Lecture Notes in Computer Science 12244

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

Springer

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

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

General Chairs

Alberto Ferrante	ALaRI - USI, Switzerland
Subhadeep Banik	EPFL, Switzerland

Program Committee Chairs

Guido Marco Bertoni	Security Pattern, Italy
Francesco Regazzoni	ALaRI - USI, Switzerland

Program Committee

Divya Arora	Intel, USA
Reza Azarderakhsh	Florida Atlantic University, USA
Josep Balasch	KU Leuven, Belgium
Goerg T. Becker	ESMT, Germany
Sonia Belaïd	CryptoExperts, France
Davide Bellizia	UCL Crypto Group, Belgium
Shivam Bhasin	Nanyang Technological University, Singapore
Elke De Mulder	Rambus Cryptography Research, USA
Fabrizio De Santis	Siemens AG, Germany
Baris Ege	Riscure, The Netherlands
Wieland Fischer	Infineon Technologies, Germany
Samaneh Ghandali	Google, USA
Jorge Guajardo	Bosch, USA
Sylvain Guilley	Secure-IC, France
Tim Güneysu	Ruhr-Universität Bochum, Germany
Annelie Heuser	CNRS, IRISA, France
Naofumi Homma	Tohoku University, Japan
James Howe	PQShield, UK
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

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