Integrated Circuits and Systems

Series Editor
Anantha Chandrakasan, Massachusetts Institute of Technology
Cambridge, Massachusetts

For other titles published in this series, go to
http://www.springer.com/series/7236

Ingrid M.R. Verbauwhede
Editor

Secure Integrated Circuits and Systems

Springer

Editor
Ingrid M.R. Verbauwhede
Department of Elektrotechniek (ESAT)
Katholieke Universiteit Leuven
COSIC Division
Kasteelpark Arenberg 10
3001 Leuven
Belgium
ingrid.verbauwhede@esat.kleuven.be

ISSN 1558-9412
ISBN 978-0-387-71827-9 e-ISBN 978-0-387-71829-3
DOI 10.1007/978-0-387-71829-3
Springer New York Dordrecht Heidelberg London

Library of Congress Control Number: 2009942092

Preface

Security is as strong as the weakest link. The mathematical design and analysis of cryptographic algorithms has evolved a lot over the last decades (ever since the invention of public key cryptography at the end of the 1970s). The mathematical strength of the cryptographic algorithms is now at such a level that the attacker will choose the 'implementation' as the weak link in the chain. Many incidents have been reported for hardware and software implementations. Even the human factor, forgetting or using easy passwords, is often the weak link.

Weak implementations are becoming an even bigger problem as more and more information processing moves to small portable embedded devices. These small devices are cheap, lightweight, easy to carry around, and also easy to loose. The need for embedded security is omnipresent in cell phones, PDA's, medical devices, automotive, consumer, smart cards, RFID tags, sensor nodes, and so on.

At the other end of the spectrum computations and storage of sensitive data move from hard disks on our personal PCs to central servers and to the so-called clouds. Also in these environments efficient and secure implementations are a necessity to provide security and privacy.

The goal of this book, *Secure Integrated Circuits and Systems*, is to give the integrated circuits and system designer an insight in the basics of security and cryptography from the implementation viewpoint. This means that the designer should aim at *efficient* implementations, i.e., optimizing power, area, throughput, as well as *secure* implementations, i.e., implementations that resist attacks and more specifically side-channel attacks. This book therefore covers techniques both to improve efficiency and to resist side-channel attacks.

The book consists of four major parts to introduce the topic. Part I gives the basics. This includes an introduction to the basic arithmetic used in mostly public-key algorithms and an introduction to side-channel attacks.

Part II describes basic building blocks of any cryptographic systems. When building a complex system, such as a system-on-chip, a designer will build, obtain, or license intellectual property (IP) modules. The basic modules are symmetric key algorithms, public key algorithms, and hash functions. Other building blocks are random number generators, nonce generators, and physically uncloneable functions (PUFs).

The aim of part III is to describe the design methods for secure design. Each link in the chain has to be secure: this means that each part of the design process should have security in mind. This has to be the case for back-end design from a register-transfer level description down to layout. This also has to be the case for higher level design: e.g., the GEZEL design environment promotes secure hardware/software co-design.

Part IV is used to illustrate the topic by examples: security for RFID, end-point security for FPGA's, and securing flash memories.

Secure Integrated Circuits and Systems is written for any integrated circuit or embedded systems designer who makes designs for ASIC's, FPGA's, small embedded processors, and/or embedded systems. By no means, I claim that this book is complete. It is only a start to get the designer going. And it is an attempt to bridge the gap between the theoretical math of cryptography and the design issues to make it possible in practice. I would like to thank the contributors of this book and the people working in this field for their indirect contributions.

July 2009 Ingrid M.R. Verbauwhede

Contents

Part IV Applications

Contributors

Lejla Batina Katholieke Universiteit Leuven, Leuven-Heverlee, Belgium and Radboud University Nijmegen, The Netherlands, lejla.batina@esat.kuleuven.be

Guido Marco Bertoni STMicroelectronics, Centro Direzionale Colleoni 20041 Agrate, Italy, guido.bertoni@st.com

Tim Güneysu Chair for Embedded Security, Ruhr University Bochum, Bochum, Germany, gueneysu@crypto.rub.de

Helena Handschuh Katholieke Universiteit Leuven, ESAT/COSIC, Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, helenahandschuh@yahoo.fr

Miroslav Knežević Katholieke Universiteit Leuven, ESAT/COSIC, Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium, miroslav.knezevic@esat.kuleuven.be

Yong Ki Lee University of California, Los Angeles, CA, USA; Electrical Engineering, 420 Westwood Plaza, Los Angeles, CA 90095-1594, USA, jfirst@ee.ucla.edu

Roel Maes Katholieke Universiteit Leuven, ESAT/COSIC, Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium, roel.maes@esat.kuleuven.be

Stefan Mangard Infineon Technologies AG, Security Innovation, Am Campeon 1-1285579 Neubiberg, Germany, stefan.mangard@infineon.com

Filippo Melzani STMicroelectronics, Centro Direzionale Colleoni 20041 Agrate, Italy, filippo.melzani@st.com

Elisabeth Oswald Computer Science Department, University of Bristol, Merchant Venturers Building, Woodland Road, Bristol, BS8 1UB, UK; Institute for Applied Information Processing and Communication, Graz University of Technology, Inffeldgasse 16a, 8010 Graz, Austria, elisabeth.oswald@bristol.ac.uk

Christof Paar Chair for Embedded Security, Ruhr University Bochum, Bochum, Germany, christof.paar@rub.de

Kazuo Sakiyama University of Electro-Communications, Tokyo, Japan, saki@ice.uec.ac.jp

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

Dries Schellekens Katholieke Universiteit Leuven, ESAT/COSIC, Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium, dries.schellekens@esat.kuleuven.be

Eric Simpson ECE Department, Virginia Tech, Blacksburg, VA 24061, USA

François-Xavier Standaert UCL Crypto Group, Place du Levant 3, B-1348 Louvain-la-Neuve, Belgium, fstandae@uclouvain.be

Berk Sunar Electrical and Computer Engineering Department, Worcester Polytechnic Institute, Worcester MA 01609–2280, USA, sunar@wpi.edu

Kris Tiri Work performed while at UCLA, kris.tiri@gmail.com

Elena Trichina Advanced System Technology ST Microelectronics Rousset, France, elena.trichina@st.com

Pim Tuyls Intrinsic-ID, Eindhoven, The Netherlands, pim.tuyls@intrinsic-id.com

Ingrid M.R. Verbauwhede Katholieke Universiteit Leuven, ESAT/COSIC, Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium, ingrid.verbauwhede@esat.kuleuven.be

Pengyuan Yu ECE Department, Virginia Tech, Blacksburg, VA 24061, USA