Preface

Hardware security is becoming increasingly more important for many embedded systems applications ranging from small RFID tag to satellites orbiting the earth. Its relevance is expected to increase in the coming decades as secure applications such as public services, communication, control and healthcare keep growing.

Concerning all the possible security threats, the vulnerability of electronic devices that implement cryptography functions (including smart cards) has become the Achille's heel in the last decade. Indeed, even though recent crypto-algorithms have been proven resistant to cryptanalysis, certain fraudulent manipulations on the hardware implementing such algorithms can allow extracting confidential information. The so-called side-channel attacks have been the first type of attacks that target the physical device. They are based on information gathered from the physical implementation of a cryptosystem. For instance, by correlating the power consumed and the data manipulated by the device, it is possible to discover the secret encryption key.

New threats have menaced secure devices and the security of the manufacturing process. The first issue is the trustworthiness of the manufacturing process. From one side, the test procedures, which increase controllability and observability of inner points of the circuit, is antinomic with respect to the security. Another threat is related to the possibility for an untrusted manufacturer to do malicious alterations to the design (for instance to bypass or to disable the security fence of the system). The threat brought by so-called hardware Trojans begins to materialize. A second issue is the hazard of faults that can appear during the circuit's lifetime and that may affect the circuit behavior by way of soft errors or deliberate manipulations, called fault attacks.

In 2012, a new COST Action, called TRUDEVICE ("Trustworthy Manufacturing and Utilization of Secure Devices") started in order to cover the above-mentioned topics. COST is an intergovernmental framework for European Cooperation in Science and Technology, allowing the coordination of nationally funded research on a European level. COST increases the mobility of researchers across Europe and fosters the establishment of scientific excellence. COST does not

fund research itself but provides a platform for European scientists to cooperate on a particular project and exchange expertise.

In the context of the TRUDEVICE COST Action, we organized in July 2014 a training school in Lisbon, Portugal. This training school aimed at providing theoretical and practical lectures on topics related to hardware security.

The school started with an introductory session on the fundamental primitives for security, from both hardware and software perspectives. This is followed by an introduction on the implementation of attacks and countermeasures, presenting an overview of physical attacks, both passive and active, and some existing countermeasures. Included in this introduction was the description of the evolution of computer technology and cryptography from the ancient past to current days.

Given this introduction, trustworthy manufacturing of integrated circuits was discussed ranging from the implementation of cryptographic primitives to the manufacturing test of secure devices. The fight against theft, cloning and counterfeiting of integrated circuits was also discussed considering both ASICs and FPGAs. Continuing with the trustworthiness of secure devices, lectures on the various forms of attacks were presented, considering fault attacks and differential power analysis and existing countermeasures.

This training school also included a practical session on performing differential power analysis and on how to test random number generation. As a boost to Ph.D. students an extra session to foster the discussion between students also took place.

The editors would like to thank all the contributing authors for their patience in meeting our deadlines and requirements. Moreover, we would like to express a heartfelt appreciation to all the speakers that made possible the training school. Thanks to their great enthusiasm and work that we could have made the TRUDEVICE training school a grand success.

TRUDEVICE training school speakers: Lejla Batina (Radboud University Nijmegen, The Netherlands), Lilian Bossuet (University of Saint-Etienne, France), Jiri Bucek (Czech Technical University in Prague, Czech Republic), Ricardo Chaves (University of Lisbon, Portugal), Amine Dehbaoui (SERMA Technologies, France), Milos Drutarovsky (Technical University of Kosice, Slovakia), Viktor Fischer (Jean Monnet University Saint-Etienne, France), Julien Francq (AIRBUS Defense and Space, France), Ilya Kizhvatov (RISCURE, The Netherlands), Patrick Haddad (STMicroelectronics and Jean Monnet University Saint-Etienne, France), Vincent van der Leest (Intrinsic-ID, The Netherlands), Victor Lomné (ANSSI, France), Nele Mentens (KU Leuven, Belgium), Giorgio Di Natale (LIRMM, France), Martin Novotny (Czech Technical University in Prague, Czech Republic), Paul-Henri Pugliesi-Conti (NXP Semiconductors, France), Francesco Regazzoni (ALaRI Institute of University of Lugano, Switzerland), Nicolas Sklavos (University of Patras, Greece).

This book follows the same structure of the training school in Lisbon. We start with a brief survey hardware implementations of the Advanced Encryption Standard, which is the cryptographic algorithm that we is used as a reference in the forthcoming chapters. The book is then divided into four main sections. The first section covers the implementation attacks, starting from an introduction on fault

attacks and side-channel attacks, followed by a practical description of the differential power analysis. The section is completed by some countermeasures against fault- and power-based attacks.

The second section covers the issues of the manufacturing testing of hardware devices implementing cryptographic algorithms. The first chapter is dedicated to the classical manufacturing testing and how it can be exploited in order to retrieve secret data. The second chapter contains a survey of the academic and industrial countermeasures.

The third section is dedicated to hardware trust. The first chapter analyzes trustworthiness of mobile devices, including both hardware and software components. The second chapter focuses on Hardware Trojan detection, particularly critical given the common outsourcing of ASIC manufacture.

The last section covers many aspects of Physically Unclonable Functions (PUFs). The first chapter introduces the topic and presents a survey of existing solutions. The next two chapters covers PUFs implemented on FPGAs using delay elements and ring oscillators.

Patra, Greece — Nicolas Sklavos
Lisbon, Portugal — Ricardo Chaves
Montpellier, France — Giorgio Di Natale
Lugano, Switzerland — Francesco Regazzoni

Springer

http://www.springer.com/978-3-319-44316-4

Hardware Security and Trust
Design and Deployment of Integrated Circuits in a Threatened Environment

Sklavos, N.; Chaves, R.; Di Natale, G.; Regazzoni, F. (Eds.)

2017, X, 254 p. 99 illus., 47 illus. in color., Hardcover
ISBN: 978-3-319-44316-4