

Naofumi Homma · Marcel Medwed (Eds.)

Smart Card Research and Advanced Applications

14th International Conference, CARDIS 2015
Bochum, Germany, November 4–6, 2015
Revised Selected Papers

Contents

Side-Channel Attacks

Side-Channel Attacks on SHA-1-Based Product Authentication ICs.	3
<i>David Oswald</i>	
Enhancing Dimensionality Reduction Methods for Side-Channel Attacks	15
<i>Eleonora Cagli, Cécile Dumas, and Emmanuel Prouff</i>	
A Semi-Parametric Approach for Side-Channel Attacks on Protected RSA Implementations	34
<i>Guilherme Perin and Łukasz Chmielewski</i>	

Java Cards

seTPM: Towards Flexible Trusted Computing on Mobile Devices Based on GlobalPlatform Secure Elements.	57
<i>Sergej Proskurin, Michael Weiß, and Georg Sigl</i>	
Java Card Virtual Machine Compromising from a Bytecode Verified Applet	75
<i>Julien Lancia and Guillaume Bouffard</i>	
Misuse of Frame Creation to Exploit Stack Underflow Attacks on Java Card	89
<i>Benoit Laugier and Tiana Razafindralambo</i>	

Evaluation Tools

From Code Review to Fault Injection Attacks: Filling the Gap Using Fault Model Inference	107
<i>Louis Dureuil, Marie-Laure Potet, Philippe de Choudens, Cécile Dumas, and Jessy Clédière</i>	
Comparing Approaches to Rank Estimation for Side-Channel Security Evaluations	125
<i>Romain Poussier, Vincent Grosso, and François-Xavier Standaert</i>	
Collision for Estimating SCA Measurement Quality and Related Applications	143
<i>Ibrahima Diop, Mathieu Carbone, Sebastien Ordas, Yanis Linge, Pierre Yvan Liardet, and Philippe Maurine</i>	

Fault Attacks

Protecting the Control Flow of Embedded Processors against Fault Attacks	161
<i>Mario Werner, Erich Wenger, and Stefan Mangard</i>	
Efficient Design and Evaluation of Countermeasures against Fault Attacks Using Formal Verification	177
<i>Lucien Goubet, Karine Heydemann, Emmanuelle Encrenaz, and Ronald De Keulenaer</i>	
Precise Laser Fault Injections into 90 nm and 45 nm SRAM-cells	193
<i>Bodo Selmke, Stefan Brummer, Johann Heyszl, and Georg Sigl</i>	

Countermeasures

The Not-so-Distant Future: Distance-Bounding Protocols on Smartphones . . .	209
<i>Sébastien Gams, Carlos Eduardo Rosar Kós Lassance, and Cristina Onete</i>	
Towards Fresh and Hybrid Re-Keying Schemes with Beyond Birthday Security	225
<i>Christoph Dobraunig, François Koeune, Stefan Mangard, Florian Mendel, and François-Xavier Standaert</i>	
On the Security of Balanced Encoding Countermeasures	242
<i>Yoo-Seung Won, Philip Hodgers, Máire O'Neill, and Dong-Guk Han</i>	

Implementations

Higher-Order Threshold Implementation of the AES S-Box	259
<i>Thomas De Cnudde, Begül Bilgin, Oscar Reparaz, Ventzislav Nikov, and Svetla Nikova</i>	
Compact Implementations of Multi-Sbox Designs	273
<i>Begül Bilgin, Miroslav Knežević, Ventzislav Nikov, and Svetla Nikova</i>	
Author Index	287