Information Security and Cryptography
Texts and Monographs

For further volumes:
http://www.springer.com/series/4752

Ahmad-Reza Sadeghi · David Naccache
Editors

Towards Hardware-Intrinsic Security

Foundations and Practice

Foreword by Pim Tuyls

Springer

Editors
Prof. Ahmad-Reza Sadeghi
Universität Bochum
Horst Görtz Institut für
Sicherheit in der
Informationstechnik
Universitätsstr. 150
44780 Bochum
Germany
ahmad.sadeghi@trust.rub.de

Prof. David Naccache
École Normale Supérieure
Dépt. Informatique
rue d'Ulm 45
75230 Paris CX 05
France
david.naccache@ens.fr

Series Editors

Prof. Dr. David Basin
Prof. Dr. Ueli Maurer
ETH Zürich
Switzerland
basin@inf.ethz.ch
maurer@inf.ethz.ch

ISSN 1619-7100
ISBN 978-3-642-14451-6 e-ISBN 978-3-642-14452-3
DOI 10.1007/978-3-642-14452-3
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2010938038

ACM Computing Classification (1998): E.3, K.6.5, B.7, C.2

Cover design: KuenkelLopka GmbH, Heidelberg

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Foreword

Nowadays, computing devices are omnipresent. The vision of the Ambient Intelligent society is becoming a reality very rapidly. Information is exchanged at the speed of light, everybody is connected anytime and anywhere, and new technological developments in the world are taking place faster than ever before. This evolution is the result of the progress in semi-conductor manufacturing processes and technologies which make ICs every year smaller, faster, and more powerful. Mobile devices, (smart) phones, PCs, laptops, smart cards, RFID-tags, personal secure tokens, sensors, etc., are typical products enabling ambient intelligence. Within this environment, information has become one of the most valuable goods and its early availability often means a competitive advantage or a guarantee to our overall security and safety. Human beings on the one hand and industrial as well as governmental organizations on the other hand have become highly dependent on the availability, accessibility, and the flow of correct information for their everyday operations.

Without proper protection, however, information is at the same time the Achilles heel of such a society. When a malicious person or organization can obtain or tamper with sensitive information, the most unexpected and severe consequences may arise. The competitive advantage of a company might disappear, the privacy of individuals and even the security of a whole nation can be compromised. In order to deal with the confidentiality and authenticity of information, cryptographic algorithms are implemented in modern computing devices to protect the link between endpoints. The fact that state-of-the-art cryptographic algorithms are very strong implies that not the links but the physical devices and implementation of the algorithms in those devices have become the weak link in the chain. In particular the secure storage of secret keys and the secure implementation of algorithms and architectures withstanding physical attacks represent some of the major challenges for the security community. The main problem stems from three facts. First, computations are physical processes that leak information on the data being processed through physical side-channels. Second, memories leak information on the stored data to attackers having the availability of "sophisticated" devices such as laser cutters, focused ion beams, and electron microscopes. Unfortunately such tools are readily available for rent nowadays. Third, security measures have to be based on and implemented in

a low-cost manner to be economically viable while attackers have high to almost unlimited budgets available.

A particular field of applications where physical attacks pose an important threat is that of counterfeiting of goods. The terminology "goods" has to be understood here in its most general sense, i.e., physical goods as well as digital goods such as (embedded) software programs, music, video, and designs. Examples of physical goods being counterfeited are automotive and avionic parts, pharmaceuticals, bank passes, smart cards, routers, etc. The total annual value of the trade in fake goods has risen from $200 billion in 2002 to as much as $450 billion in 2006 and the number is expected to have risen to $600 billion in 2009. From these numbers it follows that counterfeiting has a huge economic impact. However, since those products have often lower quality they might additionally lead to brand damage for the legitimate company as well. When counterfeit components are used within critical infrastructures, it is important to realize that the quality level might not only cause damage but contain hidden components whose functionality is not specified. Without doubt this is a threat to the national security of a country.

Recently, a new field of security research dealing with the problem of "physical attacks" and "physical leakage of information" started to develop. Many research groups started to investigate algorithmic as well as physical countermeasures to these threats. Although no general theory dealing with this problem is available, several sub-fields are well developed. The general theory of side-channel secure cryptography has made big progress and goes under the name of physical observable cryptography. Apart from general theoretic developments various practical and efficient countermeasures have been developed as well. Hardware Intrinsic Security on the other hand is a much younger field dealing with secure secret key storage. By generating the secret keys from the intrinsic properties of the silicon, e.g., from intrinsic physical unclonable functions (PUFs), no permanent secret key storage is required anymore and the key is only present in the device for a minimal amount of time. The field of Hardware Intrinsic Security is extending to hardware-based security primitives and protocols such as block ciphers and stream ciphers entangled with hardware. When successful, this will raise the bar of IC security even further. Finally, at the application level there is a growing interest in hardware security for RFID systems and the necessary accompanying system architectures.

It is a pleasure for me to write the foreword of this book. The fields of Hardware Security in general and Hardware Intrinsic Security in particular are very challenging fields with many open problems of high practical relevance. It brings together researchers and practitioners from academia and industry from collaborating and competing groups. The field is highly interdisciplinary by nature. Here, expertises and results from different fields such as physics, mathematics, cryptography, coding theory, and processor theory meet and find new applications. The meeting at Dagstuhl in the summer of 2009, from which this book is the result, brought together many experts from all over the world to discuss these topics in an open and stimulating atmosphere. Personally, I am convinced that this book will serve as an important background material for students, practitioners, and experts and stimulates much further research and developments in hardware security all

over the world. Without doubt the material covered here will lay the foundations of the future security devices guaranteeing the necessary privacy, confidentiality, and authenticity of information for our modern society.

January 2010 Pim Tuyls

Contents

List of Contributors

Frederik Armknecht Horst Görtz Institute for IT Security, Ruhr-University Bochum, Bochum, Germany; Technische Universität Darmstadt, Darmstadt, Germany, Frederik.Armknecht@trust.rub.de

Muhammad Asim Philips Research Eindhoven, Information and System Security Group, The Netherlands, muhammad.asim@philips.com

Yoo-Jin Baek System LSI Division, Samsung Electronics Co., Ltd., Suwon, Korea, yoojin.baek@samsung.com

Lejla Batina Computing Science Department/DS group, Radboud University Nijmegen, 6525 AJ Nijmegen, The Netherlands, lejla@cs.ru.nl

Heike Busch Technische Universität Darmstadt, Darmstadt, Germany, busch@seceng.informatik.tu-darmstadt.de

Andrew H. Chan University of California, Berkeley, CA, USA, andrewhc@eecs.berkeley.edu

Aykutlu Dana UNAM, Institute of Materials Science and Nanotechnology, Bilkent University, Ankara, Turkey, aykutlu@unam.bilkent.edu.tr

Daniel Y. Deng Cornell University, Ithaca, NY, USA, dyd2@cornell.edu

Loic Duflot French Network and Information Security Agency (ANSSI), Paris, France, loic.duflot@ssi.gouv.fr

G. Edward Suh Cornell University, Ithaca, NY, USA, suh@csl.cornell.edu

Vanessa Gratzer Centre de recherche en informatique, Université Paris I, Panthéon-Sorbonne, Paris, France, vanessa@gratzer.fr

Olivier Grumelard French Network and Information Security Agency (ANSSI), Paris, France, olivier.grumelard@ssi.gouv.fr

Jorge Guajardo Philips Research Eindhoven, Information and System Security Group, The Netherlands, jorge.guajardo@philips.com

Ghaith Hammouri CRIS Lab, Worcester Polytechnic Institute, Worcester, MA 01609-2280, USA, hammouri@wpi.edu

Helena Handschuh Intrinsic-ID, San Jose, CA 95110, USA; ESAT-COSIC, Katholieke Universiteit Leuven, Leuven, Belgium, helena.handschuh@intrinsic-ID.com

Kimmo Järvinen Department of Information and Computer Science, Aalto University, Aalto, Finland, kimmo.jarvinen@tkk.fi

Stefan Katzenbeisser Technische Universität Darmstadt, Darmstadt, Germany, katzenbeisser@seceng.informatik.tu-darmstadt.de

Inyoung Kim Statistics Department, Virginia Tech, Blacksburg, VA 24061, USA, inyoungk@vt.edu

Sung-Hyun Kim System LSI Division, Samsung Electronics Co., Ltd., Suwon, Korea, teri_kim@samsung.com

Darko Kirovski Microsoft Research, Redmond, WA 98052, USA, darkok@microsoft.com

Vladimir Kolesnikov Alcatel-Lucent Bell Laboratories, Murray Hill, NJ 07974, USA, kolesnikov@research.bell-labs.com

Markus G. Kuhn Computer Laboratory, University of Cambridge, Cambridge CB3 0FD, UK, Markus.Kuhn@cl.cam.ac.uk

Yong Ki Lee Department of Electrical Engineering, University of California, Los Angeles, CA 90095-1594, USA, jfirst@ee.ucla.edu

Olivier Levillain French Network and Information Security Agency (ANSSI), Paris, France, olivier.levillain@ssi.gouv.fr

Roel Maes ESAT/COSIC and IBBT, Catholic University of Leuven, Leuven, Belgium, roel.maes@esat.kuleuven.be

Abhranil Maiti ECE Department, Virginia Tech, Blacksburg, VA 24061, USA, abhranil@vt.edu

Benjamin Morin French Network and Information Security Agency (ANSSI), Paris, France, benjamin.morin@ssi.gouv.fr

David Naccache Département d'informatique, École normale supérieure, Paris, France, david.naccache@ens.fr

Leyla Nazhandali ECE Department, Virginia Tech, Blacksburg, VA 24061, USA, leyla@vt.edu

Elisabeth Oswald Department of Computer Science, University of Bristol, Department of Computer Science, Bristol, UK, Elisabeth.Oswald@bristol.ac.uk

Olivier Pereira Crypto Group, Université catholique de Louvain, Louvain-la-Neuve, Belgium, olivier.pereira@uclouvain.be

Milan Petković Philips Research Eindhoven/Eindhoven University of Technology, Eindhoven, The Netherlands, milan.petkovic@philips.com, m.petkovic@tue.nl

Bart Preneel ESAT-COSIC, Katholieke Universiteit Leuven, Leuven, Belgium, bart.preneel@esat.kuleuven.be

Jean-Jacques Quisquater Crypto Group, Université catholique de Louvain, Louvain-la-Neuve, Belgium, quisquater@dice.ucl.ac.be

Ulrich Rührmair Technische Universität München, München, Germany, ruehrmai@in.tum.de

Ahmad-Reza Sadeghi Horst Görtz Institute for IT Security, Ruhr-University Bochum, Bochum, Germany, ahmad.sadeghi@trust.rub.de

Patrick Schaumont ECE Department, Virginia Tech, Blacksburg, VA 24061, USA, schaum@vt.edu

Thomas Schneider Horst Görtz Institute for IT-Security, Ruhr-University Bochum, Bochum, Germany, thomas.schneider@trust.rub.de

Geert-Jan Schrijen Intrinsic-ID, 5656 AE Eindhoven, The Netherlands, geert.jan.schrijen@intrinsic-ID.com

Dave Singelee ESAT-COSIC, Katholieke Universiteit Leuven, Leuven, Belgium, dave.singelee@esat.kuleuven.be

François-Xavier Standaert Crypto Group, Université catholique de Louvain, Louvain-la-Neuve, Belgium, fstandae@uclouvain.be

Berk Sunar Cryptography & Information Security, Worcester Polytechnic Institute, Worcester, MA, USA, sunar@wpi.edu

Mohammad Tehranipoor University of Connecticut, Storrs, CT 06269, USA, tehrani@engr.uconn.edu

Pim Tuyls Intrinsic-ID, 5656 AE Eindhoven, The Netherlands; ESAT/COSIC and IBBT, Catholic University of Leuven, Leuven, Belgium, pim.tuyls@intrinsic-ID.com, pim.tuyls@gmail.com

Markus Ullmann Bonn-Rhein-Sieg University of Applied Sciences, Sankt Augustin, Germany; Bundesamt für Sicherheit in der Informationstechnik, Bonn, Germany, Markus.Ullmann@bsi.bund.de

Ingrid Verbauwhede ESAT-COSIC, Katholieke Universiteit Leuven, Leuven, Belgium, ingrid.verbauwhede@esat.kuleuven.be

Vignesh Vivekraja ECE Department, Virginia Tech, Blacksburg, VA 24061, USA, vigneshv@vt.edu

Matthias Vögeler NXP Semiconductors, Business Line Identification, Hamburg, Germany, Matthias.Voegeler@nxp.com

Ivan Visconti Dipartimento di Informatica ed Applicazioni, University of Salerno, Salerno, Italy, visconti@dia.unisa.it

Christian Wachsmann Horst Görtz Institute for IT-Security (HGI), Ruhr-University Bochum, Bochum, Germany, christian.wachsmann@trust.rub.de

Yu Yu Crypto Group, Université catholique de Louvain, Louvain-la-Neuve, Belgium, yu.yu@uclouvain.be

Moti Yung Department of Computer Science, Columbia University, New York, NY, USA; Google Inc, Mountain View, CA, USA, moti@cs.columbia.edu

Huaiye Zhang Statistics Department, Virginia Tech, Blacksburg, VA 24061, USA, zhanghy@vt.edu