Lecture Notes in Computer Science 10815

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

Junfeng Fan · Benedikt Gierlichs (Eds.)

Constructive Side-Channel Analysis and Secure Design

9th International Workshop, COSADE 2018
Singapore, April 23–24, 2018
Proceedings

Springer

Editors
Junfeng Fan
Open Security Research
Shenzhen
China

Benedikt Gierlichs
KU Leuven
Leuven
Belgium

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-89640-3 ISBN 978-3-319-89641-0 (eBook)
https://doi.org/10.1007/978-3-319-89641-0

Library of Congress Control Number: 2018939449

LNCS Sublibrary: SL4 – Security and Cryptology

Printed on acid-free paper

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

Preface

The 9th International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE) was held at Nanyang Technological University in Singapore during April 23–24, 2018. The workshop was held in cooperation with the International Association for Cryptologic Research (IACR). COSADE brings together researchers from academia, industry, and government who share a common interest in the design and secure implementation of cryptographic primitives. COSADE 2018 received 31 submissions. Each paper was anonymously reviewed by at least four Program Committee members in a double-blind peer review process. The review process relied on the EasyChair system. From the pool of submissions, 14 high-quality papers were selected carefully after deliberations by the 30 Program Committee members who were supported by 45 additional reviewers. The composition of the Program Committee was representative of the good mix between academic and industrial researchers, the geographic spread of researchers across the globe, and their expertise. We would like to express our sincere gratitude to both the Program Committee members and the reviewers for their hard work. We would also like to thank the invited speakers Jeroen Delvaux and Emmanuel Prouff for joining us in Singapore and for delivering inspiring talks. Finally, we would like to thank the local organizers Shivam Bhasin, Michael Kasper, and Marc Stöttinger for their support and for making this great event possible. On behalf of the COSADE community we are very grateful to our sponsors Alpha-NOV, Continental, eshard, NewAE, Riscure, Secure-IC, Cryptography Research, Nanyang Technological University, for their financial support. And most importantly, we would like to thank the authors for their excellent contributions. Without them this workshop would not exist.

April 2018

Junfeng Fan
Benedikt Gierlichs

Organization

Program Committee

Zhimin Chen	Apple, USA
Christophe Clavier	Université de Limoges, France
Elke De Mulder	Cryptography Research, Inc., USA
Hermann Drexler	G+D Mobile Security, Germany
Junfeng Fan	Open Security Research (OSR), China
Benoit Feix	Eshard, France
Wieland Fischer	Infineon Technologies, Germany
Benedikt Gierlichs	KU Leuven imec-COSIC, Belgium
Christophe Giraud	IDEMIA, France
Xu Guo	Qualcomm, USA
Naofumi Homma	Tohoku University, Japan
Michael Hutter	Cryptography Research, USA
Markus Kuhn	University of Cambridge, UK
Kerstin Lemke-Rust	Bonn-Rhein-Sieg University of Applied Sciences, Germany
Tancrède Lepoint	SRI International, USA
Yang Li	Nanjing University of Aeronautics and Astronautics, China
Roel Maes	Intrinsic-ID, The Netherlands
Stefan Mangard	TU Graz, Austria
Marcel Medwed	NXP Semiconductors Austria GmbH, Austria
Amir Moradi	Ruhr University Bochum, Germany
Debdeep Mukhopadhyay	IIT Kharagpur, India
Elisabeth Oswald	University of Bristol, UK
Thomas Peyrin	Nanyang Technological University, Singapore
Axel Y. Poschmann	DarkMatter, Abu Dhabi, UAE
Emmanuel Prouff	ANSSI, France
Francesco Regazzoni	ALaRI – USI, Switzerland
Oscar Reparaz	KU Leuven imec-COSIC, Belgium and Square Inc., USA
Matt Robshaw	Impinj, USA
Kazuo Sakiyama	The University of Electro-Communications, Japan
Patrick Schaumont	Virginia Tech, USA
Alexander Schlösser	NXP Semiconductors, Germany
Brecht Wyseur	Kudelski Group, Switzerland

Additional Reviewers

Manaar Alam
Anubhab Baksi
Subhadeep Banik
Guillaume Barbu
Debapriya Basu Roy
Alberto Battistello
Begül Bilgin
Manuel Bluhm
Martin Butkus
Nicolas Debande
Santos Merino Del Pozo
Christoph Dobraunig
Dahmun Goudarzi
Hannes Gross
Max Hoffmann
Mustafa Kairallah
Elif Bilge Kavun
Bodhisatwa Mazumdar
Florian Mendel
Xiaohan Meng
Oliver Mischke
Nicolas Moro
Ventzi Nikov
Sikhar Patranabis
Peter Pessl
Léo Reynaud
Bastian Richter
Sayandeep Saha
Hermann Seuschek
Rémi Strullu
Takeshi Sugawara
Atsushi Takayasu
Adrian Thillard
Michael Tunstall
Rei Ueno
Thomas Unterluggauer
Vincent Verneuil
Karine Villegas
Ruyang Wang
Shuang Wang
Felix Wegener
Antoine Wurcker
Mo Yang
Yuan Yao
Ville Yli-Mäyry

Contents

Countermeasures Against Side-Channel Attacks (1)

Tools for Side-Channel Analysis

Fault Attacks and Hardware Trojans

Side-Channel Analysis Attacks

Countermeasures Against Side-Channel Attacks (2)