Contents

Kernel Discriminant Analysis for Information Extraction in the Presence of Masking 1
Eleonora Cagli, Cécile Dumas, and Emmanuel Prouff

Defeating Embedded Cryptographic Protocols by Combining Second-Order with Brute Force 23
Benoit Feix, Andjy Ricart, Benjamin Timon, and Lucille Tordella

Side-Channel Analysis of the TUAK Algorithm Used for Authentication and Key Agreement in 3G/4G Networks 39
Houssem Maghrebi and Julien Bringer

Reverse Engineering Flash EEPROM Memories Using Scanning Electron Microscopy 57
Franck Courbon, Sergei Skorobogatov, and Christopher Woods

SpecTre: A Tiny Side-Channel Resistant Speck Core for FPGAs 73
Cong Chen, Mehmet Sinan İnci, Mostafa Taha, and Thomas Eisenbarth

Concealing Secrets in Embedded Processors Designs 89
Hannes Gross, Manuel Jelinek, Stefan Mangard, Thomas Unterluggauer, and Mario Werner

The Hell Forgery: Self Modifying Codes Shoot Again 105
Abdelhak Mesbah, Leo Regnaud, Jean-Louis Lanet, and Mohamed Mezghiche

Logical Attacks on Secured Containers of the Java Card Platform 122
Sergei Volokitin and Erik Poll

Single-Trace Side-Channel Attacks on Scalar Multiplications with Precomputations 137
Kimmo Järvinen and Josep Balasch

A Compact and Exception-Free Ladder for All Short Weierstrass Elliptic Curves 156
Ruggero Susella and Sofia Montrasio

Inner Product Masking for Bitslice Ciphers and Security Order Amplification for Linear Leakages 174
Weijia Wang, François-Xavier Standaert, Yu Yu, Sihang Pu, Junrong Liu, Zheng Guo, and Dawu Gu

Squeezing Polynomial Masking in Tower Fields: A Higher-Order Masked AES S-Box 192
Fabrizio De Santis, Tobias Bauer, and Georg Sigl

PRNGs for Masking Applications and Their Mapping to Evolvable Hardware 209
Stjepan Picek, Bohan Yang, Vladimir Rozic, Jo Vliegen, Jori Winderickx, Thomas De Cnudde, and Nele Mentens

Automated Detection of Instruction Cache Leaks in Modular Exponentiation Software 228
Andreas Zankl, Johann Heyszl, and Georg Sigl

An Analysis of the Learning Parity with Noise Assumption Against Fault Attacks 245
Francesco Berti and François-Xavier Standaert

Author Index 265

http://www.springer.com/978-3-319-54668-1

Smart Card Research and Advanced Applications
15th International Conference, CARDIS 2016, Cannes, France, November 7–9, 2016, Revised Selected Papers
Lemke-Rust, K.; Tunstall, M. (Eds.)
2017, XII, 265 p. 93 illus., Softcover
ISBN: 978-3-319-54668-1