

# Contents

## Security and Physical Attacks

Exploiting the Physical Disparity: Side-Channel Attacks on Memory Encryption . . . . .	3
<i>Thomas Unterluggauer and Stefan Mangard</i>	
Co-location Detection on the Cloud. . . . .	19
<i>Mehmet Sinan İnci, Berk Gulmezoglu, Thomas Eisenbarth, and Berk Sunar</i>	
Simple Photonic Emission Attack with Reduced Data Complexity. . . . .	35
<i>Elad Carmon, Jean-Pierre Seifert, and Avishai Wool</i>	

## Side-Channel Analysis (Case Studies)

Power Analysis Attacks Against IEEE 802.15.4 Nodes . . . . .	55
<i>Colin O'Flynn and Zhizhang Chen</i>	
Improved Side-Channel Analysis Attacks on Xilinx Bitstream Encryption of 5, 6, and 7 Series . . . . .	71
<i>Amir Moradi and Tobias Schneider</i>	
Dismantling Real-World ECC with Horizontal and Vertical Template Attacks . . . . .	88
<i>Margaux Dugardin, Louiza Papachristodoulou, Zakaria Najm, Lejla Batina, Jean-Luc Danger, and Sylvain Guilley</i>	

## Fault Analysis

Algorithmic Countermeasures Against Fault Attacks and Power Analysis for RSA-CRT. . . . .	111
<i>Ágnes Kiss, Juliane Krämer, Pablo Rauzy, and Jean-Pierre Seifert</i>	
Improved Differential Fault Analysis on Camellia-128. . . . .	130
<i>Toru Akishita and Noboru Kunihiro</i>	
A Note on the Security of CHES 2014 Symmetric Infective Countermeasure . . . . .	144
<i>Alberto Battistello and Christophe Giraud</i>	

**Side-Channel Analysis (Tools)**

Simpler, Faster, and More Robust T-Test Based Leakage Detection. . . . .	163
<i>A. Adam Ding, Cong Chen, and Thomas Eisenbarth</i>	
Design and Implementation of a Waveform-Matching Based Triggering System. . . . .	184
<i>Arthur Beckers, Josep Balasch, Benedikt Gierlichs, and Ingrid Verbauwhede</i>	
Robust and One-Pass Parallel Computation of Correlation-Based Attacks at Arbitrary Order. . . . .	199
<i>Tobias Schneider, Amir Moradi, and Tim Güneysu</i>	
<b>Author Index</b> . . . . .	219

Constructive Side-Channel Analysis and Secure Design  
7th International Workshop, COSADE 2016, Graz,  
Austria, April 14-15, 2016, Revised Selected Papers  
Standaert, F.-X.; Oswald, E. (Eds.)  
2016, X, 219 p. 74 illus., Softcover  
ISBN: 978-3-319-43282-3