## Contents

### Side-Channel Attacks

- Side-Channel Attacks on SHA-1-Based Product Authentication ICs... 3  
  *David Oswald*

- Enhancing Dimensionality Reduction Methods for Side-Channel Attacks... 15  
  *Eleonora Cagli, Cécile Dumas, and Emmanuel Prouff*

- A Semi-Parametric Approach for Side-Channel Attacks on Protected RSA Implementations... 34  
  *Guilherme Perin and Łukasz Chmielewski*

### Java Cards

- seTPM: Towards Flexible Trusted Computing on Mobile Devices Based on GlobalPlatform Secure Elements... 57  
  *Sergej Proskurin, Michael Weiß, and Georg Sigl*

- Java Card Virtual Machine Compromising from a Bytecode Verified Applet... 75  
  *Julien Lancia and Guillaume Bouffard*

- Misuse of Frame Creation to Exploit Stack Underflow Attacks on Java Card... 89  
  *Benoit Laugier and Tiana Razafindralambo*

### Evaluation Tools

- From Code Review to Fault Injection Attacks: Filling the Gap Using Fault Model Inference... 107  
  *Louis Dureuil, Marie-Laure Potet, Philippe de Choudens, Cécile Dumas, and Jessy Clédière*

- Comparing Approaches to Rank Estimation for Side-Channel Security Evaluations... 125  
  *Romain Poussier, Vincent Grosso, and François-Xavier Standaert*

- Collision for Estimating SCA Measurement Quality and Related Applications... 143  
  *Ibrahima 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

Mario Werner, Erich Wenger, and Stefan Mangard

Efficient Design and Evaluation of Countermeasures against Fault Attacks

Using Formal Verification

Lucien Goubet, Karine Heydemann, Emmanuelle Encrenaz, and Ronald De Keulenaer

Precise Laser Fault Injections into 90 nm and 45 nm SRAM-cells

Bodo Selmke, Stefan Brummer, Johann Heyszl, and Georg Sigl

### Countermeasures

The Not-so-Distant Future: Distance-Bounding Protocols on Smartphones

Sébastien Gambs, Carlos Eduardo Rosar Kós Lassance, and Cristina Onete

Towards Fresh and Hybrid Re-Keying Schemes with Beyond Birthday Security

Christoph Dobraunig, François Koeune, Stefan Mangard, Florian Mendel, and François-Xavier Standaert

On the Security of Balanced Encoding Countermeasures

Yoo-Seung Won, Philip Hodgers, Máire O’Neill, and Dong-Guk Han

### Implementations

Higher-Order Threshold Implementation of the AES S-Box

Thomas De Cnudde, Begül Bilgin, Oscar Reparaz, Ventzislav Nikov, and Svetla Nikova

Compact Implementations of Multi-Sbox Designs

Begül Bilgin, Miroslav Knežević, Ventzislav Nikov, and Svetla Nikova

Author Index
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