

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, Lancaster, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Zürich, Switzerland

John C. Mitchell

Stanford University, Stanford, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

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

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

© Springer International Publishing Switzerland 2014

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. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

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.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

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 Whittall	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

A Note on the Use of Margins to Compare Distinguishers	1
<i>Oscar Reparaz, Benedikt Gierlichs, and Ingrid Verbauwhede</i>	
A Theoretical Study of Kolmogorov-Smirnov Distinguishers	9
<i>Annelie Heuser, Olivier Rioul, and Sylvain Guilley</i>	
Pragmatism vs. Elegance: Comparing Two Approaches to Simple Power Attacks on AES	29
<i>Valentina Banciu and Elisabeth Oswald</i>	
Addition with Blinded Operands	41
<i>Mohamed Karroumi, Benjamin Richard, and Marc Joye</i>	
On the Use of RSA Public Exponent to Improve Implementation Efficiency and Side-Channel Resistance	56
<i>Christophe Giraud</i>	
Common Points on Elliptic Curves: The Achilles' Heel of Fault Attack Countermeasures.	69
<i>Alberto Battistello</i>	
On Adaptive Bandwidth Selection for Efficient MIA	82
<i>Mathieu Carbone, Sébastien Tiran, Sébastien Ordas, Michel Agoyan, Yannick Teglia, Gilles R. Ducharme, and Philippe Maurine</i>	
Generic DPA Attacks: Curse or Blessing?	98
<i>Oscar Reparaz, Benedikt Gierlichs, and Ingrid Verbauwhede</i>	
Support Vector Machines for Improved IP Detection with Soft Physical Hash Functions.	112
<i>Ludovic-Henri Gustin, François Durvaux, Stéphanie Kerckhof, François-Xavier Standaert, and Michel Verleysen</i>	
Collision-Correlation Attack Against a First-Order Masking Scheme for MAC Based on SHA-3.	129
<i>Luk Bettale, Emmanuelle Dottax, Laurie Genelle, and Gilles Piret</i>	
Attacking Randomized Exponentiations Using Unsupervised Learning.	144
<i>Guilherme Perin, Laurent Imbert, Lionel Torres, and Philippe Maurine</i>	
On the Optimal Pre-processing for Non-profiling Differential Power Analysis . . .	161
<i>Suvadeep Hajra and Debdeep Mukhopadhyay</i>	

Template Attacks on Different Devices	179
<i>Omar Choudary and Markus G. Kuhn</i>	
Using the Joint Distributions of a Cryptographic Function in Side Channel Analysis	199
<i>Yanis Linge, Cécile Dumas, and Sophie Lambert-Lacroix</i>	
A Multiple-Fault Injection Attack by Adaptive Timing Control Under Black-Box Conditions and a Countermeasure	214
<i>Sho Endo, Naofumi Homma, Yu-ichi Hayashi, Junko Takahashi, Hitoshi Fuji, and Takafumi Aoki</i>	
Adjusting Laser Injections for Fully Controlled Faults	229
<i>Franck Courbon, Philippe Loubet-Moundi, Jacques J.A. Fournier, and Assia Tria</i>	
ChipWhisperer: An Open-Source Platform for Hardware Embedded Security Research	243
<i>Colin O'Flynn and Zhizhang (David) Chen</i>	
Verifying Software Integrity in Embedded Systems: A Side Channel Approach.	261
<i>Mehari Msgna, Konstantinos Markantonakis, David Naccache, and Keith Mayes</i>	
Studying Leakages on an Embedded Biometric System Using Side Channel Analysis	281
<i>Maël Berthier, Yves Bocktaels, Julien Bringer, Hervé Chabanne, Taoufik Chouta, Jean-Luc Danger, Mélanie Favre, and Tarik Graba</i>	
On the Security of RSM - Presenting 5 First- and Second-Order Attacks	299
<i>Sebastian Kutzner and Axel Poschmann</i>	
Author Index	313