

Contents

Security Technologies - Session Chair: Benedikt Gierlichs

Evaluation of ASIC Implementation of Physical Random Number Generators Using RS Latches	3
<i>Hiroataka Kokubo, Dai Yamamoto, Masahiko Takenaka, Kouichi Itoh, and Naoya Torii</i>	

From New Technologies to New Solutions: Exploiting FRAM Memories to Enhance Physical Security	16
<i>Stéphanie Kerckhof, François-Xavier Standaert, and Eric Peeters</i>	

Attacks on Masking - Session Chair: Michael Hutter

Low Entropy Masking Schemes, Revisited	33
<i>Vincent Grosso, François-Xavier Standaert, and Emmanuel Prouff</i>	

On the Vulnerability of Low Entropy Masking Schemes	44
<i>Xin Ye and Thomas Eisenbarth</i>	

A Machine Learning Approach Against a Masked AES	61
<i>Liran Lerman, Stephane Fernandes Medeiros, Gianluca Bontempi, and Olivier Markowitch</i>	

Side Channel Attacks - Session Chair: François-Xavier Standaert

Clustering Algorithms for Non-profiled Single-Execution Attacks on Exponentiations	79
<i>Johann Heyszl, Andreas Ibing, Stefan Mangard, Fabrizio De Santis, and Georg Sigl</i>	

Optimization of Power Analysis Using Neural Network	94
<i>Zdenek Martinasek, Jan Hajny, and Lukas Malina</i>	

Time-Frequency Analysis for Second-Order Attacks	108
<i>Pierre Belgaric, Shivam Bhasin, Nicolas Bruneau, Jean-Luc Danger, Nicolas Debande, Sylvain Guilley, Annelie Heuser, Zakaria Najm, and Olivier Rioul</i>	

Software and Protocol Analysis - Session Chair: Lex Schoonen

Vulnerability Analysis of a Commercial .NET Smart Card	125
<i>Behrang Fouladi, Konstantinos Markantonakis, and Keith Mayes</i>	

Manipulating the Frame Information with an Underflow Attack	140
<i>Emilie Faugeron</i>	
Formal Security Analysis and Improvement of a Hash-Based NFC M-Coupon Protocol.	152
<i>Ali Alshehri and Steve Schneider</i>	
Side Channel Countermeasures - Session Chair: Svetla Nikova	
Revisiting Atomic Patterns for Scalar Multiplications on Elliptic Curves. . . .	171
<i>Franck Rondepierre</i>	
Efficient and First-Order DPA Resistant Implementations of KECCAK	187
<i>Begül Bilgin, Joan Daemen, Ventsislav Nikov, Svetla Nikova, Vincent Rijmen, and Gilles Van Assche</i>	
Practical Analysis of RSA Countermeasures Against Side-Channel Electromagnetic Attacks	200
<i>Guilherme Perin, Laurent Imbert, Lionel Torres, and Philippe Maurine</i>	
Side Channel and Fault Attacks - Session Chair: Berndt Gammel	
The Temperature Side Channel and Heating Fault Attacks	219
<i>Michael Hutter and Jörn-Marc Schmidt</i>	
Glitch It If You Can: Parameter Search Strategies for Successful Fault Injection	236
<i>Rafael Boix Carpi, Stjepan Picek, Lejla Batina, Federico Menarini, Domagoj Jakobovic, and Marin Golub</i>	
Efficient Template Attacks.	253
<i>Omar Choudary and Markus G. Kuhn</i>	
Author Index	271

Smart Card Research and Advanced Applications
12th International Conference, CARDIS 2013, Berlin,
Germany, November 27-29, 2013. Revised Selected
Papers

Francillon, A.; Rohatgi, P. (Eds.)

2014, XII, 271 p. 111 illus., Softcover

ISBN: 978-3-319-08301-8