

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 <http://www.springer.com/series/7410>

Sonia Belaïd · Tim Güneysu (Eds.)

Smart Card Research and Advanced Applications

18th International Conference, CARDIS 2019
Prague, Czech Republic, November 11–13, 2019
Revised Selected Papers

Editors
Sonia Belaïd
CryptoExperts
Paris, France

Tim Güneysu 
Ruhr-Universität Bochum
Bochum, Germany

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-42067-3 ISBN 978-3-030-42068-0 (eBook)
<https://doi.org/10.1007/978-3-030-42068-0>

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 2020

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

These proceedings contain the papers selected for presentation at the 18th International Conference on Smart Card Research and Advanced Applications (CARDIS 2019), held in Prague, Czech Republic, during November 11–13, 2019. The conference was organized by the Faculty of Information Technology of the Czech Technical University in Prague, Czech Republic.

CARDIS provides a space for security experts from industry and academia to exchange ideas on security of smart cards and related applications. Those objects have been part of our daily life for years: banking and SIM cards, electronic passports, etc. But the world is constantly changing; a secure element, such as smart cards, is now being implemented in many cases, for example as a hardware root of trust for larger systems. As such, smartcard security and core ingredients such as applied cryptography is a key enabler for the security of the entire system. At the same time, and with the growing use of smartcard technology, the attack surface is increasing, from physical attacks to logical attacks, from local attacks to remote attacks, and more recently combined attacks. It is more important than ever that we understand how smart cards and related systems, can be secured.

This year, CARDIS received 31 papers from a large number of international countries. Each paper was reviewed by three independent reviewers. The selection of 15 papers to fill the technical program was accomplished based on 142 written reviews. This task was performed by the 31 members of the Program Committee with the help of 28 external reviewers. The technical program also featured two invited talks. The first invited speaker, Peter Schwabe (Radboud University in Nijmegen, The Netherlands), presented “Post-quantum crypto on ARM Cortex-M” and the second speaker, Gilles Barthe (Max-Planck Institute in Bochum, Germany, and IMDEA Software Institute, Spain), presented “Formal Verification of Side-Channel Resistance.” We would like to thank the general chair, Martin Novotný, for the great venue and smooth operation of the conference.

We would also like to thank the Program Committee and the external reviewers for their thorough work, which enabled the technical program to be of high quality, as well as the Steering Committee for giving us the opportunity to serve as program chairs at such a prestigious conference. The financial support of all the sponsors was highly appreciated and greatly facilitated the organization of the conference. We would like to thank the sponsors Thales, Infineon, Rambus, PQSHIELD, NewAE, Riscure NAGRA and FortifyIQ, CryptoExperts, ima, and KAOS for their support and collaboration. Furthermore, we would like to thank the authors who submitted their work to CARDIS 2019, without whom the conference would not have been possible.

January 2020

Sonia Belaïd
Tim Güneysu

Organization

Program Committee

Josep Balasch	Katholieke Universiteit Leuven, Belgium
Alessandro Barenghi	Politecnico di Milano, Italy
Sonia Belaïd	CryptoExperts, France
Begül Bilgin	Cryptography Research, USA
Thomas De Cnudde	Katholieke Universiteit Leuven, Belgium
Elke De Mulder	Cryptography Research, USA
Thomas Eisenbarth	WPI, USA
Junfeng Fan	Open Security Research, The Netherlands
Jean-Bernard Fischer	NagraVision, Switzerland
Domenic Forte	University of Florida, USA
Dahmun Goudarzi	PQShield, UK
Daniel Gruss	Institute for Applied Information Processing and Communications, Graz University of Technology, Austria
Tim Güneysu	Ruhr-Universität Bochum and DFKI, Germany
Annelie Heuser	CNRS, IRISA, France
Kerstin Lemke-Rust	Bonn-Rhein-Sieg University of Applied Sciences, Germany
Roel Maes	Intrinsic ID, USA
Amir Moradi	Ruhr-Universität Bochum, Germany
Debdeep Mukhopadhyay	IIT Kharagpur, India
Colin O’Flynn	NewAE Technology Inc., Canada
Axel Poschmann	xen1thLabs, UAE
Emmanuel Prouff	ANSSI, France
Thomas Pöppelmann	Infineon Technologies AG, Germany
Francesco Regazzoni	ALaRI – USI, Switzerland
Thomas Roche	NinjaLab, France
Kazuo Sakiyama	The University of Electro-Communications, Japan
Erkay Savas	Sabancı University, Turkey
Tobias Schneider	NXP Semiconductors, The Netherlands
Peter Schwabe	Radboud University, The Netherlands
Carolyn Whinnall	University of Bristol, UK
Yuval Yarom	The University of Adelaide and Data61/CSIRO, Australia
Rina Zeitoun	IDEMIA, France

Additional Reviewers

Andreeva, Elena
Barbu, Guillaume
Bermudo Mera, Jose Maria
Bouffard, Guillaume
Bronchain, Olivier
Cao, Yang
Costa Massolino, Pedro Maat
Cuong, Bien
De Meyer, Lauren
Fritzmman, Tim
Fritzschn, Clemens
Giner, Lukas
Gonzalez, Ruben
Hara-Azumi, Yuko

Kannwischer, Matthias
Kavun, Elif Bilge
Li, Yang
Maniatakos, Mihalıs
Pelletier, Hervé
Rebeiro, Chester
Richter, Bastian
Saha, Sayandeep
Seker, Okan
Tunstall, Mike
Villegas, Karine
Wood, Tim
Yao, Yuan

Contents

System-on-a-Chip Security

In-situ Extraction of Randomness from Computer Architecture Through Hardware Performance Counters	3
<i>Manaar Alam, Astikey Singh, Sarani Bhattacharya, Kuheli Pratihari, and Debdeep Mukhopadhyay</i>	
Optimized Threshold Implementations: Minimizing the Latency of Secure Cryptographic Accelerators	20
<i>Dušan Božilov, Miroslav Knežević, and Ventzislav Nikov</i>	
Breaking the Lightweight Secure PUF: Understanding the Relation of Input Transformations and Machine Learning Resistance	40
<i>Nils Wisiol, Georg T. Becker, Marian Margraf, Tudor A. A. Soroceanu, Johannes Tobisch, and Benjamin Zengin</i>	

Post-Quantum Cryptography

Improving Speed of Dilithium's Signing Procedure	57
<i>Prasanna Ravi, Sourav Sen Gupta, Anupam Chattopadhyay, and Shivam Bhasin</i>	
An Efficient and Provable Masked Implementation of \mathbf{qTESLA}	74
<i>François Gérard and Mélissa Rossi</i>	

Side-Channel Analysis

Side-Channel Attacks on Blinded Scalar Multiplications Revisited.	95
<i>Thomas Roche, Laurent Imbert, and Victor Lomné</i>	
Remote Side-Channel Attacks on Heterogeneous SoC	109
<i>Joseph Gravellier, Jean-Max Dutertre, Yannick Tégli, Philippe Loubet Moundi, and Francis Olivier</i>	
Optimal Collision Side-Channel Attacks.	126
<i>Cezary Glowacz and Vincent Grosso</i>	

Microarchitectural Attacks

A Bit-Level Approach to Side Channel Based Disassembling	143
<i>Valence Cristiani, Maxime Lecomte, and Thomas Hiscock</i>	

CCCiCC: A Cross-Core Cache-Independent Covert Channel on AMD Family 15h CPUs	159
<i>Carl-Daniel Hailfinger, Kerstin Lemke-Rust, and Christof Paar</i>	
Design Considerations for EM Pulse Fault Injection	176
<i>Arthur Beckers, Masahiro Kinugawa, Yuichi Hayashi, Daisuke Fujimoto, Josep Balasch, Benedikt Gierlichs, and Ingrid Verbauwhede</i>	
Cryptographic Primitives	
Lightweight MACs from Universal Hash Functions.	195
<i>Sébastien Duval and Gaëtan Leurent</i>	
FELICS-AEAD: Benchmarking of Lightweight Authenticated Encryption Algorithms.	216
<i>Luan Cardoso dos Santos, Johann Großschädl, and Alex Biryukov</i>	
Advances in Side-Channel Analysis	
A Comparison of χ^2-Test and Mutual Information as Distinguisher for Side-Channel Analysis	237
<i>Bastian Richter, David Knichel, and Amir Moradi</i>	
Key Enumeration from the Adversarial Viewpoint: When to Stop Measuring and Start Enumerating?	252
<i>Melissa Azouaoui, Romain Poussier, François-Xavier Standaert, and Vincent Verneuil</i>	
Author Index	269