Ensuring High Testability without Degrading Security

Marie-Lise Flottes, Giorgio Di Natale, Paolo Maistri, Bruno Rouzeyre, Régis Leveugle

▶ **To cite this version:**

Marie-Lise Flottes, Giorgio Di Natale, Paolo Maistri, Bruno Rouzeyre, Régis Leveugle. Ensuring High Testability without Degrading Security. ETS: European Test Symposium, May 2009, Seville, Spain. lirmm-00407163

HAL Id: lirmm-00407163

https://hal-lirmm.ccsd.cnrs.fr/lirmm-00407163

Submitted on 13 Feb 2015

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Ensuring high testability without degrading security

Embedded Tutorial on "Test and Security"

G. Di Natale, M.-L. Flottes, B. Rouzeyre
Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier (LIRMM)
Université Montpellier II / CNRS UMR 5506
Montpellier, France
{dinatale, flottes, rouzeyre}@lirmm.fr

Abstract—**Cryptographic algorithms are used to protect sensitive information when the communication medium is not secure. Unfortunately, the hardware implementation of these cryptographic algorithms allows secret key retrieval using different forms of attacks based on the observation of key-related information: physical information (side-channel attacks), faulty behaviors (fault-based attacks), or internal states (DFT-based attacks) for instance. Dedicated design for security techniques have been proposed so far, ranging from the development of specific cell libraries to the implementation of extra functions for preventing the leakage of useful information for key identification. On the other hand, users can expect high quality product for secure applications and this expectation requires the development of test solutions for every component of the secure device. However, testing those devices faces a double dilemma: (i) how to test and, possibly, develop design-for-testability schemes providing high testability (high controllability/observability) while maintaining high security (no leakage), (ii) how to provide high security using dedicated design rules while maintaining high testability. This tutorial will address these issues presenting the security weaknesses generated by classical DFT techniques, pros and cons of security-dedicated DFT, BIST and Fault tolerance solutions, and impact of design for security techniques on testability**

Keywords: BIST, DFT, secure systems, cryptographic cores.

I. INTRODUCTION

Many secure systems such as smartcards include hardware implementation of symmetric cryptographic algorithms such as (Triple) Data Encryption Standard and Advanced Encryption Standard.

From a mathematical point of view, a cryptographic algorithm is a function that allows ciphering an input text (also called plaintext) by using a secret key. All classical attacks (i.e., cryptanalysis) try to find some correlations between the input and the output of that function in such a way to discover some hidden relations that would allow retrieving the secret key. The secret keys used to encrypt the data with these algorithms are large enough to prevent any brute force attack that consists in exploring the whole solution space (2^n with $64<n<256$). However, the hardware implementation of these cryptographic algorithms allows the hackers to measure the observable characteristics of the physical implementation and deduce the secret key (side-channel attacks). Besides, new other issues arise concerning to the reliability of the device. In particular, a broken device could deliver erroneous results and data that would hazard the security of the whole system.

The first part of the tutorial focuses on attacks based on the observation of the scan chains. These scan chains, which aim to provide full controllability and observability of internal states, are against the principle of security that requires minimal controllability and observability. Details about scan-based techniques for secure cores are described, such as secure scan-chain controller, detection of unauthorized scan shift by test pattern watermarking, spy flip flops, scan enable tree inspection, and data confusion.

The second part of the tutorial analyzes BIST solutions for permanent faults. It will be shown how crypto-devices are well suitable for this type of test. Indeed, from one side BIST approaches are effective for secure circuits since they do not rely on visible scan chains, thus preventing scan-based attacks. Moreover, it is shown how particular characteristics of crypto-devices allow very effective pseudo random tests.

The third part of the tutorial will analyze on-line BIST solutions to increase the fault tolerance of such devices, in particular against fault attacks. This attack is based on the intentional injection of faults (for instance by using a laser beam) into the system while an encryption occurs. By comparing the outputs of the circuits with and without the injection of the fault, it is possible to identify the secret key. To face this problem we analyze how to use error detection and correction codes as counter measure.

Since dedicated design for security techniques have been proposed so far (e.g., development of specific secure cell libraries, or implementation of extra functions for preventing the leakage of useful information for key identification), we eventually discuss perspectives and trends in digital testing of such dedicated components.

REFERENCES

[1] Hely D., Bancel F., Flottes M.-L., Rouzeyre B., "Securing Scan Control in Crypto Chips", Journal of Electronic Testing and Applications 23, 5 (2007) 457-464

[2] 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

[3] G. Di Natale, M. Doulcier, M. L. Flottes and B. Rouzeyre, "A Reliable Architecture for Parallel Implementations of the Advanced Encryption Standard", Journal of Electronic Testing (JETTA), Volume 25, Numbers 4-5, August, 2009, pp. 269-278