

Contents

Side Channel Analysis

Correlated Extra-Reductions Defeat Blinded Regular Exponentiation	3
<i>Margaux Dugardin, Sylvain Guilley, Jean-Luc Danger, Zakaria Najm, and Olivier Rioul</i>	
Horizontal Side-Channel Attacks and Countermeasures on the ISW Masking Scheme.	23
<i>Alberto Battistello, Jean-Sébastien Coron, Emmanuel Prouff, and Rina Zeitoun</i>	
Towards Easy Leakage Certification	40
<i>François Durvaux, François-Xavier Standaert, and Santos Merino Del Pozo</i>	
Simple Key Enumeration (and Rank Estimation) Using Histograms: An Integrated Approach.	61
<i>Romain Poussier, François-Xavier Standaert, and Vincent Grosso</i>	

Automotive Security

Physical Layer Group Key Agreement for Automotive Controller Area Networks	85
<i>Shalabh Jain and Jorge Guajardo</i>	
– vatiCAN – Vetted, Authenticated CAN Bus	106
<i>Stefan Nürnberger and Christian Rossow</i>	

Invasive Attacks

Mitigating SAT Attack on Logic Locking	127
<i>Yang Xie and Ankur Srivastava</i>	
No Place to Hide: Contactless Probing of Secret Data on FPGAs	147
<i>Heiko Lohrke, Shahin Tajik, Christian Boit, and Jean-Pierre Seifert</i>	

Side Channel Countermeasures I

Strong 8-bit Sboxes with Efficient Masking in Hardware	171
<i>Erik Boss, Vincent Grosso, Tim Güneysu, Gregor Leander, Amir Moradi, and Tobias Schneider</i>	

Masking AES with $d + 1$ Shares in Hardware	194
<i>Thomas De Cnudde, Oscar Reparaz, Begül Bilgin, Svetla Nikova, Ventzislav Nikov, and Vincent Rijmen</i>	

New Directions

Differential Computation Analysis: Hiding Your White-Box Designs is Not Enough	215
<i>Joppe W. Bos, Charles Hubain, Wil Michiels, and Philippe Teuwen</i>	

Antikernel: A Decentralized Secure Hardware-Software Operating System Architecture	237
<i>Andrew Zonenberg and Bülent Yener</i>	

Software Implementations

Software Implementation of Koblitz Curves over Quadratic Fields	259
<i>Thomaz Oliveira, Julio López, and Francisco Rodríguez-Henríquez</i>	

QcBits: Constant-Time Small-Key Code-Based Cryptography	280
<i>Tung Chou</i>	

μ Kummer: Efficient Hyperelliptic Signatures and Key Exchange on Microcontrollers	301
<i>Joost Renes, Peter Schwabe, Benjamin Smith, and Lejla Batina</i>	

Cache Attacks

Flush, Gauss, and Reload – A Cache Attack on the BLISS Lattice-Based Signature Scheme	323
<i>Leon Groot Bruinderink, Andreas Hülsing, Tanja Lange, and Yuval Yarom</i>	

CacheBleed: A Timing Attack on OpenSSL Constant Time RSA	346
<i>Yuval Yarom, Daniel Genkin, and Nadia Heninger</i>	

Cache Attacks Enable Bulk Key Recovery on the Cloud	368
<i>Mehmet Sinan İnci, Berk Gulmezoglu, Gorka Irazoqui, Thomas Eisenbarth, and Berk Sunar</i>	

Physical Unclonable Functions

Strong Machine Learning Attack Against PUFs with No Mathematical Model	391
<i>Fatemeh Ganji, Shahin Tajik, Fabian Fäßler, and Jean-Pierre Seifert</i>	

Efficient Fuzzy Extraction of PUF-Induced Secrets: Theory and Applications	412
<i>Jeroen Delvaux, Dawu Gu, Ingrid Verbauwhede, Matthias Hiller, and Meng-Day (Mandel) Yu</i>	

Run-Time Accessible DRAM PUFs in Commodity Devices	432
<i>Wenjie Xiong, André Schaller, Nikolaos A. Anagnostopoulos, Muhammad Umair Saleem, Sebastian Gabmeyer, Stefan Katzenbeisser, and Jakub Szefer</i>	

Side Channel Countermeasures II

On the Multiplicative Complexity of Boolean Functions and Bitsliced Higher-Order Masking	457
<i>Dahmun Goudarzi and Matthieu Rivain</i>	

Reducing the Number of Non-linear Multiplications in Masking Schemes . . .	479
<i>Jürgen Pulkus and Srinivas Vivek</i>	

Faster Evaluation of SBoxes via Common Shares	498
<i>Jean-Sébastien Coron, Aurélien Greuet, Emmanuel Prouff, and Rina Zeitoun</i>	

Hardware Implementations

FourQ on FPGA: New Hardware Speed Records for Elliptic Curve Cryptography over Large Prime Characteristic Fields	517
<i>Kimmo Järvinen, Andrea Miele, Reza Azarderakhsh, and Patrick Longa</i>	

A High Throughput/Gate AES Hardware Architecture by Compressing Encryption and Decryption Datapaths — Toward Efficient CBC-Mode Implementation	538
<i>Rei Ueno, Sumio Morioka, Naofumi Homma, and Takafumi Aoki</i>	

Efficient High-Speed WPA2 Brute Force Attacks Using Scalable Low-Cost FPGA Clustering	559
<i>Markus Kammerstetter, Markus Muellner, Daniel Burian, Christian Kudera, and Wolfgang Kastner</i>	

Fault Attacks

ENCOUNTER: On Breaking the Nonce Barrier in Differential Fault Analysis with a Case-Study on PAEQ	581
<i>Dhiman Saha and Dipanwita Roy Chowdhury</i>	

Curious Case of Rowhammer: Flipping Secret Exponent Bits Using Timing Analysis.	602
<i>Sarani Bhattacharya and Debdeep Mukhopadhyay</i>	
A Design Methodology for Stealthy Parametric Trojans and Its Application to Bug Attacks	625
<i>Samaneh Ghandali, Georg T. Becker, Daniel Holcomb, and Christof Paar</i>	
Author Index	649

Cryptographic Hardware and Embedded Systems -
CHES 2016

18th International Conference, Santa Barbara, CA, USA,

August 17-19, 2016, Proceedings

Gierlichs, B.; Poschmann, A.Y. (Eds.)

2016, XIV, 650 p. 159 illus., Softcover

ISBN: 978-3-662-53139-6