

Founding Editors

Gerhard Goos

Karlsruhe Institute of Technology, Karlsruhe, Germany

Juris Hartmanis

Cornell University, Ithaca, NY, USA

Editorial Board Members

Elisa Bertino

Purdue University, West Lafayette, IN, USA

Wen Gao

Peking University, Beijing, China

Bernhard Steffen 

TU Dortmund University, Dortmund, Germany

Gerhard Woeginger 

RWTH Aachen, Aachen, Germany

Moti Yung

Columbia University, New York, NY, USA

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

Guido Marco Bertoni · Francesco Regazzoni (Eds.)

Constructive Side-Channel Analysis and Secure Design

11th International Workshop, COSADE 2020
Lugano, Switzerland, April 1–3, 2020
Revised Selected Papers

Editors

Guido Marco Bertoni
RD
Security Pattern SRL
Brescia, Italy

Francesco Regazzoni
AlaRI
Università della Svizzera italiana
Lugano, Switzerland

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-68772-4 ISBN 978-3-030-68773-1 (eBook)
<https://doi.org/10.1007/978-3-030-68773-1>

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 2021

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

It is our pleasure to welcome you to COSADE 2020, the 11th edition of the International Workshop on Constructive Side-Channel Analysis and Secure Design. The conference was originally planned in Lugano, Switzerland, April 1–3, 2020. However, the physical version of the conference had to be canceled due to COVID-19, and the conference was turned into a virtual event. Since 2010, COSADE has provided a well-established international platform for researchers, academics, and industry participants to present their work and their current research topics in implementation attacks, secure implementation, implementation attack-resilient architectures and schemes, secure design and evaluation, and practical attacks, test platforms, and open benchmarks.

COSADE 2020 was organized by Università della Svizzera italiana. This year, we received 36 papers, each of which was assigned to 4 reviewers. All the submissions went through a rigorous double-blind peer-review process. The Program Committee included 35 members from 15 countries, selected among experts from academia and industry in the areas of secure design, side channel attacks and countermeasures, and architectures and protocols. Overall, the program committee returned 176 reviews. During the decision process, 15 papers were selected for publication. These manuscripts are contained in these proceedings and the corresponding presentations were part of the COSADE 2020 program. We would like to express our gratitude to the program committee members and the 32 subreviewers for their reviews and for their active participation in the paper discussion phase.

In addition to the 15 presentations of selected papers, the program of COSADE 2020 was completed by 2 keynotes and one industrial session. The first keynote was titled “Tracking a Three Billion Dollar Bug with Electromagnetic Fault Injection” and was given by Colin O’Flynn from NewAE Technology Inc. and Dalhousie University. The talk explored a product safety incident through the lens of a hardware security researcher using tools with which hardware security researchers are familiar. The second keynote was titled “Security Aspects of CPSs: a Dive into Threat Modelling” and was given by Davide Ariu from Pluribus One. The talk provided an introduction to Threat Modeling, surveying possible Threat Modeling methodologies that can be applied to Cyber-Physical Systems of Systems and discussing the main challenges related to their application. The industrial session included three talks from Secure-IC (“Catalyzr tool: an environment to get your software secure; application to Post-Quantum Cryptography”), from Riscure (“Riscure tooling; ‘we love FI’”), and from FortifyIQ (“Applying the best security and development practices to HW security”).

We would like to thank the general chairs, Alberto Ferrante and Subhadeep Banik, and the local organizers, Liliana Sampietro and Nadia Ruggiero-Ciresa, from Università della Svizzera italiana, for the local organization. We would also like to thank the two Web administrators, Helmut Häfner and Lothar Hellmeier of the

University of Stuttgart, for maintaining the COSADE website for 2020. We are very grateful for the financial support received from our generous sponsors Hasler Stiftung, FortiyfIQ, NewAE Technology Inc., Riscure, Secure-IC, PQShield, and Rambus Cryptography Research.

October 2020

Guido Marco Bertoni
Francesco Regazzoni

Organization

Steering Committee

Jean-Luc Danger
Werner Schindler

Télécom Paris, France
Bundesamt für Sicherheit in der Informationstechnik
(BSI), Germany

General Chairs

Alberto Ferrante
Subhadeep Banik

ALaRI - USI, Switzerland
EPFL, Switzerland

Program Committee Chairs

Guido Marco Bertoni
Francesco Regazzoni

Security Pattern, Italy
ALaRI - USI, Switzerland

Program Committee

Divya Arora
Reza Azarderakhsh
Josep Balasch
Goerg T. Becker
Sonia Belaïd
Davide Bellizia
Shivam Bhasin
Elke De Mulder
Fabrizio De Santis
Baris Ege
Wieland Fischer
Samaneh Ghandali
Jorge Guajardo
Sylvain Guilley
Tim Güneysu
Annelie Heuser
Naofumi Homma
James Howe
Jens-Peter Kaps
Michael Kasper
Elif Bilge Kavun
Osnat Keren
Roel Maes

Intel, USA
Florida Atlantic University, USA
KU Leuven, Belgium
ESMT, Germany
CryptoExperts, France
UCL Crypto Group, Belgium
Nanyang Technological University, Singapore
Rambus Cryptography Research, USA
Siemens AG, Germany
Riscure, The Netherlands
Infineon Technologies, Germany
Google, USA
Bosch, USA
Secure-IC, France
Ruhr-Universität Bochum, Germany
CNRS, IRISA, France
Tohoku University, Japan
PQShield, UK
George Mason University, USA
Fraunhofer Singapore, Singapore
The University of Sheffield, UK
Bar-Ilan University, Israel
Intrinsic ID, The Netherlands

Pedro Massolino	Radboud University, The Netherlands
Marcel Medwed	NXP Semiconductors, Austria
Debdeep Mukhopadhyay	IIT Kharagpur, India
Makoto Nagata	Kobe University, Japan
Paolo Palmieri	University College Cork, Ireland
Colin O'Flynn	NewAE Technology Inc., Canada
Gerardo Pelosi	Politecnico di Milano, Italy
Ilia Polian	Universität Stuttgart, Germany
Kazuo Sakiyama	The University of Electro-Communications, Japan
Johanna Sepúlveda	Airbus, Germany
Patrick Schaumont	Worcester Polytechnic Institute, USA
Georg Sigl	TU Munich, Germany
Marc Stöttinger	Continental AG, Germany
Ruggero Susella	STMicroelectronics, Italy

Additional Reviewers

Abubakr Abdulgadir	Thorben Moos
Manaar Alam	Adriaan Peetermans
Florian Bache	Jan Richter-Brockmann
Jakub Breier	Sayandeep Saha
Olivier Bronchain	Thomas Schamberger
Lauren De Meyer	Tobias Schneider
William Diehl	Hermann Seuschek
Farnoud Farahmand	Hadi Soleimany
Michael Gruber	Patrick Struck
Dirmanto Jap	Lars Tebelmann
Pantea Kiaei	Jan Thoma
Kris Kwiatkowski	Rei Ueno
Yohei Hori	Florian Unterstein
Yang Li	Gilles Van Assche
Silvia Mella	Ville Yli-Mäyry
Julien Montmasson	Fan Zhang

Contents

Fault and Side Channel Attacks

Persistent Fault Analysis with Few Encryptions	3
<i>Sébastien Carré, Sylvain Guilley, and Olivier Rioul</i>	
A Template Attack to Reconstruct the Input of SHA-3 on an 8-Bit Device. . .	25
<i>Shih-Chun You and Markus G. Kuhn</i>	
Single-Trace Side-Channel Analysis on Polynomial-Based MAC Schemes . . .	43
<i>Rei Ueno, Kazuhide Fukushima, Yuto Nakano, Shinsaku Kiyomoto, and Naofumi Homma</i>	

Side-Channel Analysis Methodologies

Wavelet Scattering Transform and Ensemble Methods for Side-Channel Analysis	71
<i>Gabriel Destouet, Cécile Dumas, Anne Frassati, and Valérie Perrier</i>	
Scatter: a Missing Case?.	90
<i>Yuan Yuan Zhou, Sébastien Duval, and François-Xavier Standaert</i>	
Augmenting Leakage Detection Using Bootstrapping.	104
<i>Yuan Yao, Michael Tunstall, Elke De Mulder, Anton Kochepasov, and Patrick Schaumont</i>	

Evaluation of Attacks and Security

Security Assessment of White-Box Design Submissions of the CHES 2017 CTF Challenge	123
<i>Estuardo Alpirez Bock and Alexander Treff</i>	
On the Implementation Efficiency of Linear Regression-Based Side-Channel Attacks	147
<i>Maamar Ouladj, Sylvain Guilley, and Emmanuel Prouff</i>	

Side-Channel Attacks and Deep Learning

Kilroy Was Here: The First Step Towards Explainability of Neural Networks in Profiled Side-Channel Analysis.	175
<i>Daan van der Valk, Stjepan Picek, and Shivam Bhasin</i>	

Online Performance Evaluation of Deep Learning Networks for Profiled
Side-Channel Analysis 200
*Damien Robissout, Gabriel Zaid, Brice Colombier, Lilian Bossuet,
and Amaury Habrard*

Primitives and Tools for Physical Attacks Resistance

Custom Instruction Support for Modular Defense Against Side-Channel
and Fault Attacks 221
*Pantea Kiaei, Darius Mercadier, Pierre-Evariste Dagand,
Karine Heydemann, and Patrick Schaumont*

Processor Anchor to Increase the Robustness Against Fault Injection
and Cyber Attacks. 254
*Jean-Luc Danger, Adrien Facon, Sylvain Guilley, Karine Heydemann,
Ulrich Kühne, Abdelmalek Si Merabet, Michaël Timbert,
and Baptiste Pecatte*

Integrating Side Channel Security in the FPGA Hardware Design Flow 275
*Alessandro Barengi, Matteo Brevi, William Fornaciari,
Gerardo Pelosi, and Davide Zoni*

Side-Channel Countermeasures

Self-secured PUF: Protecting the Loop PUF by Masking 293
Lars Tebelmann, Jean-Luc Danger, and Michael Pehl

Leakage-Resilient Authenticated Encryption from Leakage-Resilient
Pseudorandom Functions 315
Juliane Krämer and Patrick Struck

Author Index 339