the key. The area overhead was found to be 0.34% over the scan design. This method is very useful when key length is high but area overhead will also increase [8].

CONCLUSION

Scan-based DFT technique is a well known and established DFT technique but arise security concerns as it enables a side channel for adversary to access the sensitive data in crypto cores. A few counter measures have been reviewed in this paper that can be used to secure a scan design against the scan based side-channel attacks. All these work are reviewed with regards to security, area overhead, impact on testability and other compromise to the design performance.

ACKNOWLEDGEMENT

We thank our colleagues from RVCE who provided insight and expertise that greatly assisted this review, although they may not agree with all of the interpretations/conclusions of this paper.

REFERENCES

[1] Jean D.R.; Amitabh D.; Giorgio N.; Marie-Lise F.; Bruno R.; Ingrid V. *Test versus Security: Past and Present*, IEEE Transactions on Emerging Topics in Computing, 2 (1): 50 – 62. 2014

[2] Cheng X.; Sungju P.; Ji Z. *Analysis of Recent Secure Scan Test Techniques*, Journal of Software Engineering and Applications, 09 (03): 91-101. 2016

[3] Wei Z.; Aijiao C.; Huawei L.; Gang Q.; *How to secure scan design against scan-based side-channel attacks?*, IEEE 26th Asian Test Symposium (ATS), ISSN: 23775386. 2017

[4] Yuta A.; Youhua S.; Masao Y.; Nozomu T. *Dynamically changeable secure scan architecture against scan-based side channel attack*, International SoC Design Conference (ISOCC), ISBN: 978-1-4673-2990-3, 2012

[5] Yanping G.; Fengyu Q.; Lei W. *A secure scan chain test scheme exploiting retention loss of memristors*, IEEE International Symposium on Circuits and Systems (ISCAS), ISBN: 978-1-4673-6853-7. 2017

[6] Rahul P.; Sakshee P.; C.S Mohammed Shaul Hammed, *Security in Design for Testability (DFT)*, ISSN: 2473943X. 2017

[7] Samta D. T.; Pravin Z.; Pradnya Z. *A secure architecture for the design for testability structures*, 19th International Symposium on VLSI Design and Test, ISBN: 978-1-4799-1743-3. 2015

[8] Yanhui L.; Aijiao C.; Gang Q.; Huawei L. *A new countermeasure against scan-based side-channel attacks*, IEEE International Symposium on Circuits and Systems (ISCAS), ISSN: 2379447X. 2016

[9] Masoud R.; Farinaz K.; Ramesh K. *A Primer on Hardware Security: Models, Methods, and Metrics*, Proceedings of the IEEE, 102 (8): 1283 – 1295. 2014

[10] Sudeendra kumar K.; Kalpesh L.; Sauvagya R. S.; K.K. Mahapatra *On-chip comparison based secure output response compactor for scan-based attack resistance*, International Conference on VLSI Systems, Architecture, Technology and Applications (VLSI-SATA), ISBN: 978-1-4799-7926-4, 201