

# Contents

Does Coupling Affect the Security of Masked Implementations? . . . . .	1
<i>Thomas De Cnudde, Begül Bilgin, Benedikt Gierlichs, Ventsislav Nikov, Svetla Nikova, and Vincent Rijmen</i>	
Scaling Trends for Dual-Rail Logic Styles Against Side-Channel Attacks: A Case-Study . . . . .	19
<i>Kashif Nawaz, Dinal Kamel, François-Xavier Standaert, and Denis Flandre</i>	
Dissecting Leakage Resilient PRFs with Multivariate Localized EM Attacks: A Practical Security Evaluation on FPGA . . . . .	34
<i>Florian Unterstein, Johann Heyszl, Fabrizio De Santis, and Robert Specht</i>	
Toward More Efficient DPA-Resistant AES Hardware Architecture Based on Threshold Implementation . . . . .	50
<i>Rei Ueno, Naofumi Homma, and Takafumi Aoki</i>	
Enhanced Elliptic Curve Scalar Multiplication Secure Against Side Channel Attacks and Safe Errors . . . . .	65
<i>Jeremy Dubeuf, David Hely, and Vincent Beroulle</i>	
SafeDRP: Yet Another Way Toward Power-Equalized Designs in FPGA . . . .	83
<i>Maik Ender, Alexander Wild, and Amir Moradi</i>	
On the Construction of Side-Channel Attack Resilient S-boxes . . . . .	102
<i>Liran Lerman, Nikita Veshchikov, Stjepan Picek, and Olivier Markowitch</i>	
Efficient Conversion Method from Arithmetic to Boolean Masking in Constrained Devices . . . . .	120
<i>Yoo-Seung Won and Dong-Guk Han</i>	
Side-Channel Analysis of Keymill . . . . .	138
<i>Christoph Dobraunig, Maria Eichlseder, Thomas Korak, and Florian Mendel</i>	
On the Easiness of Turning Higher-Order Leakages into First-Order . . . . .	153
<i>Thorben Moos and Amir Moradi</i>	

Side-Channel Attacks Against the Human Brain: The PIN Code Case Study . . . . .	171
<i>Joseph Lange, Clément Massart, André Mouraux, and Francois-Xavier Standaert</i>	
Impacts of Technology Trends on Physical Attacks? . . . . .	190
<i>Philippe Maurine and Sylvain Guilley</i>	
Low-Cost Setup for Localized Semi-invasive Optical Fault Injection Attacks: How Low Can We Go?. . . . .	207
<i>Oscar M. Guillen, Michael Gruber, and Fabrizio De Santis</i>	
DFA on LS-Designs with a Practical Implementation on SCREAM. . . . .	223
<i>Benjamin Lac, Anne Canteaut, Jacques Fournier, and Renaud Sirdey</i>	
Multiple-Valued Debiasing for Physically Unclonable Functions and Its Application to Fuzzy Extractors . . . . .	248
<i>Manami Suzuki, Rei Ueno, Naofumi Homma, and Takafumi Aoki</i>	
Getting the Most Out of Leakage Detection: Statistical Tools and Measurement Setups Hand in Hand. . . . .	264
<i>Santos Merino del Pozo and François-Xavier Standaert</i>	
Mind the Gap: Towards Secure 1st-Order Masking in Software . . . . .	282
<i>Kostas Papagiannopoulos and Nikita Veshchikov</i>	
<b>Author Index</b> . . . . .	299

Constructive Side-Channel Analysis and Secure Design  
8th International Workshop, COSADE 2017, Paris,  
France, April 13-14, 2017, Revised Selected Papers  
Guilley, S. (Ed.)  
2017, X, 299 p. 127 illus., Softcover  
ISBN: 978-3-319-64646-6