

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 series at <https://link.springer.com/bookseries/558>

Josep Balasch · Colin O’Flynn (Eds.)

Constructive Side-Channel Analysis and Secure Design

13th International Workshop, COSADE 2022
Leuven, Belgium, April 11–12, 2022
Proceedings

Editors

Josep Balasch
KU Leuven
Leuven, Belgium

Colin O'Flynn
Dalhousie University
Halifax, NS, Canada

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-030-99765-6

ISBN 978-3-030-99766-3 (eBook)

<https://doi.org/10.1007/978-3-030-99766-3>

© The Editor(s) (if applicable) and The Author(s), under exclusive license
to Springer Nature Switzerland AG 2022

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

The 13th International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE 2022), was held in Leuven, Belgium, during April 11–12, 2022. The COSADE series of workshops began in 2010 and provides a well-established international platform for researchers, academics, and industry participants to present their current research topics in implementation attacks, secure implementation, implementation attack-resilient architectures and schemes, secure design and evaluation, practical attacks, test platforms, and open benchmarks.

COSADE 2022 was organized by KU Leuven. This year, the workshop received 25 papers from authors in 14 countries. Each paper was reviewed in a double-blind peer-review process by four Program Committee members. The Program Committee included 31 members from 15 countries, selected among experts from academia and industry in the areas of secure design, side channel attacks and countermeasures, fault injection attacks, efficient implementations, and architectures and protocols. Overall, the Program Committee returned 94 reviews with the help of 11 additional reviewers. During the decision process, 12 papers were selected for publication. These manuscripts are contained in these proceedings and the corresponding presentations were part of the COSADE 2022 program. We would like to express our gratitude to the Program Committee members for their timely reviews, their active participation in the paper discussion phase, and their willingness to contribute to the shepherding of conditionally accepted papers.

In addition to the 12 presentations of selected papers, the program was completed by two keynotes and an industrial session. The first keynote entitled “Abstractions and Tooling for Leakage Evaluation” was given by Dan Page from the University of Bristol. The talk gave an overview of support for cryptography on the RISC-V ISA, as well as current research directions related to tooling for high-level leakage evaluation tasks. The second keynote entitled “Repurposing Wireless Stacks for In-Depth Security Analysis” was given by Jiska Classen from the Secure Mobile Networking Lab at TU Darmstadt. The talk presented recent research related to the exploration of closed-source wireless ecosystems, and demonstrated practical tools and discovered vulnerabilities. The industrial session included three talks from industry players in the field of hardware security.

We would like to thank the general chair, Benedikt Gierlichs, and the local organizers of KU Leuven for the organization, which made this workshop a memorable event. We are very grateful for the financial support received from our generous sponsors Riscure, Secure-IC, NewAE Technology, PQShield, Rambus, Texplained, and NXP. We would also like to thank the authors who submitted their work to COSADE 2022, without whom the workshop would not have been possible.

April 2022

Josep Balasch
Colin O’Flynn

Organization

Steering Committee

Jean-Luc Danger
Werner Schindler

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

General Chair

Benedikt Gierlichs

KU Leuven, Belgium

Program Committee Chairs

Colin O'Flynn
Josep Balasch

NewAE Technology Inc., Canada
KU Leuven, Belgium

Program Committee

Diego F. Aranha
Victor Arribas
Alessandro Barenghi
Shivam Bhasin
Jakub Breier
Olivier Bronchain
Chitchanok Chuengsatiansup
Fabrizio De Santis
Jean-Max Dutertre

Aarhus University, Denmark
Rambus Cryptography Research, The Netherlands
Politecnico di Milano, Italy
Nanyang Technological University, Singapore
Silicon Austria Labs, Austria
Université Catholique de Louvain, Belgium
University of Adelaide, Australia
Siemens AG, Germany
Ecole Nationale Supérieure des Mines de
Saint-Étienne (ENSMSE), France
Infineon Technologies, Germany
Worcester Polytechnic Institute, USA
CNRS/IRISA, France
Fraunhofer AISEC, Germany
Tohoku University, Japan
George Mason University, USA
University of Regensburg, Germany
NinjaLab, France
Microsoft Research, USA
Intrinsic ID, The Netherlands
NXP Semiconductors, Austria

Wieland Fischer
Fatemeh Ganji
Annelie Heuser
Johann Heyszl
Naofumi Homma
Jens-Peter Kaps
Juliane Krämer
Victor Lomne
Patrick Longa
Roel Maes
Marcel Medwed

Thorben Moos	Université Catholique de Louvain, Belgium
Daniel Page	University of Bristol, UK
Michael Pehl	Technical University of Munich, Germany
Stjepan Picek	Delft University of Technology, The Netherlands
Chester Rebeiro	Indian Institute of Technology Madras, India
Francesco Regazzoni	University of Amsterdam, The Netherlands, and Università della Svizzera italiana, Switzerland
Sujoy Sinha Roy	TU Graz, Austria
Marc Stöttinger	RheinMain University of Applied Sciences, Germany
Ruggero Susella	STMicroelectronics, Italy
Lennert Wouters	KU Leuven, Belgium
Fan Zhang	Zhejiang University, China

Additional Reviewers

Reetwik Das	Martin Rehberg
Lukas Giner	Thomas Schamberger
Mustafa Khairallah	Nikhilesh Singh
Soundes Marzougui	Emanuele Strieder
Tim Music	Lars Tebelmann
Antoon Purnal	

Contents

Machine/Deep Learning

Machine-Learning Assisted Side-Channel Attacks on RNS ECC Implementations Using Hybrid Feature Engineering	3
<i>Naila Mukhtar, Louiza Papachristodoulou, Apostolos P. Fournaris, Lejla Batina, and Yinan Kong</i>	
Focus is Key to Success: A Focal Loss Function for Deep Learning-Based Side-Channel Analysis	29
<i>Maikel Kerkhof, Lichao Wu, Guilherme Perin, and Stjepan Picek</i>	
On the Evaluation of Deep Learning-Based Side-Channel Analysis	49
<i>Lichao Wu, Guilherme Perin, and Stjepan Picek</i>	

Tools and References

A Second Look at the ASCAD Databases	75
<i>Maximilian Egger, Thomas Schamberger, Lars Tebelmann, Florian Lippert, and Georg Sigl</i>	
FIPAC: Thwarting Fault- and Software-Induced Control-Flow Attacks with ARM Pointer Authentication	100
<i>Robert Schilling, Pascal Nasahl, and Stefan Mangard</i>	
Body Biasing Injection: To Thin or Not to Thin the Substrate?	125
<i>G. Chancel, J.-M. Galliere, and P. Maurine</i>	

Attacks

On the Susceptibility of Texas Instruments SimpleLink Platform Microcontrollers to Non-invasive Physical Attacks	143
<i>Lennert Wouters, Benedikt Gierlichs, and Bart Preneel</i>	
Single-Trace Clustering Power Analysis of the Point-Swapping Procedure in the Three Point Ladder of Cortex-M4 SIKE	164
<i>Aymeric Genêt and Novak Kaluđerović</i>	
Canonical DPA Attack on HMAC-SHA1/SHA2	193
<i>Frank Schuhmacher</i>	

Masking

Provable Secure Software Masking in the Real-World 215
*Arthur Beckers, Lennert Wouters, Benedikt Gierlichs, Bart Preneel,
and Ingrid Verbauwhede*

Systematic Study of Decryption and Re-encryption Leakage: The Case
of Kyber 236
*Melissa Azouaoui, Olivier Bronchain, Clément Hoffmann,
Yulia Kuzovkova, Tobias Schneider, and François-Xavier Standaert*

Handcrafting: Improving Automated Masking in Hardware with Manual
Optimizations 257
Charles Momin, Gaëtan Cassiers, and François-Xavier Standaert

Author Index 277