

*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*

Friedemann Mattern

*ETH Zurich, Zurich, Switzerland*

John C. Mitchell

*Stanford University, Stanford, CA, USA*

Moni Naor

*Weizmann Institute of Science, Rehovot, Israel*

C. Pandu Rangan

*Indian Institute of Technology Madras, Chennai, 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*

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

Begül Bilgin · Jean-Bernard Fischer (Eds.)

# Smart Card Research and Advanced Applications

17th International Conference, CARDIS 2018  
Montpellier, France, November 12–14, 2018  
Revised Selected Papers

*Editors*

Begül Bilgin  
Rambus - Cryptography Research  
Rotterdam, Zuid-Holland, The Netherlands

Jean-Bernard Fischer  
Nagravision  
Cheseaux-sur-Lausanne, Vaud, Switzerland

KU Leuven  
Leuven-Heverlee, Belgium

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-030-15461-5              ISBN 978-3-030-15462-2 (eBook)  
<https://doi.org/10.1007/978-3-030-15462-2>

Library of Congress Control Number: 2019933892

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 2019

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, express 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 17th Smart Card Research and Advanced Applications Conference (CARDIS 2018), which was held in Montpellier, France, during November 12–14, 2018, and organized by the Montpellier Laboratory of Informatics, Robotics and Microelectronics (LIRMM).

Since 1994, CARDIS has provided a forum for experts from industry and academia to exchange ideas on the security of smart cards and related applications. The smart card object has been part of our daily life for so many years in the form of personal devices (banking cards, SIM cards, electronic IDs, etc.) that we do not remember a life without it. In relation to smart card security, the root of trust of embedded solutions is becoming key as Machine-to-Machine (M2M) and Internet of Things (IoT) applications are increasing massively. This increased exposure naturally widens the attack space, whether physical or logical, local or remote. It is more important than ever to understand how smart cards and other embedded devices can be secured by discussing all aspects of their design, development, deployment, evaluation, and application.

This year, CARDIS received 28 valid submissions from 12 countries. Each paper was double-blind reviewed by at least three independent reviewers. We selected 13 papers based on 102 written reviews from the 30 members of the Program Committee with the help of 35 external reviewers. The technical program also featured three invited talks: Frank Piessens from KU Leuven in Belgium presented “Security Specifications for the Hardware/Software Interface”; Benoit Feix from eshard in France presented “Exploiting a New Dimension in Side-Channel Analysis: Scatter on Symmetric and Asymmetric Embedded Cryptography”; and Wyseur Brecht from Nagravision in Switzerland presented “Challenges in Securing Industrial IoT and Critical Infrastructure.” A free tutorial was held co-located with the conference: “Understanding Leakage Detection” organized by the REASSURE Consortium.

We would like to thank the general chair, Philippe Maurine, for the great venue and smooth operation of the conference. We would also like to express our gratitude to the Program Committee and the external reviewers for their thorough work, which enabled the technical program to be of such high quality, and 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 thank the sponsors: ANSSI, CNRS, Gemalto, Nagra-Kudelski, LETI-CEA, LIRMM, Rambus, STMicroelectronics, University of Montpellier. Last but not least, we would like to thank all the authors who submitted their work to CARDIS 2018.

January 2019

Begül Bilgin  
Jean-Bernard Fischer

# Organization

## General Chair

Philippe Maurine

University of Montpellier, France

## Program Chairs

Begül Bilgin

Rambus-Cryptography Research, The Netherlands  
and KU Leuven, Belgium

Jean-Bernard Fischer

Nagravision, Switzerland

## Steering Committee

François-Xavier Standaert  
(Chair)

UC Louvain, Belgium

Thomas Eisenbarth

Worcester Polytechnic Institute, USA

Aurélien Francillon

EURECOM, France

Edouard de Jong

De Jong Frz. Holding BV

Marc Joye

NXP Semiconductors, USA

Konstantinos

Royal Holloway University of London, UK

Markantonakis

Amir Moradi

Ruhr University Bochum, Germany

Svetla Nikova

KU Leuven, Belgium

Pierre Paradinas

Inria and CNAM, France

Jean-Jacques Quisquater

UC Louvain, Belgium

Francesco Regazzoni

University of Lugano, Switzerland

Yannick Tégli

Gemalto, France

## Program Committee

Josep Balasch

KU Leuven, Belgium

Guillaume Barbu

IDEMIA, France

Alessandro Barengi

Politecnico di Milano, Italy

Sonia Belaid

CryptoExperts, France

Thomas De Cnudde

KU Leuven, Belgium

Jeroen Delvaux

Nanyang Technological University, Singapore

Thomas Eisenbarth

Universität zu Lübeck, Germany

Benoix Feix

eshard, France

Domenic Forte

University of Florida, USA

Aurélien Francillon

Eurecom, France

Elke De Mulder

Rambus-Cryptography Research, USA

Hannes Gross

TU Graz, Austria

|                      |   |
|----------------------|---|
| Vincent Grosso       | Radboud University, The Netherlands           |
| Annelie Heuser       | CNRS/IRISA, France                            |
| Marc Joye            | NXP Semiconductors, USA                       |
| Kerstin Lemke-Rust   | Bonn-Rhein-Sieg University, Germany           |
| Roel Maes            | Intrinsic ID, The Netherlands                 |
| Oliver Mischke       | Infineon, Germany                             |
| Amir Moradi          | Ruhr University Bochum, Germany               |
| Debdeep Mukhopadhyay | IIT Kharagpur, India                          |
| Axel Y. Poschmann    | DarkMatter, UAE                               |
| Emmanuel Prouff      | ANSSI, France                                 |
| Francesco Regazoni   | ALaRi, Switzerland                            |
| Kazuo Sakiyama       | University of Electro-Communications, Japan   |
| Erkay Savaş          | Sabanci University, Turkey                    |
| Tobias Schneider     | UC Louvain, Belgium                           |
| Yannick Teglia       | Gemalto, France                               |
| Yuval Yarom          | University of Adelaide, and Data61, Australia |
| Carolyn Whittall     | University of Bristol, UK                     |
| Marc Witteman        | Riscure, The Netherlands                      |

## Additional Reviewers

|                     |                    |
|---------------------|--------------------|
| Alberto Battistello | Erdinc Ozturk      |
| Ryad Benadjila      | Jungmin Park       |
| Shivam Bhasin       | Sikhar Patranabis  |
| Manuel Bluhm        | Thomas Pöppelmann  |
| Olivier Bronchain   | Bastian Richter    |
| Giovanni Camurati   | Debapriya Basu Roy |
| Nicolas Debande     | Okan Seker         |
| David El-Baze       | Rémi Strullu       |
| Berk Gulmezoglu     | Shahin Tajik       |
| Christoph Herbst    | Benjamin Timon     |
| James Howe          | Lucille Tordella   |
| Malika Izabachene   | Rei Ueno           |
| Angshuman Karmakar  | Aurelien Vasselle  |
| Elif Bilge Kavun    | Nikita Veshchikov  |
| Albert Levi         | Junwei Wang        |
| Marco Martinoli     | Felix Wegener      |
| Ahmet Can Mert      | Jan Wichelmann     |
| Marius Muench       |                    |

# Contents

|  |     |
|--|-----|
| Convolutional Neural Network Based Side-Channel Attacks<br>in Time-Frequency Representations . . . . .                                 | 1   |
| <i>Guang Yang, Huizhong Li, Jingdian Ming, and Yongbin Zhou</i>  |     |
| A Systematic Study of the Impact of Graphical Models on Inference-Based<br>Attacks on AES . . . . .                                    | 18  |
| <i>Joey Green, Arnab Roy, and Elisabeth Oswald</i>   |     |
| Improving Side-Channel Analysis Through Semi-supervised Learning . . . . .   | 35  |
| <i>Stjepan Picek, Annelie Heuser, Alan Jovic, Karlo Knezevic,<br/>and Tania Richmond</i>   |     |
| Non-profiled Mask Recovery: The Impact of Independent<br>Component Analysis . . . . .  | 51  |
| <i>Si Gao, Elisabeth Oswald, Hua Chen, and Wei Xi</i>  |     |
| How (Not) to Use Welch's T-Test in Side-Channel Security Evaluations . . . .   | 65  |
| <i>François-Xavier Standaert</i>   |     |
| Scalable Key Rank Estimation (and Key Enumeration) Algorithm<br>for Large Keys . . . . .   | 80  |
| <i>Vincent Grosso</i>  |     |
| Shorter Messages and Faster Post-Quantum Encryption with Round5<br>on Cortex M . . . . .   | 95  |
| <i>Markku-Juhani O. Saarinen, Sauvik Bhattacharya,<br/>Oscar Garcia-Morchon, Ronald Rietman, Ludo Tolhuizen,<br/>and Zhenfei Zhang</i> |     |
| Yet Another Size Record for AES: A First-Order SCA Secure<br>AES S-Box Based on $GF(2^8)$ Multiplication . . . . .                     | 111 |
| <i>Felix Wegener and Amir Moradi</i>   |     |
| Jitter Estimation with High Accuracy for Oscillator-Based TRNGs . . . . .  | 125 |
| <i>Shaofeng Zhu, Hua Chen, Limin Fan, Meihui Chen, Wei Xi,<br/>and Dengguo Feng</i>  |     |
| Electromagnetic Activity vs. Logical Activity: Near Field Scans<br>for Reverse Engineering . . . . .                                   | 140 |
| <i>Marc Lacruche and Philippe Maurine</i>  |     |



|  |     |
|--|-----|
| An In-Depth and Black-Box Characterization of the Effects of Laser<br>Pulses on ATmega328P . . . . .       | 156 |
| <i>Dilip S. V. Kumar, Arthur Beckers, Josep Balasch, Benedikt Gierlichs,<br/>and Ingrid Verbauwhede</i>    |     |
| Breaking All the Things—A Systematic Survey of Firmware Extraction<br>Techniques for IoT Devices . . . . . | 171 |
| <i>Sebastian Vasile, David Oswald, and Tom Chothia</i>   |     |
| Exploiting JCVM on Smart Cards Using Forged References<br>in the API Calls . . . . .                       | 186 |
| <i>Sergei Volokitin</i>  |     |
| <b>Author Index</b> . . . . .  | 201 |