International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 6 –NOVEMBER 2014.

Performance of sheltered IC for exposure of Security Hacking Attacks by using Scan Based TPG

K.RAMESH[*1] and M.PURNASEKHAR[#2]

[*]*Student, Dept of Electronics and Communication, Nova College of Engineering and Technology, India*

[#]*Associate Professor, Dept of Electronics and Communication, Nova College of Engineering and Technology, India*

Abstract— Hardware development of cryptographic algorithms is subject to various attacks. It has been previously demonstrated that scan chains introduce for hardware testability open a back door to potential attacks. Scan based testing is one of the mainly used and powerful test technique since it provides full observability and controllability of the internal nodes of the IC. It has been previously demonstrated that scan chains introduced for hardware testability open a back door to possible attacks. Here, we propose a scan-protection scheme that provides testing facilities both at production time and over the course of the circuit's life. Here the underlying principles to scan-in both input vectors and expected responses and to compare expected and actual responses inside the circuit. Compared to regular scan tests, this technique has no impact on the quality of the test or the model-based fault diagnosis. It entails negligible area overhead and avoids the use of an authentication test mechanism.

Index Terms— security, testability, Design-for-testability (DfT), scan-based attack, test pattern generator

I. INTRODUCTION

Many aspects of our daily lives rely on electronic data interchange. Encryption algorithms are used to guarantee the confidentiality, integrity, and validity of these exchanges. These algorithms are implemented on dedicated hardware for performance optimization and to embed confidential information, which must be kept secret from illegal users.

Imperfect production processes of electronic devices lead to the need for manufacturing testing to sort out defective circuits from good quality ones, whatever be the aim application. This is even more relevant for secure circuits where a physical fault could jeopardize the security of the classified information.

However, the most common practice for testing digital devices relies on a scan-chains insertion that guarantees high fault coverage and thus an ultimate product quality, but open backdoors to security threats too. The "Scan attacks" described for instance in [1] and [2] utilize the access offered by scan chains' IOs for retrieving the secret key of an encryption core. These attacks rely on the possibility to observe the circuit's internal state while this state is related to the secret.

A common industrial practice to solve this security threat is to physically disconnect the scan chains after production testing by blow the fuses located at both ends of the scan chains. However, this solution impedes the testing of those devices require being tested after manufacturing. In particular, the correct performance of the secure circuits should be validated after the introduction of the secret key, which can be programmed at any time of the circuit's lifecycle. This secured information can indeed be owned by any circuit producer (e.g., designer, manufacturer, and system integrator) or user (e.g., reseller or final customer). In addition, scan disconnection stops any further analysis, e.g., diagnostic, or cannot be considered as an appropriate response to the scan attack if the connection can be reconstructed. In the literature, several solutions have thus been proposed to avoid disconnecting scan chains after manufacturing testing. However, the solutions are either expensive or not fully safe against latest scan attacks.

In this brief, we explain a new design-for-testability (DfT) architecture that eliminates the need to separate the scan chains. This approach is based on the concept of maintenance information. The test procedure consists in providing both the test vectors and expected test responses to the device-under-test (DUT) for an on-chip comparison.

Methods for the on-chip comparison of actual and expected test responses have already been explored in other contexts [3]–[6], mainly to lessen the test data volume to transfer from DUTs to test equipment. However, none of these solutions achieve the target security requirements since individual bit values stored in the scan chains can still be observed or deducted from observed data, thanks to the test circuitry.

Because testability features must not be implemented to the detriment of the security of the circuit, and vice versa, this brief also discusses test and diagnostic procedures with our DfT proposal, as well as security of the circuit with respect to attacks perpetrate on the test infrastructure.

Cryptography is the science of secure communication and information protection from unauthorized access. Cryptography enables communicating parties to exchange information securely over an insecure channel. Modern cryptography not only applies to secure communication, but

also has applications in software security, security of electronic devices (smart cards, RFIDs, memories, etc.), data protection (disk encryption), copyright protection (Digital Rights Management (DRM)) and more. Examples include RFID based access control systems, authenticating users for bank transactions using smart cards supporting cryptographic protocols, and full hard disk encryption employing symmetric-key cryptography. Cryptography as a technology can be used to provide the following security properties: confidentiality of data, data integrity, entity authentication of the sender and the receiver, and non-repudiation of sender and receiver, among others [89]. Various cryptographic primitives and protocols can help in attaining these objectives. Though the mathematical or theoretical strength of these primitives can be quite high, their implementations in hardware or software are prone to information leakages. Cryptographic implementations in hardware and software need to be protected against attacks aimed at revealing the secret information stored within them. Hardware attacks can be characterized as follows:

• Active or passive attacks: active attacks require the attacker to tamper or troubles bate the device internals (by probing, laser impingement, etc.) and derive the secret data from the observed response. Passive attacks require the attacker to only observe passively and infer the secret from the observed behavior by exploiting one or more physical characteristics of the device when it is in operation. Some of these characteristics include power consumption, electromagnetic radiation, execution timing, or the data coming in or out of the external interface.
• Invasive, semi-invasive or non-invasive attacks: invasive attacks require opening the device package and contact the electronic circuits inside; semi invasive attacks also require opening the device package but no contact to the internal circuits is needed, while non-invasive attacks do not require modification of the device package.

Scan has been generally accepted as the standard method of testing chips due to high fault coverage and relatively lower area overhead. Inserting scan-chains while designing the chip requires a few additional/multiplexed pins to the primary inputs/outputs to serve as the scan-enable, scan-inputs and scan-outputs. Internally, there is little impact on the design since the standard flip-flops (FFs) are replaced by scan flip-flops (SFFs) (i.e., flip-flops with an input multiplexer) which are then linked to one another creating a shift register (scan chain). An example of a scan chain is shown in the Figure 1.1. Scan-enable selects between functional and test mode operations. It controls each multiplexer, choosing between the normal mode input of the FF or the output of the previous SFF in the chain.

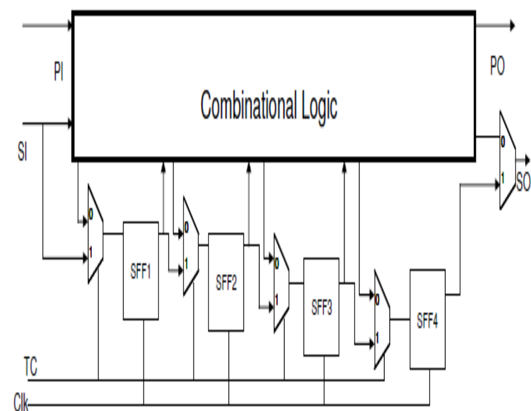


Figure 1.1: Scan chain DfT structure

II. SECURITY, TEST, AND DIAGNOSTIC ISSUES

This section discusses the security improvements related to the observation of a single pass/fail result as well as issues related to test and diagnosis.

A. Security Analysis

The role of the proposed Secure Comparator is to avoid the observation of SFFs containing secret information. If the result of the comparison was accessible at each clock cycle instead of each test vector, an attacker could easily observe the scan chain content by shifting in “000…000” on the *S*exp pin. Each bit-comparison would then validate that either the actual bit was “0” when Test Res = 1 and vice versa. On the contrary, with the proposed vector-wise comparison, the only way to retrieve the sensitive data information is to apply a brute-force attack by trying every possible response until Test Res is asserted. This attack would thus require 2#SFF attempts. If other attacks such as side-channel attacks [16] or faults attacks [17] are dreaded, the Secure Comparator has to be protected as the rest of the circuit. Even if countermeasures can lead to a large area overhead (e.g., [18]) their implementation concerns a very small part of the circuit.

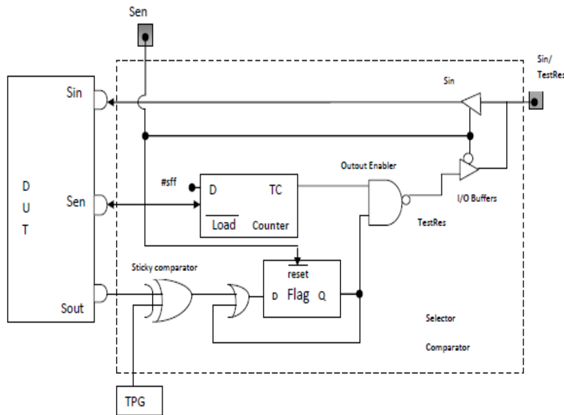


Fig 2 Proposed secure comparator Using Test Pattern Generator

B. Testability

The secure comparator does not impact the fault coverage. In fact, each test response is compared to the expected one as in a classical ATE-based test scheme. Therefore, the achievable fault coverage is not altered. Test time is not increased either, since the expected responses are scanned-in at the same time as the next input vector is scanned-in. Concerning the test of the Secure Comparator itself, any DfT technique controlled by the external ATE (e.g., a dedicated scan chain to test the counter of the Output Enabler) would jeopardize the overall security. Nevertheless, the Secure Comparator can be totally tested by using only its inputs (*S*en, *S*exp, *S*in, Test Res). We have identified a procedure to test all stuck-at faults no matter of the size of the Secure Comparator. This functional test involves the comparison of the actual SFF values with a partially matching, a fully un-matching, and a correct response. Moreover, it includes the application of a two un-matching responses without the intermediate capture cycle, and twice the execution of the capture cycle. This test procedure requires 6· (#SFF+1) clock cycles to provide 100% stuck at fault coverage.

A limitation of our technique is related to the presence of possible unpredictable values in the SFFs. Computing expected values for the on-chip comparison is indeed no longer possible. To fix this limitation, the Sticky Comparator should ignore the comparison result (and keep unchanged its flag) when *S*out is unknown. This can be implemented by providing an additional mask signal that is asserted when needed. However, an attacker must not be able to mask as many bits as wanted. In fact, if it were possible to mask all but one bit, it would be obvious to discover the value of each single bit in the scan response. This would reduce the complexity of the brute-force attack from exponential [O (2#SFF)] to linear [O (#SFF)]. Therefore, the number of masked bit (per test vector) must be limited to P such that a brute force attack on 2#SFF–P remains unfeasible. The extra cost to tolerate unknown values includes an extra pin for the mask, a log2 P counter to limit the number of masked bits and two logic gates. Fig. 2 shows a possible implementation.

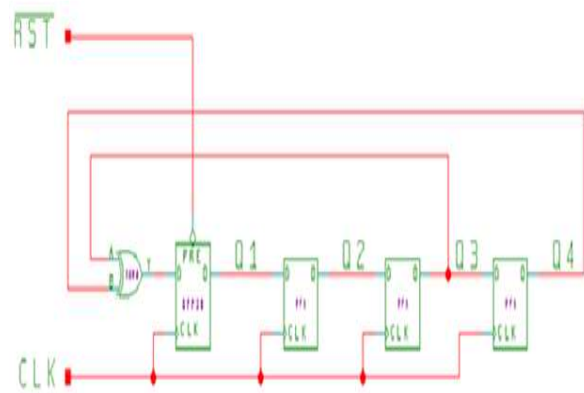
Test pattern generator

Linear Feedback Shift Registers (LFSRs)

Efficient design for Test Pattern Generators & Output Response Analyzers FFs plus a few XOR gates better than counter

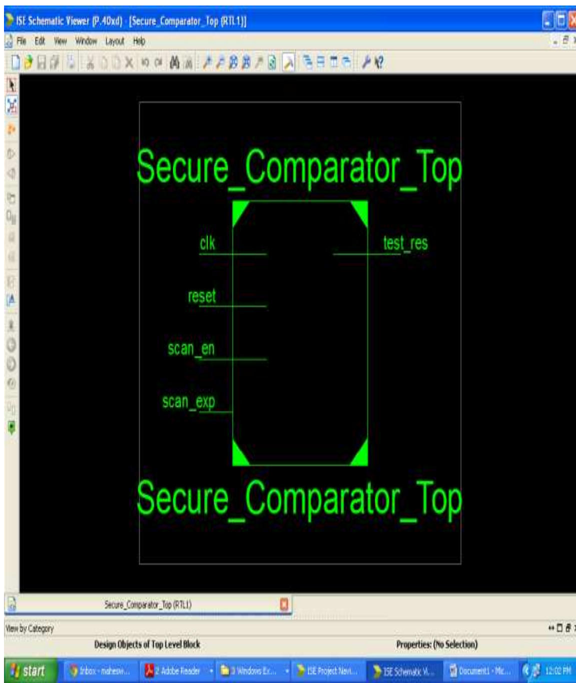
- Fewer gates
- Higher clock frequency
- Two types of LFSRs exterior Feedback, Internal Feedback
- High clock frequency

An LFSR generates periodic sequence must start in a non-zero situation, The maximum length of an LFSR sequence is 2n -1 does not generate all 0s pattern The characteristic polynomial of an LFSR generating maximum-length sequence is a primitive polynomial A maximum-length series is pseudo-random: number of 1s =number of 0s + 1 same number of runs of successive 0s and 1s 1/2 of the runs have length1 1/4 of the runs have length 2 (as long as fractions result in integral numbers of runs).

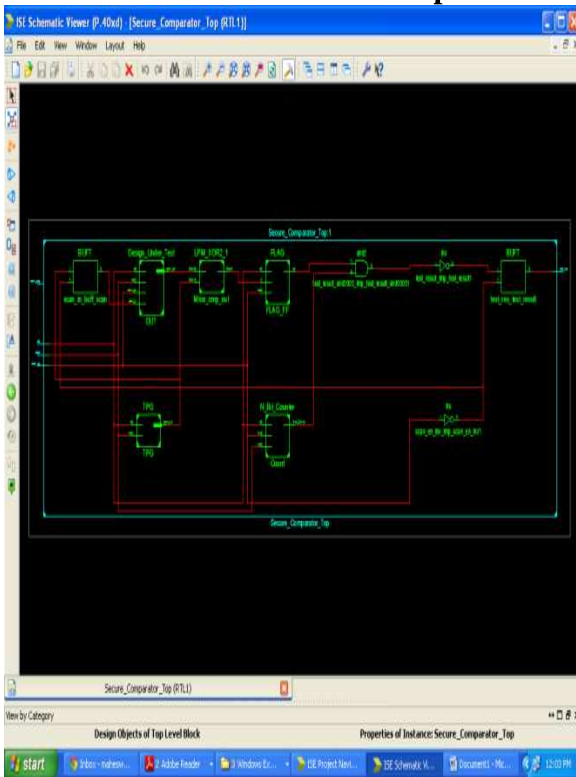


III. SIMULATION RESULTS

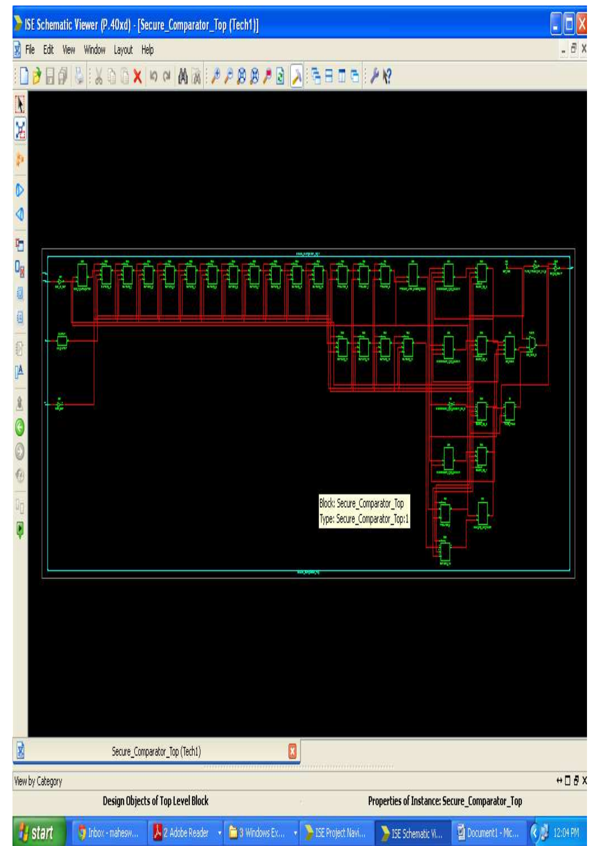
Block diagram



RTL Schematic Secure Comparator



Technology schematic



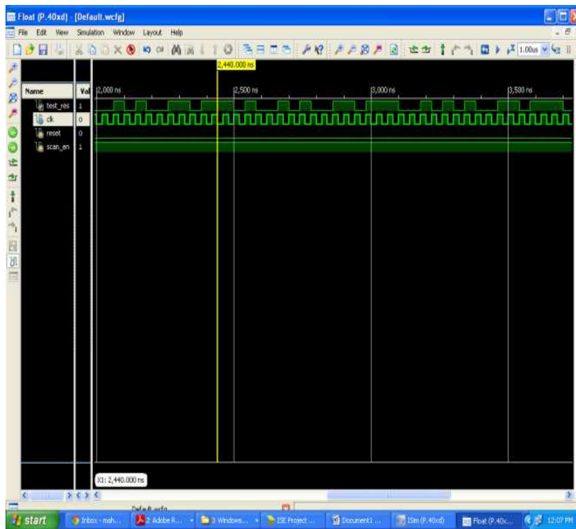
Design Summary

Secure_Comparator_Top Project Status (06/28/2014 - 11:55:22)			
Project File:	thwarting_extention.xise	Parser Errors:	No Errors
Module Name:	Secure_Comparator_Top	Implementation State:	Synthesized
Target Device:	xc3s500e-5pq208	•Errors:	No Errors
Product Version:	ISE 14.3	•Warnings:	2 Warnings (1 new)
Design Goal:	Balanced	•Routing Results:	
Design Strategy:	Xilinx Default (unlocked)	•Timing Constraints:	
Environment:	System Settings	•Final Timing Score:	

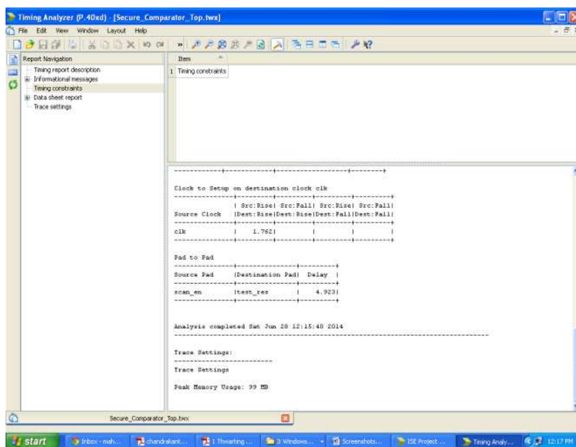
Device Utilization Summary (estimated values)			
Logic Utilization	Used	Available	Utilization
Number of Slices	15	4656	0%
Number of Slice Flip Flops	25	9312	0%
Number of 4 input LUTs	9	9312	0%
Number of bonded IOBs	4	158	2%
Number of GCLKs	1	24	4%

Detailed Reports					
Report Name	Status	Generated	Errors	Warnings	Infos
Synthesis Report	Current	Sat Jun 28 11:55:21 2014	0	2 Warnings (1 new)	1 Info (0 new)
Translation Report					
Map Report					
Place and Route Report					
Power Report					
Post-PAR Static Timing Report					
Bitgen Report					

Simulation Results



Delay Report



IV. CONCLUSION

Inserting scan into a secure design implies new approaches of the technique eventually; applying ones of these countermeasures has also proven that at a suitable cost, scan and security can live together. In this paper we do not give the expected outputs. But in the scan circuit to generate the expected values by using TPG. Here linear feedback circuit used for TPG (Test pattern generator). The proposed approach is based on the idea of withholding information. The idea is to compare test responses within the chip. Both input vectors and expected responses are scanned into the circuit and the compare between expected and actual responses is done at vector level. It does not provide information on the value of every individual scan bit for security purposes. In this paper we proposed a novel DfT technique for scan design to ensure security not including relying on costly test infrastructures to switch from mission to test modes.

REFERENCES

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

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

[3] Y. Wu and P. MacDonald, “Testing ASICs with multiple identical cores,” IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 22, no. 3, pp. 327–336, Mar. 2003.

[4] K. J. Balakrishnan, G. Giles, and J. Wingfield, “Test access mechanism in the quad-core AMD opteron microprocessor,” IEEE Design Test Comput., vol. 26, no. 1, pp. 52–59, Jan. 2009.

[5] D. Andreu, “System and method for wirelessly testing integrated circuits,” U.S. Patent 0 244 814, Oct. 6, 2011.

[6] Goessel, “On-chip evaluation, compensation and storage of scan diagnosis data,” IET Comput. Digit. Tech., vol. 1, no. 3, pp. 207–212, 2007.

[7] G.-M. Chiu and J. C.-M. Li, “A secure test wrapper design against internal and boundary scan attacks for embedded cores,” IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 20, no. 1, pp. 126–134, Jan. 2012.

[8] K. Rosenfeld and R. Karri, “Attacks and defenses for JTAG,” IEEE Design Test Comput., vol. 27, no. 1, pp. 36–47, Jan. 2010.

[9] C. J. Clark, “Anti-tamper JTAG TAP design enables DRM to JTAG registers and P1687 on-chip instruments,” in Proc. IEEE Int. Symp. Hardw.-Oriented Security Trust, Jun. 2010, pp. 19–24.

[10] D. Hely, F. Bancel, N. Berard, M. L. Flottes, and B. Rouzeyre, “Test control for secure scan designs,” in Proc. IEEE Eur. Test Symp., May 2005, pp. 190–195.

[11] D. Hely, M.-L. Flottes, F. Bancel, B. Rouzeyre, N. Berard, and M. Renovell, “Scan design and secure chip [secure IC testing],” in Proc. IEEE Int. On-Line Test. Symp., Jul. 2004, pp. 219–224.

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

[13] H. Fujiwara and M. E. J. Obien, “Secure and testable scan design using extended de Bruijn graphs,” in Proc. Asia South Pacific Design Autom. Conf., 2010, pp. 413–418.

[14] J. Da Rolt, G. Di Natale, M.-L. Flottes, and B. Rouzeyre, “New security threats against chips containing scan chain structures,” in Proc. IEEE Int. Symp. Hardw.-Oriented Security Trust, Jun. 2011, pp. 110–115.

[15] L. Chunsheng and Y. Huang, “Effects of embedded decompression and compaction architectures on side-channel attack resistance,” in Proc. IEEE VLSI Test Symp., May 2007, pp. 461–468.

[16] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” in Proc. Int. Cryptol. Conf. Adv. Cryptol., 1999, pp. 388–397.

[17] P. Dusart, G. Letourneux, and O. Vivolo, “Differential fault analysis on A.E.S,” in Applied Cryptography and Network Security, vol. 2846. New York, NY, USA: Springer-Verlag, 2003, pp. 293–306.

[18] A. Moradi, T. Eisenbarth, A. Poschmann, C. Rolfes, C. Paar, M. T. M. Shalmani, and M. Salmasizadeh, “Information leakage of flip-flops in DPA-resistant logic styles,” in Proc. IACR Cryptology ePrint Archive, 2008, pp. 188–188. 2008, pp. 188–188.