Lecture Notes in Computer Science 9689

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

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

Springer

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

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 Nederlands
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 Whitnall	University of Bristol, UK

Additional Reviewers

Abdullin, Nikita
Barbu, Guillaume
Bauer, Sven
Becker, Georg T.
Bocktaels, Yves
Breier, Jakub
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

Side-Channel Analysis (Case Studies)

Fault Analysis

Side-Channel Analysis (Tools)