Scan design and secure chip [secure IC testing]

David Hely, Marie-Lise Flottes, Frédéric Bancel, Bruno Rouzeyre, Nicolas Berard, Michel Renovell

Scan Design and Secure Chip

David Hély[1], Marie-Lise Flottes[2], Frédéric Bancel[1], Bruno Rouzeyre[2], Nicolas Bérard[1], and Michel Renovell[2]

[1]ST Microelectronics
ZI de Rousset BP 2
F-13106 Rousset CEDEX, France
david.hely@st.com

[2]LIRMM – UMII
161 rue Ada
F-34392 Montpellier, France

Abstract

Testing a secure system is often considered as a severe bottleneck. While testability requires to an increase in both observability and controllability, secure chips are designed with the reverse in mind, limiting access to chip content and on-chip controllability functions. As a result, using usual design for testability techniques when designing secure ICs may seriously decrease the level of security provided by the chip. This dilemma is even more severe as secure applications need well-tested hardware to ensure that the programmed operations are correctly executed. In this paper, a security analysis of the scan technique is performed. This analysis aims at pointing out the security vulnerability induced by using such a DfT technique. A solution securing the scan is finally proposed.

1. Introduction

Secure cryptographic hardware is intensively used in order to perform confidential operations (e.g. financial transactions, personal authentication...) [Tho97], [Rag03]. During these operations, data (plaintext) is converted (encrypted) into code (ciphertext) by combining it with a small piece of information (key). As a consequence such chips are designed so that attackers have serious difficulties in uncovering on-chip content or using it without the required permission. Thus, in order to prevent security failures, designers are introducing more and more tamper-resistant hardware in such a way that the secure IC fulfils the following properties [Haf91]:

- It never permits access to plain-text, partially encrypted text or unencrypted keys
- System failure (such as hardware damage) is immediately detected and indicated [Bon01].
- Each attempt of unauthorised access is immediately detected, keys and sensitive data are erased, and system operation is inhibited (the transaction is cancelled, and none others are possible).

Moreover, a secure design implies high quality test processes in order not to deliver a supposedly "secure chip" on which secure operations may fail. High quality testing of security hardware is thus primordial to ensure an acceptable level of security. Whilst a secure design aims at reducing controllability and observability to a minimum, an easily testable one should be very controllable and observable. Thus, testability and security may be difficult to associate [Bon93], even if the second requires the first. Introducing on-chip testability features in a secure design may decrease significantly the degree of security offered by the on-chip circuitry. This paper presents the risks encountered when inserting testability features into a secure design and proposes a new architectural solution for improving security in scan designs. Section 2 discusses the potential vulnerability of secure systems due to design for test principles. Section 3 presents a vulnerability analysis of scan technique. In section 4, current countermeasures against DfT vulnerability are discussed. Section 5 presents a new scan design for secure chip.

2. General vulnerability induced by DFT

When analysing the vulnerability, which may be induced by the design for testability techniques, we are faced with two different issues. Indeed we can consider the vulnerabilities from two different points of view:

- The controllability point of view: controllability-induced vulnerability
- The observability point of view: observability-induced vulnerability

2.1. Controllability

Design for controllability techniques aim at improving the application of test data from outside to the on-chip circuitry. However a test access mechanism is also a potential path for introducing corrupted data into the chip. A design for controllability technique could be used for controlling some on-chip security blocks. For instance, for testability purpose, it may be possible to deactivate security features such as memory firewall or on-chip data encryption. Thus using such controllability capability, a

hacker may decrease the on-chip security level by disabling some security block. Controllability may also facilitate 'side channel attacks' such eavesdropping attack, which consists in deducing secret information from accessible sources. For instance, the various instructions or data processed by the chip cause variations in power consumption, then using statistical analysis on the power traces [Koc99] it is possible to identify what is being processed on chip. Controlling the chip clock facilitates the analysis of power trace and thus increases the effectiveness of such an attack [Hes00]. In test mode, the clock is controllable from external pad in order to synchronise the chip and the tester together, creating thus an opportunity for the hacker to control it also.

2.2. Observability

The observability enhancement offered by design for testability technique also induces security hazard. During test operation, the chip is configured so that it is possible to observe on-chip data resulting from applied test patterns. A common attack against cryptographic equipment consists in injecting error during the run of a cryptographic algorithm and to compare the result with a fault safe one. Iterating this process, cryptanalysts are able to retrieve secret key of secret key algorithm. Increasing data observability may make such an attack more easily realisable thanks to the increase of accessible data, which permits to analyse not only primary output but also some internal registers.

3. Security vulnerability with the scan Technique

3.1. Observability-induced vulnerability

A scan circuitry links all the storage elements of a design, or part of them, to realise a large shift register the so-called scan chain. A major vulnerability of the scan designs relies on the fact that activating the scan mode provides full controllability and observability of the memory elements included in the scan chain [Mue02]. Namely, during the scan mode, all the data present in the scan chain are shifted out and can thus be observed at the extremity of the scan chain: the scan-out pin. In other words, the observation of only one node in the circuit (the last flip-flop's output in the scan chain) provides full observation of all the data stored into the scan flip-flops. A signal monitoring attack is thus simplified. Indeed, let consider the hardly realisable attack which consists in probing a data register which contains for instance a secret key. This attack requires placement of as many probes as the register bit width. Here no matter the bit-width of the register, only two probes are sufficient. The attack requires one probe on the scan-out signal in order to observe the data flow, and another one on the scan-enable signal in order to control the shift operation (figure 1).

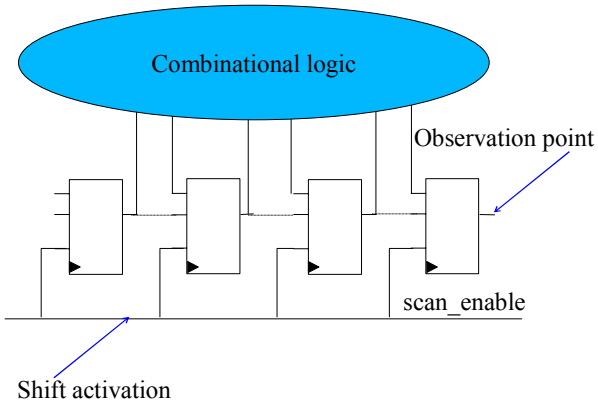

Figure 1: probing attack

A new attack based on the differential fault analysis [Bih97] concept can also be imagined using scan circuitry. The hacker can abuse the scan circuitry to shift out the chip content during a cryptographic operation. By iterating this process, the hacker can have the on-chip content of the chip at different times of the cryptographic operation. Then analysing these different 'snapshots' bit to bit, identification of the registers dedicated to cryptographic algorithm becomes possible. Then by knowledge of the algorithm, data reconstruction leading to secret key is realizable [Sko02].

3.2. Controllability-induced vulnerability

Scan circuitry can also be exploitable in order to perform a "control-oriented" attack on a secured chip (figure 2). A hacker can use the scan circuitry in order to introduce data to a part of the chip, which is not usually accessible to the user for security reasons. For instance, consider a flag register whose purpose is to indicate if the user has the right to access a certain zone of a memory. If this flag is part of the scan chain, the desired value can be easily set into this flag using the scan-in shift operation. The desired functionality is then activated when the chip is switched back to the functional mode.

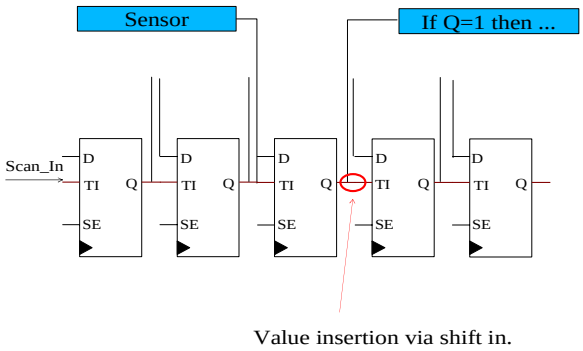

Figure 2: control-oriented attack

Fortunately, the drawback of such an attack is that when inserting a value into the Nth element of a scan chain, all the N-1 elements preceding the Nth element are impacted. It is thus extremely difficult to control the value of only one element without disturbing the other storage elements. The modification of the values stored into these N flip-flops may hopefully provoke a malfunction (i.e. for instance place the CPU into an illegal state), which in secure design is immediately detected and often induces a full-chip reset. Moreover, such a precise attack implies pre-required information on the scan architecture as the position of the target register into the scan chain. Despite this, the hacker has still the possibility to perform a kind of random attack which consists in shifting in random data with the idea of disabling security features. The most sensitive attack due to this controllability opportunity may be the fact that a new channel to perform fault injection is provided through the scan-in pin. All the circuitry added in order to make the chip scannable is at least as sensible to fault injection as the original circuitry. Then inserting scan statically increases the sensitivity to such attack.

3.3. Side effect

Design modifications implied by the scan insertion introduce other vulnerabilities, namely concerning the control of asynchronous signal used for security purpose. Asynchronous signals are commonly used for security in order to instantaneously reset the chip in case an anomaly is detected. However, for ATPG purpose, all asynchronous signals should be controlled by a "Test_Mode" signal [Jar00]. When scan data are shifted in and out of the design under test, the asynchronous reset and clear pins of storage cells must be held in an inactive state. Thus, when the test mode is active, all the asynchronous signals are disabled, which introduces a real vulnerability since the reset designed to protect the data is no longer effective. Attacks requiring to inhibit the reset of chips are simplified since the test mode signal is much more accessible than an asynchronous reset signal generated by combinational logic.

4. Existing countermeasure

A common practice concerning secure IC is to blow test circuitry [Sou93] after production test. This technique consists in disabling the test mode activation, so that after production test, only a restrictive end-user mode is accessible. Actually, these fuses configure the chip either in test mode (i.e. all the test functions are available) or end user mode. This technique, broadly used in the smart-card community, guarantees to the chip maker that the chip secrecy will not be abuse using the chip as a test engineer could do. In order to overcome such a protection, chip modification is necessary to either bypass the configuration or rebuild the fuse. Such an attack becomes then hardly realizable since such fuses are often deeply hidden in the chip and thus hardly accessible [Kuh99].

Concerning the particular case of scan technique, in [Mue02], the authors propose to make the SCAN path unusable by interrupting the SCAN chain at a majority of locations by means of fuses as EEPROM fuses for instance. With this solution, the SCAN chain is no more usable from outside, since only small scan chain segments remain on-chip. Most of the vulnerabilities presented in section 3 are inhibited with such a protection. However "probing attack" remains possible on the small segments present between the fuses. Moreover, the main drawback of this countermeasure relies on the fact that in order to be efficient against brute attack, many fuses would be necessary. This solution is unfortunately not acceptable for designs for which area is a major concern. Finally, such techniques make impossible all opportunity of diagnosis in case of chip return after the production step.

5. Scan chain scrambling

5.1. Motivations

The following countermeasure, the so-called scan chain scrambling, consists in making the analysis of data stolen via the scan chain hardly realizable. The major risk induced by the scan chain remains on the possibility of on chip data analysis by shifting the chain during cryptographic operations. The hazard is real if the hacker is capable of shifting the scan chain several time so that data analysis is possible by comparing the different shifting results.

We propose to introduce a new module, the scan chain scrambler (figure 3), that controls the scan chain elements order such a manner that:

- When the scan mode has been securely reached (before the fuses are blown and after a strong authentication for instance), the scan chain elements order is fixed to a predetermined order.
- When the chip is not in test configuration, the scan

chain elements order changes at a given frequency.

Retrieving secret key or data becomes then much more difficult, since data analysis by comparing scan chain out data cannot be performed directly. The scan chain (or sensitive part of it) is divided into small segments, each segments are connected together through the scrambler, which manages their order in the chain (figure 6).

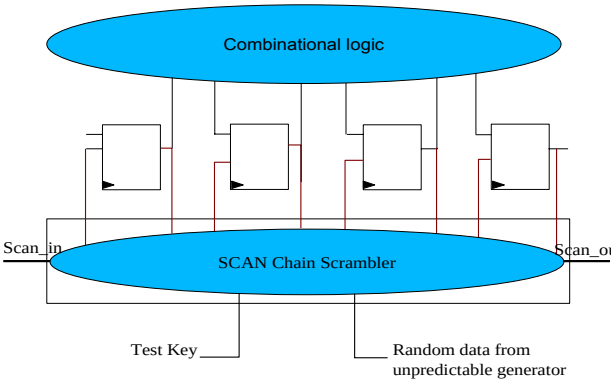

Figure 3: Scan chain scrambling

For instance let's consider a scan chain divided into 8 segments. These segments are connected together through the scan chain scrambler, which can either order them in a fix configuration or a random configuration. Figure 4 shows the element order at two different times when the test mode is not active. Let's assume the hacker needs n shifting out of the chip at different times of the cryptographic process.

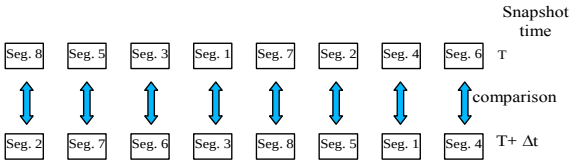

Figure 4: Segment order at two different instants

At time t, the segments order is [8, 5, 3, 1, 7, 2, 4, 6]. The scan chain is unloaded by activating the scan_enable signal either by brute attack or by corrupting the test controller. In order to analyse the data, successive unloads are necessary, at different times. So the hacker unloads the chain one more time at time t+dt, but at this time the order is [2, 7, 6, 3, 8, 5, 1, 4]. Comparing data of the two unloads becomes then much more difficult since comparison bit to bit has no sense here.

5.2. Implementation

In order to perform such scrambling a multiplexer is inserted between scan chain segments. The test input of the i th segment is fed by the multiplexer output; the multiplexer data in can either come from the (i-1) th segment (in test mode) or from one of the segments connected to this multiplexer through the scrambler (figure 5).

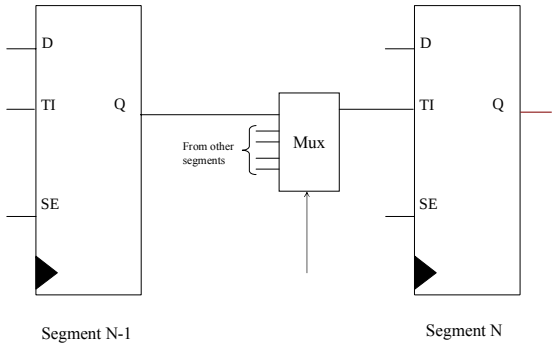

Figure 5: Segment connexion

A scrambling controller generates the control signals of the multiplexers inserted between the scan chain segments. During the test mode, a test key allows to certify the validity of the mode of operation. The scrambler controller reads this key and generates adequate control signals in order to connect the scan chain segment in the appropriate and fixed order. In any other mode of operation, or when the test key is not valid, the scrambling controller sends random values to the multiplexer control inputs.

Figure 6 shows a possible simplified implementation, the bold path corresponds to the scan path used in test mode. Between the four segments (here only one scan cell per segment), two-to-one multiplexers are inserted. In the "segment connexion block", the multiplexers are connected together so that the ith element is fed either by the (i-1)th or the (i+1)th combined with other segments (dot line). The scan path is fixed when the test mode is activated otherwise segments connexion is made random following the unpredictable number generator, which commands the multiplexers.

5.3. Trade-off efficiency versus cost

The protection relies on the scan chain data scrambling, thus in order to improve the scrambling it is necessary to decrease the segment length i.e. to increase the number of segments. Decreasing the segment length will increase security since when the scrambling is active; it is hardly likely to find long bit sequence corresponding to the same flip-flops comparing two shift-outs.

Nevertheless, decreasing the segment length can have a non negligible impact on the design. First concerning area, increasing the number of segments will require more logic cells to manage connexions between them. The routing constraints will also be more difficult to reach since scan dedicated nets will increase with the segments number. Last of all, during scan insertion, a new step is required in order to define and specify the different segments, which needs more attention than standard scan insertion.

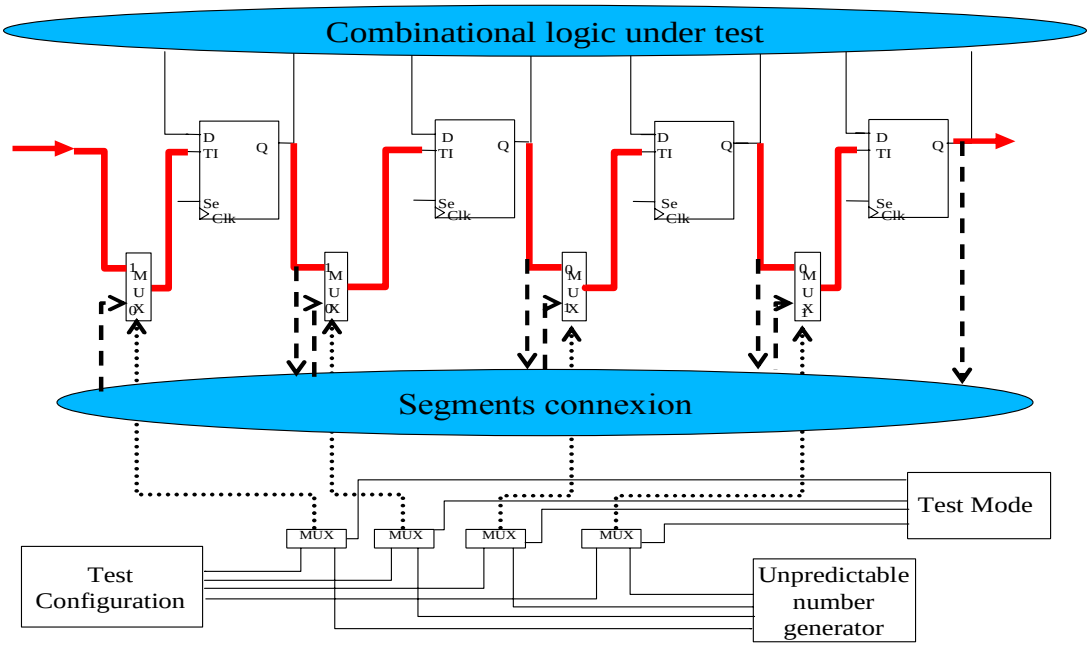

Figure 6: scan chain scrambling implementation

6. Discussion and conclusions

In this paper, scan induced vulnerabilities have been presented. It has been shown that introducing such a DfT technique into secure chip is not without risks. In order to improve existing countermeasure, scan chain scrambling can be a potential solution. This solution benefits from the fact that at the opposite of other solutions, this one still offers diagnosis capability since the test circuitry is not irremediably disabled after production.

Acknowledgements

We are very grateful for the helpful discussions with Director Laurent Sourgen (ST Microelectronics).

References

[Bih97] E. Biham and A. Shamir, "Differential Fault Analysis of Secret Key Cryptosystems ", CRYPTO '97, pp. 156-171, 1997

[Bon01] "On the importance of checking cryptographic protocols for faults" by D. Boneh, R. DeMillo, and R. Lipton. Journal of Cryptology, Springer-Verlag, Vol. 14, No. 2, pp. 101--119, 2001.

[Bon93] H. Bonnenberg, "Secure Testing of VLSI Cryptographic Equipment", ETH Zurich, Series in Microelectronics vol.25

[Gan01] K. Gandolfi, C. Mourtel, F. Olivier "Electromagnetic Analysis: Concrete Results", CHES 2001, vol. 2162 of Lecture Notes in Computer Science, pp. 251-261, Springer-Verlag, 2001.

[Haf91] K. Hafner, H.C. Ritter, T.M. Schwair, S. Wallstrab, M. Depperman, J. Gessner, S. Koesters, W-D. Moeller and G. Sandweg. "Design and Test of an Integrated Cryptochip" IEEE Design & Test, pages 6-17, December 1991

[Hes00] E. Hess, N. Janssen, B. Meyer, T. Schütze "Information Leakage Attacks Against Smartcard Implementations of Cryptographic Algorithms and Countermeasure: a Survey" in Proc. Eurosmart Conference, pp 55-64, June 2000

[Jar00] Ken Jaramillo and Subbu Meiyappan, Philips Semiconductors, “10 tips for successful design: part one” -- *EDN*, 2/17/2000

[Koc99] P. Kocher, J. Jaffe, B. Jun "Differential Power Analysis". Advances in Cryptology--CRYPTO'99, LNCS 1666 (1999), 388- 397

[Kuh99] M.G. Kuhn, O. Kommerling, "Design principles for tamper resistant smart-card processors", USENIX Workshop on Smart-card Technology Proceedings, Chicago Illinois, pp9-20. May 10-11 1999

[Mue02] D. Mueller, United States Patent, "Method of protecting a circuit arrangement for processing data". US 2002/0087284

[Rag03] A. Raghunathan, S. Hattangady, J-J. Quisquater "Securing Mobile Appliances: New Challenges for the System Designer", Design Automation and Test in Europe, 2003, 2003 pages 176-181

[Sko02] Sergei P. Skorobogatov, Ross J. Anderson: "Optical Fault Induction Attacks", Cryptographic Hardware and Embedded Systems Workshop (CHES-2002), San Francisco, CA, USA, 13-15 August 2002

[Sou93] L. Sourgen, US Patents 638459, "Security Locks for Integrated Circuits"

[Tho97] J.-P. Thomasson, L.Baldi "Smartcards: portable security" Proceedings, Second Annual IEEE International Conference on Innovative Systems in Silicon, pp 259 -265, 8-10 Oct. 1997.