ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

Scan-chain free functional testing for secured hardware systems.

Ananth Hari R[1]*, and R Muthaiah[2].

[1]M.Tech VLSI Design, SASTRA University, Thanjavur, Tamil Nadu
[2]Professor, Dept.of School of Computing, SASTRA University, Thanjavur, Tamil Nadu

ABSTRACT

Security is an important constraint and has to be maintained, when we are performing Testing methods for Secure hardware systems. Scan Chain Test is a very efficient technique for testing the hardware. But when it is used in circuits where security is maintained, it can acts as a Gateway for the attackers to access secret keys. Hence Built-in Self test is widely used for secure testing, thereby security is maintained. This Built-in Self Test is used to perform Testing for Fuzzy Extractor (FE) Block in which area overhead is reduced by repeatedly using the FE blocks. Scan chain free functional testing is the aim of the secure testing.

Keywords: Security, Built-in Self-Test, Fuzzy Extractor, Secure testing.

*Corresponding author

INTRODUCTION

Testing a circuit is one of the important strategies for circuits, where security is maintained. Scan Chain Test is a very efficient technique for testing the hardware .But when it is used in circuits where security is maintained, it can acts as a Gateway for the attackers to access secret keys. Hence Built-in Self test is widely used for secure testing, in which the internal hardware is not scanned and scan attacks can be avoided, thereby security is maintained. In Built-in Self Test fault coverage can be improved by Reseeding Technique. This Built-in Self Test is used to perform Testing for Fuzzy Extractor (FE) Block in which area overhead is reduced by repeatedly using the FE blocks. Scan chain free functional testing is the aim of the secure testing. In order to inspect the use of scan-chain in a circuit a Smart Controller can be used which can eradicate scan attacks in the circuit.

EXISTING METHODS

IC fabrication is done at the foreign countries due to low costs [1]. Hence this may lead to easy access of secured information by an attacker, which ultimately results in loss of security in IC. The attacker may use Trojan IC's as a sub-circuit to access a information. In order to maintain security ,a set of finger-prints have been developed using noise modeling techniques and using side channel information such as power. Finger-prints are developed using few set of IC's and remaining IC's are tested against the finger prints and the results are analyzed in which IC's magnitude which are 3-4 orders less than main circuit are Trojan IC's.

DFT [2] is the most common technique for testing the circuit in VLSI systems. However when it is used in circuits, where security is maintained it can act as a Gateway for an attacker. The attacker can gain access to circuit, when the circuit is switched from normal mode to test mode. One such countermeasure is to reset the circuit, when switched from normal mode to test mode. In Built-in Self Test fault coverage can be improved by Reseeding Technique in the paper [3]. Reseeding is done by storing the seeds in an external tester. In this Method, Built-in Reseeding is done in which seeds are encoded in on-chip hardware. By this method Area-overhead is minimized and at the same time 100% fault coverage is also achieved in BIST.

Scan Chain Test[4] is a very efficient technique for testing the hardware .But when it is used in circuits where security is maintained, it can acts as a Gateway for the attackers to access secret keys from DES. Hence it is recommended to use Built-in Self Test method as a testing method for the hardware where the internal hardware is not scanned and scan attacks can be avoided, thereby security is maintained. Built-in self test is an efficient test method [5], where security is maintained .The method has high Stuck-at-fault coverage and performs testing for Fuzzy extractor. The Area overhead can be reduced by repeatedly using the given Fuzzy Extractor Block. The Area overhead is reduced by 2.2% by repeatedly using the same FE block.

There are various Testing methods available of which scan-chain is the most common test technique [6] used. But in circuits where security is a important issue, use of scan-chain is considered as ill-legal way of trying to break the security by the users. Hence users are restricted to use Scan-chain method and can use other test methods. In order to inspect the use of scan-chain in a circuit a Smart Controller can be used which can eradicate scan attacks. Also the area overhead introduced by the controller is less.

Scan-chain Test [7], method is a powerful test method but it can act as a Gateway for an attacker to access secret key. Several test methods have been proposed for scan-chain method to prevent the scan attacks, one such method is adding anti-fuse on scan pins and blowing them after manufacturing in the paper .IC fabrication is done at the foreign countries [8] due to low costs. Hence this may lead to easy access of secured information by an attacker, which ultimately results in loss of security in IC. In order to restrict the access of secured information by an attacker, a secure access mechanism has been proposed, which needs storage of authentication secrets in a external non-volatile memory (NVM). This PUF-based test wrapper method reduces the area overhead by which it enhances the efficiency of the proposed method and does not requires storage in NVM. Built-in Self test is a very efficient test technique that assures scan chain-free testing [9]. BIST along with crypto-cores is done for the circuits and the output of core is given as input again and is tested for certain number of iterations and the output is compared with pre-defined signature. This method gives 100% fault coverage and negligible area-overhead. FuzzyExtractor [10] extracts a sampled uniform distribution which is equally probable and random in nature. This extraction can be used as a key and the extract remains the same irrespective of any input. Hence it can be used to produce key for biometric applications and other noisy data. In the paper [11], Built-in Self Test is a very powerful test method that assures scan-chain free functional testing. But it requires extra-circuitry for executing signature analysis and test pattern generation. Test cost reduction can be obtained by repeatedly using the embedded resources three additional modes are added which reduces the extra cost in terms of area. It is very common to include Intellectual Property (IP) [12] into the circuits. The main reason to include IP is to create license for the hardware and thereby ensures the safe way of marketing the hardware with various features in it and another reason to use IP is to reuse the features in the hardware. But there is a possibility of creating a multiple copy of secure code while programming the FPGA, and can use it to program other circuits without actually buying the license. This creates loss for the manufacturers and this can be avoided by using a PUF (Physical Unclonable Function) on the SRAM based FPGA. PUF cannot be cloned and provides security for the hardware manufacturers.

There are various types of attacks faced by the hardware ICs in the paper [13]. There are three main reason for hacking the hardware. The first reason is, to access the secure key present inside the hardware and the second is to gain license for the IP in the hardware and create multiple copies of the licensed data , so that it can be used in other FPGAs and the third reason is to alter the original function of the systems. There are protection techniques proposed to avoid these attacks. The techniques are masking, adding Pseudo Random Number Generator (PRNG), Sensorsetc. Multi-polynomial LFSR [14] is used to cover the test faults for large and complex systems. The test data which is obtained after compression is stored in a external memory. Group of test bits are represented as test data up to 16 polynomials in it.

Scan based attacks are more common type of attack for secured hardware in the paper [15]. In order to reduce these type of attacks, various security measures are proposed. Insertion of DES IP, 4 shift spy Flip-flops are inserted between 198 flip-flops. Also a scan enable signal is inserted in the circuit and the output of the circuit is observed at scan output pin. The output of the signal should come within 3 clock cycles.

TABLE 1: COMPARISION TABLE

Ref.nos	ADVANTAGES	DISADVANTAGES
[1]	This technique is used to detect Trojans in the circuit using set of fingerprints.	This Technique does not completely eradicate the problem, but provides a starting point for the removal of Trojan detection.
[2]	In this technique we are protecting the circuit against scan-chain attack by resetting the device when switching from normal mode to test mode.	Mode-reset countermeasure does not give complete protection against scan attacks.
[3]	In Built-in reseeding, area overhead is reduced.	Modifying the Circuit under Test(CUT) is not suitable for this because it affects performance and intellectual property.
[4]	Scan chain test is used to recover secret keys from the hardware implementation of DES.	This Scan chain test can acts as a attacking tool by the user to break the security in hardware and access secret keys.
[5]	Scan chain attack can acts as a gateway for the attackers to access the secret keys from hardware hence it is recommended to use some other testing methods and hence we move to Built-in self test.	It is very difficult to achieve low area overhead and low clock cycles at the same time. A trade-off is maintained between these constraints in this method.
[6]	Smart Controller can be used to eradicate scan attacks in a hardware because it is used to inspect the use of scan chain in a circuit.	It introduces a small area overhead.
[7]	In order to prevent scan attacks, adding anti-fuse on scan pins and blowing them after manufacturing is one such method.	Maintenance in this field id difficult and reduces the controllability and observability.
[8]	It enhances the efficiency of the secured authentication mechanism by reducing the	This method is used for small scale cannot be extended to hardware Trojan

	area overhead of the authentication secrets.	detection and IP protection.
[9]	This method has 100% fault coverage with no visible scan-chain and low area overhead.	It is very difficult to achieve low area overhead and low clock cycles at the same time. A trade-off is maintained between these constraints in this method.
[10]	In this method, the keys are obtained from noisy information for secured authenticationdata.	It has input-dependent ,random, and Computationally bounded Errors.
[11]	Extra cost in terms of area is very low due to reusing the embedded resources.	They require extra circuitry to implement and signature analysis and test pattern generation, which increases the area overhead.
[12]	IP protection For FPGA is done by using PUF, which cannot be duplicated thereby protecting IP from creating multiple copies of license keys.	It increases the area overhead since extra circuitry is added.
[13]	Masking, adding Pseudo Random Number Generator (PRNG) are the techniques which is used to avoid hacking in hardware.	It increases the test time of the circuit.
[14]	Multi-polynomial LFSR are used to generate test patterns which is used to increase the fault coverage for complex systems.	It increases the area overhead and test time of the circuit.
[15]	Insertion of DES IP, 4 shift spy Flip-flops are inserted between 198 flip-flops are used to reduce the scan chain attacks in the circuit.	It increases test time and test data volume of the circuit.

This table gives advantages and disadvantages of above 15 reference papers.

CONCLUSION

There are several ways of testing the circuit, where security is maintained. Scan-chain test is one of the testing method for testing the secure circuit, but it may act as a gateway for the attackers to access secret keys. Hence scan-chain test is not used for secure testing. Scan-chain free functional testing is an important aim for secure testing. Hence we go for other testing methods for secure testing and Built-in Self test (BIST) is used and it is one of the efficient method for testing the secure circuits. BIST has high fault coverage. There are various methods proposed for increasing the efficiency of BIST and if needed we can use a Smart Controller for monitoring the use of scan chain test.

REFERENCES

[1] Agrawal D, Baktir S, Karakoyunlu D, Rohatgi P, Sunar B (2007)Trojan Detection using IC Fingerprinting, IEEE Symposium onSecurity and Privacy (SP) pp 296–310.

[2] Ali SS, Said SM, Sinanoglu O, Karri R (2013) Scan Attack in Presence of Mode-Reset Countermeasures. IEEE International onlinetesting symposium (IOLTS) 230:231.

[3] Al-Yamani AA, McCluskey EJ (2003) Built-in reseeding for serialBIST. VLSI TestSymp: 63–68.

[4] Bo Y, Kaijie W, Karri R (2004) Scan-based Side-Channel Attack on Dedicated Hardware Implementations of Data EncryptionStandard, Proceedings of International Test Conference, pp 339–344.

[5] Cortez M, Roelofs G, Hamdioui S, Di Natale G (2014) TestingPUF-Based Secure Key storage Circuits Design, Automation andTest in Europe Conference and Exhibition (DATE), pp 1–6.

[6] Da Rolt J, Di Natale G, Flottes ML, Rouzeyre B (2013) A Smart test controller for scan-chains in secure circuits' .IEEE International On-line Testing Symposium (IOLTS):228–229.

[7] Da Rolt J, Di Natale G, Flottes ML, Rouzeyre B (2012) new security threats against chips containing scan chain structure.IEEE International Symposium on Hardware-Oriented Securityand Trust (HOST) p 110.

[8] Das A, Kocabas¸U, Sadeghi AR, Verbauwhede I, SadeghiAR, Verbauwhede I (2012) PUF-based Secure Test WrapperDesign for Cryptographic SoC Testing Design, Automation andTest in Europe Conference and Exhibition pp 866–869

[9] Di Natale G, Doulcier M, Flottes ML, Rouzeyre B (2010)Self-test techniques for crypto-devices. IEEE Trans VLSI Syst18:2.

[10] Dodis Y, Reyzin L, Smith A (2004) Fuzzy Extractors: Howto Generate Strong Keys from Biometrics and other NoisyData, Advances in Cryptology-EUROCRYPT vol. 3027, LNCS,Springer Berlin Heidelberg, pp 523–540.

[11] Doulcier M, Flottes ML, Rouzeyre B (2008) AES-based BIST:self-test, test pattern generation and signature analysis. IEEE Internationalsymposium on electronic design, Test & Applications, pp314–321.

[12] Guajardo J, Kumar SS, Schrijen GJ, Tuyls P (2007) FPGAIntrinsic PUFs and their Use for IP Protection. Workshopon Cryptographic Hardware and Embedded Systems (CHES):63–80.

[13] Hamdioui S, Di Natale G, van Battum G, Danger JL, SmailbegovicF, Tehranipoo(2014) Hacking and Protecting IC HardwareDesign, Automation and Test in Europe Conference and Exhibition,pp 1–7.

[14] Hellebrand S, Rajski J, Tarnick S, Venkataraman S, Courtois B(1995) Built-in test for circuits with scan based on reseeding ofmultiple-polynomial linear feedback shift registers. IEEE TransComput 44(2):223–233.

[15] Hely D, Bancel F, Flottes ML, Rouzeyre B (2006) A Secure Scan Design Methodology Design, Automation and Test in Europe Conference and Exhibition,pp. 1–2.