Lecture Notes in Computer Science 13211

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

Springer

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

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

General Chair

Benedikt Gierlichs	KU Leuven, Belgium

Program Committee Chairs

Colin O'Flynn	NewAE Technology Inc., Canada
Josep Balasch	KU Leuven, Belgium

Program Committee

Diego F. Aranha	Aarhus University, Denmark
Victor Arribas	Rambus Cryptography Research, The Netherlands
Alessandro Barenghi	Politecnico di Milano, Italy
Shivam Bhasin	Nanyang Technological University, Singapore
Jakub Breier	Silicon Austria Labs, Austria
Olivier Bronchain	Université Catholique de Louvain, Belgium
Chitchanok Chuengsatiansup	University of Adelaide, Australia
Fabrizio De Santis	Siemens AG, Germany
Jean-Max Dutertre	Ecole Nationale Superieure des Mines de Saint-Étienne (ENSMSE), France
Wieland Fischer	Infineon Technologies, Germany
Fatemeh Ganji	Worcester Polytechnic Institute, USA
Annelie Heuser	CNRS/IRISA, France
Johann Heyszl	Fraunhofer AISEC, Germany
Naofumi Homma	Tohoku University, Japan
Jens-Peter Kaps	George Mason University, USA
Juliane Krämer	University of Regensburg, Germany
Victor Lomne	NinjaLab, France
Patrick Longa	Microsoft Research, USA
Roel Maes	Intrinsic ID, The Netherlands
Marcel Medwed	NXP Semiconductors, Austria

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

Contents

Masking