Lecture Notes in Computer Science 8622

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

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

Emmanuel Prouff (Ed.)

Constructive Side-Channel Analysis and Secure Design

5th International Workshop, COSADE 2014
Paris, France, April 13–15, 2014
Revised Selected Papers

Springer

Editor
Emmanuel Prouff
FNISA
Paris
France

ISSN 0302-9743 ISSN 1611-3349 (electronic)
ISBN 978-3-319-10174-3 ISBN 978-3-319-10175-0 (eBook)
DOI 10.1007/978-3-319-10175-0

Library of Congress Control Number: 2014947448

Springer Cham Heidelberg New York Dordrecht London

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

The 5th workshop on Constructive Side-Channel Analysis and Secure Design (COSADE 2014), was held in Paris, France, during April 13–15, 2014. The workshop was supported by three golden sponsors (ANSSI, Secure IC, RISCURE) and three silver sponsors (Cryptography Research, INVIA, and SERMA Technologies).

COSADE 2014 received 51 submissions. Each submission was reviewed by at least 3, and on average 4, Program Committee members. The review process was double-blind, and conflicts of interest were carefully handled. The review process was handled through an online review system (Easychair) that supported discussions among Program Committee members. Eventually, the Program Committee selected 20 papers (a 39 % acceptance rate) for publication in the proceedings. The Committee decided to give the Best Paper Award to Mohamed Karroumi, Benjamin Richard, and Marc Joye for their paper "Addition with Blinded Operands," and the Best Student Paper Award to Guilherme Perin for his contribution to the paper "Attacking Randomized Exponentiations Using Unsupervised Learning." The program also included two invited talks, by Dmitry Nedospasov from the Security in Telecommunications (SECT) research group at the Berlin University of Technology (TU Berlin), and by Sebastian Faust from EPFL Lausanne.

Many people contributed to COSADE 2014. I thank the authors for contributing their excellent research. I thank the Program Committee members, and their external reviewers, for making a significant effort over an extended period of time to select the right papers for the program. I particularly thank Jean-luc Danger, the general chair, who took care of many practical details of the event. I also thank Sorin Huss and Werner Schindler for their support and their fruitful advices. I am very grateful to the Telecom Paristech members, and especially Guillaume Duc, for their excellent organization of the event. Finally, I thank our sponsors for supporting COSADE financially: ANSSI, Cryptography Research, Secure IC, Riscure, Invia, and Serma Technologies. COSADE 2014 collects truly exciting results in cryptographic engineering, from concepts to artifacts, from software to hardware, from attack to countermeasure. I feel privileged for the opportunity to develop the COSADE 2014 program. I hope that the papers in this proceedings will continue to inspire, guide, and clarify your academic and professional endeavors.

June 2014 Emmanuel Prouff

Organization

Program Committee

Ray Cheung	City University of Hong Kong, China
Christophe Clavier	University of Limoges, France
Jean-Sebastien Coron	University of Luxembourg, Luxembourg
Jean-Christophe Courrège	THALES Communications and Security S.A, France
Odile Derouet	NXP, Germany
Markus Dichtl	Siemens AG, Germany
Hermann Drexler	Giesecke and Devrient, Germany
Cécile Dumas	CEA, France
Benoit Feix	UL Transaction Security, France
Benedikt Gierlichs	KU Leuven, ESAT-COSIC, Belgium
Christophe Giraud	Oberthur Technologies, France
Sylvain Guilley	GET/ENST, CNRS/LTCI, France
Naofumi Homma	School of Information Sciences, Tohoku University, Japan
Michael Hutter	University of Technology Graz, IAIK, Austria
Eliane Jaulmes	ANSSI, France
Ilya Kizhvatov	RISCURE, The Netherlands
Markus Kuhn	University of Cambridge, UK
Thanh Ha Le	MORPHO, France
Stefan Mangard	Infineon Technologies, Germany
Amir Moradi	Horst Görtz Institute for IT-Security, Ruhr University Bochum, Germany
Debdeep Mukhopadhyay	IIT Kharagpur, India
Axel Poschmann	PACE, Nanyang Technological University, Singapore
Emmanuel Prouff	ANSSI, France
Anand Rajan	Intel, USA
Denis Real	DGA, Germany
Matthieu Rivain	CryptoExperts, France
Kazuo Sakiyama	The University of Electro-Communications, Japan
Patrick Schaumont	Virginia Tech, USA
Joern-Marc Schmidt	University of Technology Graz, IAIK, Austria
Francois-Xavier Standaert	UCL Crypto Group, Belgium
Yannick Teglia	ST Microelectronics, France
David Vigilant	Gemalto, The Netherlands
Carolyn Whitnall	University of Bristol, UK

Additional Reviewers

Agoyan, Michel
Andouard, Philippe
Balasch, Josep
Banciu, Valentina
Basu Roy, Debapriya
Battistello, Alberto
Bhasin, Shivam
Breier, Jakub
Buhan, Ileana
Carbone, Mathieu
Chen, Donald
Dambra, Arnaud
Danger, Jean-Luc
El Mrabet, Nadia
Endo, Sho
Farhady Ghalaty, Nahid
Finiasz, Matthieu
Fontaine, Arnaud
Ghosh, Santosh
Gross, Hannes
Guo, Xiaofei
Hajra, Suvadeep
Heuser, Annelie
Hoffmann, Lars
Jap, Dirmanto
Jessy, Clédière
Korak, Thomas
Kutzner, Sebastian
Li, Yang
Lomné, Victor
Omic, Jasmina
Pan, Jing
Poucheret, François
Razafindralambo, Tiana
Renauld, Mathieu
Reparaz, Oscar
Ricart, Andjy
Roche, Thomas
Rousselet, Mylène
Seysen, Martin
Stöttinger, Marc
Subidh Ali, Sk
Susella, Ruggero
Taha, Mostafa
Therond, Carine
Thierry, Loic
Tordella, Lucille
Unterluggauer, Thomas
van Oldeneel, Loic
Verneuil, Vincent
Villegas, Karine
Wenger, Erich
Witteman, Marc
Wojcik, Marcin
Wurcker, Antoine
Yao, Gavin

Contents