A smart test controller for scan chains in secure circuits

Jean Da Rolt, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre

A Smart Test Controller for Scan Chains in Secure Circuits

Jean Da Rolt, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre
LIRMM – Université Montpellier II/CNRS
Montpellier, France

***Abstract*—Structural testing is one important step in the production of integrated circuits. The most common DfT technique is the insertion of scan-chains, which increases the observability and the controllability of the circuit's internal nodes. Nevertheless, malicious users can use the scan chains to observe confidential data stored in devices implementing cryptographic primitives. Therefore, scan chains inserted in secure ICs can be considered as a source of information leakage. Several countermeasures exist to cope with this type of problem. However, they either introduce high area overheads or they require modifications to the original design or the test protocol. In this paper we present a smart test controller that is able to prevent all known scan attacks. The controller does not require any additional signals, it is transparent to the designer and it does not require any modifications of the test protocol and procedure. Moreover, it introduces a very small area overhead.**

Keywords—Scan-based Attacks; Secure Test Controller

I. INTRODUCTION AND STATE-OF-THE-ART

Testing digital ICs is essential to sort defective circuits, thus ensuring the product's quality. However, nowadays designs require Design-for-Testability (DfT) structures to be inserted in order to enhance the testability: achieving high fault-coverage and precise diagnostic. The most common DfT technique is the insertion of scan-chains, which allow shifting in test vectors and shifting out test responses. These structures increase the observability and controllability of internal nodes, by allowing internal states to be reached easily. Moreover, it enables the generation of efficient test vectors.

Although scan chains are present in most designs, malicious users can exploit this increase of observability of internal nodes. In the case of secure circuits that rely on encryption keys, an attacker may shift out the information stored in the flip-flops by using the scan chains and exploit the obtained data to retrieve the secret key. Therefore scan chains impose a security drawback, often described as scan-based attacks.

Several attacks have been described in the literature. Initially, scan-based attacks targeted circuits with single and multiple scan chains. For instance, attacks on the Data Encryption Standard (DES) [1], Advanced Encryption Standard (AES) [2], stream ciphers [3], RSA [4] and Elliptic Curve Cryptosystems (ECC) [5] have been proposed. Lately, advanced attacks have been proposed in order consider more complex DfT structures such as response compactors, pattern decompressors and mask decoders, which impose an intrinsic difficulty to analyze the internal data and then to retrieve the secret key [6]. All these attacks rely on the observation of the internal nodes but not on the possibility of controlling internal states, therefore they are considered as "observability attacks".

In order to cope with these attacks, countermeasures have been proposed. For instance in [7] authors show that AES implementations can be easily self-tested thus achieving 100% fault coverage. However not all circuits can achieve high fault coverage with pseudo-random patterns. A common technique adopted by smart-card providers is to disable test circuitry after receiving the manufacturing test by blowing the anti-fuses located at the ends of the scan chain. It permits a full scan and high quality diagnosis. However, once the circuit is packaged, in-field maintenance and debugging are compromised. Another solution is to ensure the confusion of the stream shifted out from the scan outputs for unauthorized testers by scrambling the scan chain bits [8]. However this technique requires a circuit to detect authorized users and to allow them to test the circuit without any scramble.

To cope with the problem of in-field testability, authors in [9] proposed to use internal test responses comparison. The underlying principle is to scan-in both input vectors and expected responses and to compare expected and actual responses within the circuit. This technique has no impact on the quality of the test but it is limited to the diagnosis of only modeled faults. Another improvement is proposed in [2] by defining two modes: secure and insecure. After any kind of power-off incident, the circuit goes into insecure mode where the secret key is not loaded. Switching from insecure to secure mode implies the loading of the secret key (stored in a mirror-register outside of the scan chain) and the test is then disabled. This scheme works properly although it requires specific design requirements and it is not compliant with test standards.

In this paper we present a smart test controller that is able to prevent all known scan attacks. Conversely to already proposed methods, the controller does not require any additional signals, it is transparent to the designer and it does not require any modifications of the test protocol and procedure.

II. THE SMART TEST CONTROLLER

The proposed test controller will exploit the following observations:

- The scan-based test of digital circuits follows a predefined scheme: input vectors are shifted-in via the scan-in (with scan-en asserted), one functional clock cycle is applied (also known as capture cycle, with scan-en not asserted), and output responses are shifted-out via scan-out (while, at the same time, the next input vector is shifted in). When delay faults are targeted and the Launch-On-Capture technique is used, 2 capture cycles may be required.
- Known attacks are based on the fact that the circuit is first run in normal mode for a certain number of clock cycles in order to bring the circuit to a desired state (for instance in the AES, the circuit is run up to the first

978-1-4799-0664-2/13/$31.00 ©2013 IEEE

encryption round). Then the scan chain is used to observe the state of the circuit in that moment.

The principle of the proposed controller relies on the masking of the scan-out signal in such a way that it does not deliver any sensitive data until the whole scan chain is first freshen. Fig. 1 sketches the Circuit Under Test (CUT) connected to the proposed smart test controller, while Fig. 2. details its finite state machine. The controller reads the scan-en signal and, based on its value, it forces to 0 the OUT_en signal that drives a 2-bit AND gate whose other input is the CUT's scan-out.

The controller is automatically armed at power-on (*Normal* state). Once it is armed, OUT_en is forced to 0 in order to filter any shift-out operations. In this initial state, a down-counter is set to #L, i.e., the number of scan flip-flops in CUT. After #L consecutive clock cycles with scan-en asserted (*Flushing* state), the controller is disarmed. During the Flushing state, the controller is still armed (OUT_en=0) to prevent the observation of the scan chain content after a normal execution (i.e. scan attacks). After disarming the controller, OUT_en is set to 1 so that any scan operation is performed without masking. The controller allows one or two capture cycles (*Stuck-At-Capture* and *Delay-Capture* states) without re-arming OUT_en. If more than 2 capture cycles are executed, the controller goes back to the Normal state. The Shifting state allows shifting input vectors into the scan chain. The down-counter is not used in this state because the sensible data already disappeared from the scan chains. In this way, the controller enables the test of the scan-chain itself where longer than #L sequences are shifted without capture cycles.

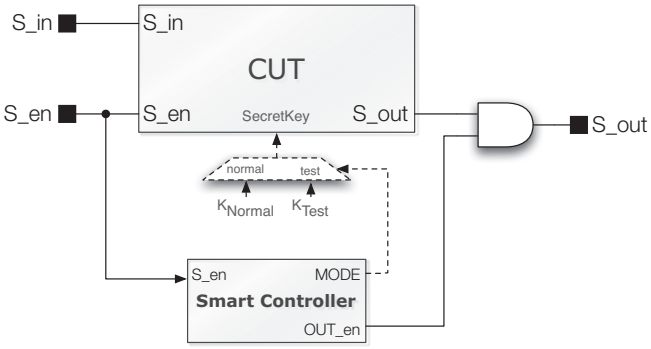

Fig. 1. The Smart Controller within the original design

As proposed in [2], the controller allows identifying two execution modes: normal and test (*MODE* signal). Nevertheless, it does not require any additional signal to force one of the two modes since the detection of the mode is performed automatically: the *Normal* state is the normal mode, while all the other states define the test mode. the controller automatically detects. The execution mode may be possibly used when two secret keys are used (as shown with dotted lines in Fig. 1).

The security of secure devices using the proposed controlled is guaranteed by the fact that it is not possible to bring the circuit in a desired state and then to shift out the content of the scan flip-flops. Indeed, the first time the scan chain is shifted out, the scan-out signal is forced to 0 for #L clock cycles. After this phase, the circuit can be fully tested. However, as soon as the attacker tried to run more than 2 functional clock cycles (to possibly reach the desired state), the controller would be armed again and the next scan-out operation would be masked.

This controller can be inserted into the design at the very end of the design, thus not perturbing the overall design flow. It is also transparent to the tester because it does not modify the classical and standard test procedures. The area introduced by the controller is meaningless.

REFERENCES

[1] B. Yang, K. Wu, R. Karri, Scan based side channel attack on dedicated hardware implementations of Data Encryption Standard, Proceedings of IEEE International Test Conference. 2004 pp. 339- 344.

[2] B. Yang, K. Wu, R. Karri, Secure Scan: A Design-for-Test Architecture for Crypto Chips, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. 25 (10) (2006) 2287-2293.

[3] Y. Liu, K. Wu, R. Karri, "Scan-based Attacks on Linear Feedback Shift Register Based Stream Ciphers," In ACM Transactions on Design Automation of Electronic Systems (TODAES), 2011, 16, 2, 1-15.

[4] R. Nara, K. Satoh, M.Yanagisawa, T. Ohtsuki, N. Togawa, "Scan-based side-channel attack against RSA cryptosystems using scan signatures," IEICE Transaction on Fundamentals of Electronics, Communications and Computer Sciences, 2010, E93-A, 12, 2481-2489.

[5] R. Nara, N. Togawa, M.Yanagisawa, T. Ohtsuki, "Scan-based attack against elliptic curve cryptosystems". 15th IEEE Asia and South Pacific Design Automation Conference (ASP-DAC'10). 407-412.

[6] J. Darolt, G. Di Natale, M-L. Flottes, B. Rouzeyre, "Are advanced DfT structures sufficient for preventing scan-attacks", IEEE VLSI Test Symposium 2012 (VTS'12), pp. 246-251, DOI: 10.1109/VTS.2012.6231061

[7] G. Di Natale, M. Doulcier, M. L. Flottes, B. Rouzeyre, "Self-Test Techniques for Crypto-Devices, ", IEEE Transaction on VLSI Systems, pp. 1-5, 2009, DOI: 10.1109/TVLSI.2008.2010045

[8] D. Hely, F. Bancel, M.-L. Flottes, B. Rouzeyre, "Secure scan techniques: a comparison". In Proceedings of the 12th IEEE International On-Line Testing Symposium (IOLTS'06). 119-124

[9] J. Darolt, G. Di Natale, M-L. Flottes, B. Rouzeyre, "Thwarting scan-based attacks on secure-ICs with on-chip comparison", IEEE Transaction on VLSI Systems,, DOI 10.1109/TVLSI.2013.2257903

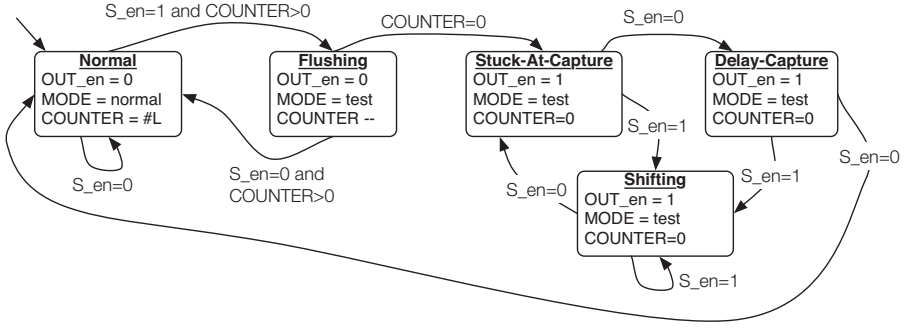

Fig. 2. Finite State Machine of the Smart Controller