

# Contents

## Side-Channel Attacks

Improving Non-profiled Attacks on Exponentiations Based on Clustering and Extracting Leakage from Multi-channel High-Resolution EM Measurements . . . . .	3
<i>Robert Specht, Johann Heyszl, Martin Kleinsteuber, and Georg Sigl</i>	
Template Attacks vs. Machine Learning Revisited (and the Curse of Dimensionality in Side-Channel Analysis) . . . . .	20
<i>Liran Lerman, Romain Poussier, Gianluca Bontempi, Olivier Markowitch, and François-Xavier Standaert</i>	
Efficient Selection of Time Samples for Higher-Order DPA with Projection Pursuits . . . . .	34
<i>François Durvaux, François-Xavier Standaert, Nicolas Veyrat-Charvillon, Jean-Baptiste Mairy, and Yves Deville</i>	
Exploring the Resilience of Some Lightweight Ciphers Against Profiled Single Trace Attacks . . . . .	51
<i>Valentina Banciu, Elisabeth Oswald, and Carolyn Whitnall</i>	
Two Operands of Multipliers in Side-Channel Attack . . . . .	64
<i>Takeshi Sugawara, Daisuke Suzuki, and Minoru Saeki</i>	

## FPGA Countermeasures

Evaluating the Duplication of Dual-Rail Precharge Logics on FPGAs . . . . .	81
<i>Alexander Wild, Amir Moradi, and Tim Güneysu</i>	
Side-Channel Protection by Randomizing Look-Up Tables on Reconfigurable Hardware: Pitfalls of Memory Primitives . . . . .	95
<i>Pascal Sasdrich, Oliver Mischke, Amir Moradi, and Tim Güneysu</i>	

## Timing Attacks and Countermeasures

A Faster and More Realistic <i>Flush+Reload</i> Attack on AES . . . . .	111
<i>Berk Gülmemoğlu, Mehmet Sinan İnci, Gorka Irazoqui, Thomas Eisenbarth, and Berk Sunar</i>	
Faster Software for Fast Endomorphisms . . . . .	127
<i>Billy Bob Brumley</i>	

Toward Secure Implementation of McEliece Decryption . . . . . 141  
*Mariya Georgieva and Frédéric de Portzamparc*

**Fault Attacks**

Fault Injection with a New Flavor: Memetic Algorithms Make a Difference . . . . 159  
*Stjepan Picek, Lejla Batina, Pieter Buzing, and Domagoj Jakobovic*

Differential Fault Intensity Analysis on PRESENT and LED Block Ciphers . . . . 174  
*Nahid Farhady Ghalaty, Bilgiday Yuce, and Patrick Schaumont*

A Biased Fault Attack on the Time Redundancy Countermeasure for AES. . . 189  
*Sikhar Patranabis, Abhishek Chakraborty, Phuong Ha Nguyen, and  
Debddeep Mukhopadhyay*

**Countermeasures**

Faster Mask Conversion with Lookup Tables . . . . . 207  
*Praveen Kumar Vadnala and Johann Großschädl*

Towards Evaluating DPA Countermeasures for KECCAK on a Real ASIC . . . . 222  
*Michael Muehlberghuber, Thomas Korak, Philipp Dunst,  
and Michael Hutter*

**Hands-on Side-Channel Analysis**

Side-Channel Security Analysis of Ultra-Low-Power FRAM-Based MCUs. . . 239  
*Amir Moradi and Gesine Hinterwälder*

Side Channel Attacks on Smartphones and Embedded Devices  
Using Standard Radio Equipment . . . . . 255  
*Gabriel Goller and Georg Sigl*

**Author Index** . . . . . 271

Constructive Side-Channel Analysis and Secure Design  
6th International Workshop, COSADE 2015, Berlin,  
Germany, April 13-14, 2015. Revised Selected Papers  
Mangard, S.; Poschmann, A.Y. (Eds.)  
2015, X, 271 p. 87 illus., Softcover  
ISBN: 978-3-319-21475-7