

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, Zurich, 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, Chennai, 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

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

Ilia Polian · Marc Stöttinger (Eds.)

Constructive Side-Channel Analysis and Secure Design

10th International Workshop, COSADE 2019
Darmstadt, Germany, April 3–5, 2019
Proceedings

Editors
Ilia Polian 
Universität Stuttgart
Stuttgart, Germany

Marc Stöttinger
Continental AG
Frankfurt, Germany

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-16349-5 ISBN 978-3-030-16350-1 (eBook)
<https://doi.org/10.1007/978-3-030-16350-1>

Library of Congress Control Number: 2019935139

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 2019

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, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

COSADE 2019, the 10th International Workshop on Constructive Side-Channel Analysis and Secure Design, was held in Darmstadt, Germany, April 3–5, 2019. This workshop is a well-established platform for researchers and practitioners from academia, industry, and government to exchange and discuss the state of the art in implementation attacks, e.g., side-channel attacks or fault-injection attacks, and secure implementation of cryptographic algorithms and security controls. The workshop was conducted in cooperation with the International Association for Cryptographic Research. COSADE 2019 was organized by Technische Universität Darmstadt in collaboration with the Collaborative Research Center (SFB) CROSSING.

This year 34 papers were submitted to the COSADE workshop. Each paper was anonymously reviewed in a double-blind peer-review process by at least four Program Committee members. In total, 130 reviews were written by the Program Committee members with the help of 39 additional reviewers. The international Program Committee consisted of 35 members from 13 countries. The members were carefully selected experts in the area of side-channel analysis, fault injection analysis, and secure design to represent academia and industry. The decision process was very challenging and resulted in the selection of 14 papers. These 14 papers were part of the contribution to COSADE 2019 and are contained in these workshop proceedings. We are deeply grateful to all reviewers for their dedication and hard work in reviewing, assessing, and discussing.

Beside the 14 presentations of the selected papers, two keynotes and one invited talk were given at the COSADE 2019. The first invited talk was about RowHammer like exploits given by Onur Mutlu from Carnegie Mellon University and ETH Zürich. This talk provided a comprehensive overview of the various versions of implementation attacks and appropriate countermeasures. The second invited talk was given by Ramesh Karri from New York University about secure high-level synthesis. His talk focused on secure design process for hardware designs with increased resilience against malicious circuits and backdoors. Sylvain Guilley gave an invited talk on detection and prevention of cache-timing attacks. The talks of Mutlu and Guilley are also summarized in a paper and contained in the proceedings of COSADE 2019. In addition, an anniversary talk was given by Sorin A. Huss to mark the tenth edition of COSADE. He presented the highlights and some historical facts of the last nine COSADE workshops as well as the scientific motivation to proceed with research on novel countermeasure strategies and techniques.

We would like to thank the general chair, Stefan Katzenbeisser, and the local organizers, Daniela Fleckenstein and Ursula Paeckel, all of TU Darmstadt, for the local organization, which made this workshop a memorable event. We would also like to thank the two Web administrators, Helmut Haefner and Lothar Hellmeier of the University of Stuttgart, for maintaining the COSADE website for 2019.

We are very grateful for the financial support received from our generous sponsors ALPha NOV, Continental, eshard, FortiyfIQ, Rambus Cryptography Research, Ris-cure, and Secure-IC.

April 2019

Ilia Polian
Marc Stöttinger

Organization

The 10th International Workshop on Constructive Side-Channel Analysis and Secure Design

Darmstadt, Germany, April 3–5, 2019

Steering Committee

Jean-Luc Danger	Télécom ParisTech, France
Werner Schindler	Bundesamt für Sicherheit in der Informationstechnik (BSI), Germany

General Chair

Stefan Katzenbeisser	Technische Universität Darmstadt, Germany
----------------------	---

Program Committee Chairs

Ilia Polian	Universität Stuttgart, Germany
Marc Stöttinger	Continental AG, Germany

Program Committee

Divya Arora	Intel, USA
Navid Asadizanjani	University of Florida, USA
Reza Azarderakhsh	Florida Atlantic University, USA
Josep Balasch	KU Leuven, Belgium
Goerg T. Becker	EMST, Germany
Sonia Belaïd	CryptoExperts, France
Shivam Bhasin	Nanyang Technological University, Singapore
Anupam Chattopadhyay	Nanyang Technological University, Singapore
Elke De Mulder	Cryptography Research, USA
Fabrizio De Santis	Siemens AG, Germany
Wieland Fischer	Infineon Technologies, Germany
Jorge Guajardo	Robert Bosch LLC, Research and Technology Center, USA
Sylvain Guilley	Secure-IC, France
Annelie Heuser	CNRS, IRISA, France
Naofumi Homma	Tohoku University, Japan
Michael Hutter	Cryptography Research, USA
Jens-Peter Kaps	George Mason University, USA

Michael Kasper	Fraunhofer Singapore, Singapore
Elif Bilge Kavun	The University of Sheffield, UK
Osnat Keren	Bar-Ilan University, Israel
Roel Maes	Intrinsic-ID, The Netherlands
Marcel Medwed	NXP Semiconductors, Austria
Nele Mentens	KU Leuven, Belgium
Amir Moradi	Ruhr-Universität Bochum, Germany
Debdepp Mukhopadhyay	IIT Kharagpur, India
Makoto Nagata	Kobe University, Japan
Collin O'Flynn	NewAE Technology, Canada
Axel Poschmann	DarkMatter, United Arab Emirates
Francesco Regazzoni	ALaRi-USI, Swiss
Kazuo Sakiyama	The University of Electro-Communications, Japan
Patrick Schaumont	Virginia Tech, USA
Georg Sigl	TU München and Fraunhofer AISEC, Germany
Francois-Xavier Standaert	UCL Crypto Group, Belgium
Marc Witteman	Riscure, The Netherlands

Additional Reviewers

Nikolaos Athanasios Anagnostopoulos	Kimmo Järvinen	Pascal Sasdrich
Melissa Azouaoui	Bernhard Jungk	Thomas Schamberger
Alexander Bajic	Mehran Mozaffari Kermani	Hermann Seuschek
Arthur Beckers	Rami El Khatib	Hadi Soleimany
Sarani Bhattacharya	Philipp Koppermann	Lars Tebelmann
Begul Bilgin	Bodhisatwa Mazumdar	Michael Tunstall
Manuel Bluhm	Hatame Mosanaei	Rei Ueno
Joppe Bos	Guilherme Perin	Gilles Van Assche
Martin Butkus	Romain Poussier	Vincent Verneuil
Vincent Grosso	Prasanna Ravi	Junwei Wang
Michael Gruber	Bastian Richter	Felix Wegener
Amir Jalali	Mélissa Rossi	Florian Wilde
Dirmanto Jap	Steffen Sanwald	Ville Yli-Mäyry

Contents

Keynotes and Invited Talks

RowHammer and Beyond	3
<i>Onur Mutlu</i>	
Cache-Timing Attack Detection and Prevention: Application to Crypto Libs and PQC.	13
<i>Sébastien Carré, Adrien Facon, Sylvain Guilley, Sofiane Takarabt, Alexander Schaub, and Youssef Souissi</i>	

Side-Channel Attacks

Fast Side-Channel Security Evaluation of ECC Implementations: Shortcut Formulas for Horizontal Side-Channel Attacks Against ECSCM with the Montgomery Ladder	25
<i>Melissa Azouaoui, Romain Poussier, and François-Xavier Standaert</i>	
Side-Channel Analysis of the TERO PUF	43
<i>Lars Tebelmann, Michael Pehl, and Vincent Immler</i>	

Fault-Injection Attacks

FIMA: Fault Intensity Map Analysis	63
<i>Keyvan Ramezanzpour, Paul Ampadu, and William Diehl</i>	
Differential Fault Attacks on KLEIN	80
<i>Michael Gruber and Bodo Selmke</i>	

White-Box Attacks

Another Look on Bucketing Attack to Defeat White-Box Implementations. . .	99
<i>Mohamed Zeyad, Houssein Maghrebi, Davide Alessio, and Boris Batteux</i>	
Higher-Order DCA against Standard Side-Channel Countermeasures	118
<i>Andrey Bogdanov, Matthieu Rivain, Philip S. Vejre, and Junwei Wang</i>	

Side-Channel Analysis Methodologies

Gradient Visualization for General Characterization in Profiling Attacks	145
<i>Loïc Masure, Cécile Dumas, and Emmanuel Prouff</i>	

Fast Analytical Rank Estimation 168
Liron David and Avishai Wool

Security Aspects of Post-Quantum Schemes

Fault Attacks on UOV and Rainbow 193
Juliane Krämer and Mirjam Loiero

Towards Optimized and Constant-Time CSIDH on Embedded Devices 215
Amir Jalali, Reza Azarderakhsh, Mehran Mozaffari Kermani, and David Jao

Number “Not Used” Once - Practical Fault Attack on *pqm4* Implementations of NIST Candidates. 232
Prasanna Ravi, Debapriya Basu Roy, Shivam Bhasin, Anupam Chattopadhyay, and Debdeep Mukhopadhyay

Countermeasures Against Implementation Attacks

Practical Evaluation of Masking for NTRUEncrypt on ARM Cortex-M4 253
Thomas Schamberger, Oliver Mischke, and Johanna Sepulveda

Shuffle and Mix: On the Diffusion of Randomness in Threshold Implementations of KECCAK 270
Felix Wegener, Christian Baiker, and Amir Moradi

Trade-offs in Protecting KECCAK Against Combined Side-Channel and Fault Attacks 285
Antoon Purnal, Victor Arribas, and Lauren De Meyer

Author Index 303