# Contents

## Side-Channel Attacks

Side-Channel Attacks on SHA-1-Based Product Authentication ICs

*David Oswald*

Enhancing Dimensionality Reduction Methods for Side-Channel Attacks

*Eleonora Cagli, Cécile Dumas, and Emmanuel Prouff*

A Semi-Parametric Approach for Side-Channel Attacks on Protected RSA Implementations

*Guilherme Perin and Łukasz Chmielewski*

## Java Cards

seTPM: Towards Flexible Trusted Computing on Mobile Devices Based on GlobalPlatform Secure Elements

*Sergej Proskurin, Michael Weiβ, and Georg Sigl*

Java Card Virtual Machine Compromising from a Bytecode Verified Applet

*Julien Lancia and Guillaume Bouffard*

Misuse of Frame Creation to Exploit Stack Underflow Attacks on Java Card

*Benoît Laugier and Tiana Razafindralambo*

## Evaluation Tools

From Code Review to Fault Injection Attacks: Filling the Gap Using Fault Model Inference

*Louis Dureuıl, Marie-Laure Potet, Philippe de Choudens, Cécile Dumas, and Jessy Clédière*

Comparing Approaches to Rank Estimation for Side-Channel Security Evaluations

*Romain Poussier, Vincent Grosso, and François-Xavier Standaert*

Collision for Estimating SCA Measurement Quality and Related Applications

*Ibrahim Diop, Mathieu Carbone, Sebastien Ordas, Yanis Linge, Pierre Yvan Liardet, and Philippe Maurine*
Fault Attacks

Protecting the Control Flow of Embedded Processors against Fault Attacks . . . . 161
  Mario Werner, Erich Wenger, and Stefan Mangard

Efficient Design and Evaluation of Countermeasures against Fault Attacks

Using Formal Verification ................................................................. 177
  Lucien Goubet, Karine Heydemann, Emmanuelle Encrenaz,
  and Ronald De Keulenaer

Precise Laser Fault Injections into 90 nm and 45 nm SRAM-cells .............. 193
  Bodo Selmke, Stefan Brummer, Johann Heyszl, and Georg Sigl

Countermeasures

The Not-so-Distant Future: Distance-Bounding Protocols on Smartphones . . 209
  Sébastien Gambs, Carlos Eduardo Rosar Kós Lassance,
  and Cristina Onete

Towards Fresh and Hybrid Re-Keying Schemes with Beyond Birthday Security ................................................................. 225
  Christoph Dobraunig, François Koeune, Stefan Mangard,
  Florian Mendel, and François-Xavier Standaert

On the Security of Balanced Encoding Countermeasures ....................... 242
  Yoo-Seung Won, Philip Hodgers, Máire O’Neill, and Dong-Guk Han

Implementations

Higher-Order Threshold Implementation of the AES S-Box ..................... 259
  Thomas De Cnudde, Begül Bilgin, Oscar Reparaz, Ventzislav Nikov,
  and Svetla Nikova

Compact Implementations of Multi-Sbox Designs .............................. 273
  Begül Bilgin, Miroslav Knežević, Ventzislav Nikov, and Svetla Nikova

Author Index .................................................................................. 287
Smart Card Research and Advanced Applications
14th International Conference, CARDIS 2015, Bochum, Germany, November 4-6, 2015. Revised Selected Papers
Homma, N.; Medwed, M. (Eds.)
2016, XII, 287 p. 92 illus. in color., Softcover
ISBN: 978-3-319-31270-5