Table of Contents

Side-Channel Attacks

EM Attack Is Non-invasive? - Design Methodology and Validity Verification of EM Attack Sensor 1
Naofumi Homma, Yu-ichi Hayashi, Noriyuki Miura, Daisuke Fujimoto, Daichi Tanaka, Makoto Nagata, and Takafumi Aoki

A New Framework for Constraint-Based Probabilistic Template Side Channel Attacks 17
Yossef Oren, Ofir Weisse, and Avishai Wool

How to Estimate the Success Rate of Higher-Order Side-Channel Attacks 35
Victor Lomné, Emmanuel Prouff, Matthieu Rivain, Thomas Roche, and Adrian Thillard

Good Is Not Good Enough: Deriving Optimal Distinguishers from Communication Theory 55
Annelie Heuser, Olivier Rioul, and Sylvain Guilley

New Attacks and Constructions

"Ooh Aah... Just a Little Bit" : A Small Amount of Side Channel Can Go a Long Way 75
Naomi Benger, Joop van de Pol, Nigel P. Smart, and Yuval Yarom

Destroying Fault Invariant with Randomization: A Countermeasure for AES against Differential Fault Attacks 93
Harshal Tupsamudre, Shikha Bisht, and Debdeep Mukhopadhyay

Reversing Stealthy Dopant-Level Circuits 112
Takeshi Sugawara, Daisuke Suzuki, Ryoichi Fujii, Shigeaki Tawa, Ryohei Hori, Mitsuru Shiozaki, and Takeshi Fujino

Constructing S-boxes for Lightweight Cryptography with Feistel Structure 127
Yongqiang Li and Mingsheng Wang

Countermeasures

A Statistical Model for Higher Order DPA on Masked Devices 147
A. Adam Ding, Liwei Zhang, Yunsi Fei, and Pei Luo

Fast Evaluation of Polynomials over Binary Finite Fields and Application to Side-Channel Countermeasures 170
Jean-Sébastien Goron, Arnab Roy, and Srinivas Vivek

Secure Conversion between Boolean and Arithmetic Masking of Any Order 188
Jean-Sébastien Coron, Johann Großschädl, and Praveen Kumar Vadnala

Making RSA–PSS Provably Secure against Non-random Faults 206
Gilles Barthe, François Dupressoir, Pierre-Alain Fouque, Benjamin Grégoire, Mehdi Tibouchi, and Jean-Christophe Zapalowicz

Algorithm Specific SCA

Side-Channel Attack against RSA Key Generation Algorithms 223
Aurélie Bauer, Éliane Jaulmes, Victor Lomné, Emmanuel Prouff, and Thomas Roche

Get Your Hands Off My Laptop: Physical Side-Channel Key-Extraction Attacks on PCs 242
Daniel Genkin, Itamar Pipman, and Eran Tromer

RSA Meets DPA: Recovering RSA Secret Keys from Noisy Analog Data 261
Noboru Kunihiro and Junya Honda

Simple Power Analysis on AES Key Expansion Revisited 279
Christophe Clavier, Damien Marion, and Antoine Wurcker

ECC Implementations

Efficient Pairings and ECC for Embedded Systems 298
Thomas Unterluggauer and Erich Wenger

Curve41417: Karatsuba Revisited 316
Daniel J. Bernstein, Chitchanok Chuengsatiansup, and Tanja Lange

Implementations

Cofactorization on Graphics Processing Units 335
Andrea Miele, Joppe W. Bos, Thorsten Kleinjung, and Arjen K. Lenstra

Enhanced Lattice-Based Signatures on Reconfigurable Hardware 353
Thomas Pöppelmann, Léo Ducas, and Tim Güneysu

Compact Ring-LWE Cryptoprocessor 371
Sujoy Sinha Roy, Frederik Vercauteren, Nele Mentens, Donald Donglong Chen, and Ingrid Verbauwhede

Hardware Implementations of Symmetric Cryptosystems

ICEPOLE: High-Speed, Hardware-Oriented Authenticated Encryption 392
Paweł Morawiecki, Kris Gaj, Ekawat Homsirikamol, Krystian Matusiewicz, Josef Pieprzyk, Marcin Rogawski, Marian Srebrny, and Marcin Wójcik

FPGA Implementations of SPRING: And Their Countermeasures against Side-Channel Attacks 414
Hai Brenner, Lubos Gaspar, Gaëtan Leurent, Alon Rosen, and François-Xavier Standaert

FOAM: Searching for Hardware-Optimal SPN Structures and Components with a Fair Comparison 433
Khoongming Khoo, Thomas Peyrin, Axel Y. Poschmann, and Huihui Yap

PUFs

Secure Lightweight Entity Authentication with Strong PUFs: Mission Impossible? 451
Jeroen Delvaux, Dawu Gu, Dries Schellekens, and Ingrid Verbauwhede

Efficient Power and Timing Side Channels for Physical Unclonable Functions 476
Ulrich Rührmair, Xiaolin Xu, Jan Sölter, Ahmed Mahmoud, Mehrdad Majzoobi, Farinaz Koushanfar, and Wayne Burleson

Physical Characterization of Arbiter PUFs 493
Shahin Tajik, Enrico Dietz, Sven Frohmann, Jean-Pierre Seifert, Dmitry Nedospasov, Clemens Helfmeier, Christian Boit, and Helmar Dittrich

Bitline PUF: Building Native Challenge-Response PUF Capability into Any SRAM 510
Daniel E. Holcomb and Kevin Fu

RNGs and SCA Issues in Hardware

Embedded Evaluation of Randomness in Oscillator Based Elementary TRNG 527
Viktor Fischer and David Lubicz

Entropy Evaluation for Oscillator-Based True Random Number Generators 544
Yuan Ma, Jingqiang Lin, Tianyu Chen, Changwei Xu, Zongbin Liu, and Jiwu Jing

Side-Channel Leakage through Static Power: Should We Care about in Practice? 562
Amir Moradi

Gate-Level Masking under a Path-Based Leakage Metric 580
Andrew J. Leiserson, Mark E. Marson, and Megan A. Wachs

Early Propagation and Imbalanced Routing, How to Diminish in FPGAs 598
Amir Moradi and Vincent Immler

Author Index 617