Contents

Processing Techniques in Side-Channel Analysis

Robust Profiling for DPA-Style Attacks ........................................... 3
   Carolyn Whitnall and Elisabeth Oswald

Less is More: Dimensionality Reduction from a Theoretical Perspective. . . . . 22
   Nicolas Bruneau, Sylvain Guilley, Annelie Heuser, Damien Marion,
   and Olivier Rioul

Blind Source Separation from Single Measurements Using Singular
Spectrum Analysis ................................................................. 42
   Santos Merino Del Pozo and François-Xavier Standaert

Cryptographic Hardware Implementations

Highly Efficient $GF(2^8)$ Inversion Circuit Based on Redundant GF
Arithmetic and Its Application to AES Design ................................. 63
   Rei Ueno, Naofumi Homma, Yukihiro Sugawara, Yasuyuki Nogami,
   and Takafumi Aoki

NaCl’s Crypto_box in Hardware .................................................... 81
   Michael Hutter, Jürgen Schilling, Peter Schwabe, and Wolfgang Wieser

Lightweight Coprocessor for Koblitz Curves: 283-Bit ECC Including
Scalar Conversion with only 4300 Gates ...................................... 102
   Sujoy Sinha Roy, Kimmo Järvinen, and Ingrid Verbauwhede

Single Base Modular Multiplication for Efficient Hardware RNS
Implementations of ECC ............................................................ 123
   Karim Bigou and Arnaud Tisserand

Homomorphic Encryption in Hardware

Accelerating Homomorphic Evaluation on Reconfigurable Hardware ........ 143
   Thomas Pöppelmann, Michael Naehrig, Andrew Putnam,
   and Adrian Macias

Modular Hardware Architecture for Somewhat Homomorphic
Function Evaluation ............................................................... 164
   Sujoy Sinha Roy, Kimmo Järvinen, Frederik Vercauteren,
   Vassil Dimitrov, and Ingrid Verbauwhede
Accelerating LTV Based Homomorphic Encryption
in Reconfigurable Hardware .................................................. 185
  Yarkın Doröz, Erdinç Özütürk, Erkay Savaş, and Berk Sunar

Side-Channel Attacks on Public Key Cryptography

Stealing Keys from PCs Using a Radio: Cheap Electromagnetic Attacks
on Windowed Exponentiation .................................................. 207
  Daniel Genkin, Lev Pachmanov, Itamar Pipman, and Eran Tromer

Exclusive Exponent Blinding May Not Suffice to Prevent Timing
Attacks on RSA ................................................................. 229
  Werner Schindler

Who Watches the Watchmen?: Utilizing Performance Monitors
for Compromising Keys of RSA on Intel Platforms ...................... 248
  Sarani Bhattacharya and Debdeep Mukhopadhyay

Cipher Design and Cryptanalysis

Improved Cryptanalysis of the DECT Standard Cipher .................. 269
  Iwen Coisel and Ignacio Sanchez

Practical Key Recovery for Discrete-Logarithm Based Authentication
Schemes from Random Nonce Bits ........................................... 287
  Aurélie Bauer and Damien Vergnaud

The Simeck Family of Lightweight Block Ciphers ......................... 307
  Gangqiang Yang, Bo Zhu, Valentin Suder, Mark D. Aagaard,
  and Guang Gong

TriviA: A Fast and Secure Authenticated Encryption Scheme .......... 330
  Avik Chakraborti, Anupam Chattopadhyay, Muhammad Hassan,
  and Mridul Nandi

True Random Number Generators and Entropy Estimations

A Physical Approach for Stochastic Modeling of TERO-Based TRNG .... 357
  Patrick Haddad, Viktor Fischer, Florent Bernard, and Jean Nicolai

Predictive Models for Min-entropy Estimation .......................... 373
  John Kelsey, Kerry A. McKay, and Meltem Sönmez Turan
Side-Channel Analysis and Fault Injection Attacks

Improved Side-Channel Analysis of Finite-Field Multiplication .......................... 395
Sonia Belaïd, Jean-Sébastien Coron, Pierre-Alain Fouque, Benoît Gérard, Jean-Gabriel Kammerer, and Emmanuel Prouff

Evaluation and Improvement of Generic-Emulating DPA Attacks ......................... 416
Weijia Wang, Yu Yu, Junrong Liu, Zheng Guo, François-Xavier Standaert, Dawu Gu, Sen Xu, and Rong Fu

Transient-Steady Effect Attack on Block Ciphers ............................................ 433
Yanting Ren, An Wang, and Liji Wu

Higher-Order Side-Channel Attacks

Assessment of Hiding the Higher-Order Leakages in Hardware:
What Are the Achievements Versus Overheads? ............................................. 453
Amir Moradi and Alexander Wild

Multi-variate High-Order Attacks of Shuffled Tables Recomputation .................. 475
Nicolas Bruneau, Sylvain Guilley, Zakaria Najm, and Yannick Teglia

Leakage Assessment Methodology: A Clear Roadmap
for Side-Channel Evaluations ................................................................. 495
Tobias Schneider and Amir Moradi

Physically Unclonable Functions and Hardware Trojans

Secure Key Generation from Biased PUFs ..................................................... 517
Roel Maes, Vincent van der Leest, Erik van der Sluis, and Frans Willems

The Gap Between Promise and Reality: On the Insecurity of XOR Arbiter PUFs ................................................................. 535
Georg T. Becker

End-To-End Design of a PUF-Based Privacy Preserving Authentication Protocol ................................................................. 556
Aydin Aysu, Ege Gulcan, Daisuke Moriyama, Patrick Schaumont, and Moti Yung

Improved Test Pattern Generation for Hardware Trojan Detection
Using Genetic Algorithm and Boolean Satisfiability ..................................... 577
Sayandeep Saha, Rajat Subhra Chakraborty, Srinivasa Shashank Nuthakki, Anshul, and Debdeep Mukhopadhyay
Side-Channel Attacks in Practice

DPA, Bitslicing and Masking at 1 GHz ........................................... 599  
   Josep Balasch, Benedikt Gierlichs, Oscar Reparaz,  
   and Ingrid Verbauwhede

SoC It to EM: ElectroMagnetic Side-Channel Attacks on a Complex  
System-on-Chip ............................................................... 620  
   J. Longo, E. De Mulder, D. Page, and M. Tunstall

Finding the AES Bits in the Haystack: Reverse Engineering and SCA  
Using Voltage Contrast ...................................................... 641  
   Christian Kison, Jürgen Frinken, and Christof Paar

Lattice-Based Implementations

Efficient Ring-LWE Encryption on 8-Bit AVR Processors .................... 663  
   Zhe Liu, Hwajeong Seo, Sujoy Sinha Roy, Johann Großschädl,  
   Howon Kim, and Ingrid Verbauwhede

A Masked Ring-LWE Implementation ........................................... 683  
   Oscar Reparaz, Sujoy Sinha Roy, Frederik Vercauteren,  
   and Ingrid Verbauwhede

Author Index ........................................................................... 703
Cryptographic Hardware and Embedded Systems -- CHES 2015
17th International Workshop, Saint-Malo, France, September 13–16, 2015, Proceedings
Güneysu, T.; Handschuh, H. (Eds.)
2015, XIV, 704 p. 204 illus., Softcover
ISBN: 978-3-662-48323-7