

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, Lancaster, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Zürich, Switzerland

John C. Mitchell

Stanford University, Stanford, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbrücken, Germany

More information about this series at <http://www.springer.com/series/7410>

François-Xavier Standaert · Elisabeth Oswald (Eds.)

Constructive Side-Channel Analysis and Secure Design

7th International Workshop, COSADE 2016
Graz, Austria, April 14–15, 2016
Revised Selected Papers

Editors

François-Xavier Standaert
UCL Crypto Group
Louvain-la-Neuve
Belgium

Elisabeth Oswald
University of Bristol
Bristol
UK

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-43282-3 ISBN 978-3-319-43283-0 (eBook)
DOI 10.1007/978-3-319-43283-0

Library of Congress Control Number: 2016945799

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer International Publishing Switzerland 2016

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG Switzerland

Preface

The 7th International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE) was held in Graz, Austria, during April 14–15, 2016. This now well-established workshop brings together researchers from academia, industry, and government who share a common interest in the design and secure implementation of cryptographic primitives. COSADE 2016 received 32 submission; the review process relied on the EasyChair system.

From the pool of submissions, 12 high-quality papers were selected carefully after deliberations of the 30 Program Committee members who were supported by 24 additional reviewers. The composition of the Program Committee was representative of the good mix between academic and industrial researchers as well as the geographic spread of researchers across the globe. We would like to express our sincere gratitude to both the Program Committee members and reviewers.

As it has become custom, the Program Committee members voted on the best paper among the accepted papers. The resulting winner was “Exploiting the Physical Disparity: Side-Channel Attacks on Memory Encryption” authored by Thomas Unterluggauer and Stefan Mangard. The program also featured three invited talks. Tom Chothia elaborated on advanced statistical tests for detecting information leakage. François Dupressoir spoke about formal and compositional proofs of probing security for masked algorithms. Aurélien Francillon discussed what security problems can be spotted with large-scale static analysis of systems. We would like to thank the invited speakers for joining us in Graz.

Finally, we would like to thank the local organizers, in particular Stefan Mangard (general chair) and Thomas Korak, for their support and for making this great event possible. On behalf of the COSADE community we would also like to thank our GOLD sponsors Infineon Technologies AG, NewAE Technology Inc., NXP Semiconductors, Riscure, and Secure-IC, as well as our SILVER sponsors Rambus Cryptography Research and Oberthur Technologies, for their support.

And most importantly, we would like to thank the authors for their excellent contributions.

May 2016

Elisabeth Oswald
François-Xavier Standaert

Organization

Program Committee

Josep Balasch	KU Leuven, Belgium
Guido Bertoni	STMicroelectronics, Italy
Shivam Bhasin	Nanyang Technological University, Singapore
Christophe Clavier	University of Limoges, France
Hermann Drexler	Giesecke & Devrient, Germany
Cécile Dumas	CEA LETI, France
Thomas Eisenbarth	WPI, USA
Wieland Fischer	Infineon Technologies, Germany
Benoît Gérard	DGA Maîtrise de l'Information, France
Christophe Giraud	Oberthur Technologies, France
Vincent Grosso	UCL, Belgium
Johann Groszschädl	University of Luxembourg, Luxembourg
Tim Güneysu	University of Bremen, Germany
Sylvain Guilley	Télécom ParisTech, France
Johann Heyszl	Fraunhofer AISEC, Germany
Naofumi Homma	Tohoku University, Japan
Michael Hutter	CRI, USA
Ilya Kizhvatov	Riscure, The Netherlands
Thanh-ha Le	Morpho, France
Kerstin Lemke-Rust	Bonn-Rhein-Sieg University of Applied Sciences, Germany
Marcel Medwed	NXP Semiconductors, Austria
Amir Moradi	Ruhr-Universität Bochum, Germany
Debdeep Mukhopadhyay	Indian Institute of Technology Kharagpur, India
Elisabeth Oswald	University of Bristol, UK
Emmanuel Prouff	ANSSI, France
Francesco Regazzoni	University of Lugano, Switzerland
Matthieu Rivain	CryptoExperts, France
Kazuo Sakiyama	The University of Electro-Communications Tokyo, Japan
Francois-Xavier Standaert	UCL Crypto Group, Belgium
Carolyn Whinnall	University of Bristol, UK

Additional Reviewers

Abdullin, Nikita
Barbu, Guillaume
Bauer, Sven
Becker, Georg T.
Bocktaels, Yves
Breier, Jakob
Chabrier, Thomas
Chen, Cong
Dabosville, Guillaume
De Santis, Fabrizio
Dinu, Daniel
Goodwill, Gilbert
Greuet, Aurélien
Hayashi, Yuichi

He, Wei
Hoffmann, Lars
Irazoqui, Gorka
Jap, Dirmanto
Knezevic, Miroslav
Li, Yang
Lomne, Victor
Longo Galea, Jake
Martin, Daniel
Mather, Luke
Melzani, Filippo
Miura, Noriyuki
Oder, Tobias
Omic, Jasmina

Patranabis, Sikhar
Riou, Sebastien
Samarin, Peter
Sasdrich, Pascal
Schellenberg, Falk
Schneider, Tobias
Selmke, Bodo
Susella, Ruggero
Takahashi, Junko
Ueno, Rei
Vermoen, Dennis
Yli-Mayry, Ville

Contents

Security and Physical Attacks

Exploiting the Physical Disparity: Side-Channel Attacks on Memory Encryption	3
<i>Thomas Unterluggauer and Stefan Mangard</i>	
Co-location Detection on the Cloud.	19
<i>Mehmet Sinan İnci, Berk Gulmezoglu, Thomas Eisenbarth, and Berk Sunar</i>	
Simple Photonic Emission Attack with Reduced Data Complexity.	35
<i>Elad Carmon, Jean-Pierre Seifert, and Avishai Wool</i>	

Side-Channel Analysis (Case Studies)

Power Analysis Attacks Against IEEE 802.15.4 Nodes	55
<i>Colin O'Flynn and Zhizhang Chen</i>	
Improved Side-Channel Analysis Attacks on Xilinx Bitstream Encryption of 5, 6, and 7 Series	71
<i>Amir Moradi and Tobias Schneider</i>	
Dismantling Real-World ECC with Horizontal and Vertical Template Attacks	88
<i>Margaux Dugardin, Louiza Papachristodoulou, Zakaria Najm, Lejla Batina, Jean-Luc Danger, and Sylvain Guilley</i>	

Fault Analysis

Algorithmic Countermeasures Against Fault Attacks and Power Analysis for RSA-CRT.	111
<i>Ágnes Kiss, Juliane Krämer, Pablo Rauzy, and Jean-Pierre Seifert</i>	
Improved Differential Fault Analysis on Camellia-128.	130
<i>Toru Akishita and Noboru Kunihiro</i>	
A Note on the Security of CHES 2014 Symmetric Infective Countermeasure	144
<i>Alberto Battistello and Christophe Giraud</i>	

Side-Channel Analysis (Tools)

Simpler, Faster, and More Robust T-Test Based Leakage Detection. 163
A. Adam Ding, Cong Chen, and Thomas Eisenbarth

Design and Implementation of a Waveform-Matching Based
Triggering System. 184
*Arthur Beckers, Josep Balasch, Benedikt Gierlichs,
and Ingrid Verbauwhede*

Robust and One-Pass Parallel Computation of Correlation-Based Attacks
at Arbitrary Order. 199
Tobias Schneider, Amir Moradi, and Tim Güneysu

Author Index 219