

Contents

Processing Techniques in Side-Channel Analysis

| | |
|---|----|
| Robust Profiling for DPA-Style Attacks | 3 |
| <i>Carolyn Whitnall and Elisabeth Oswald</i> | |
| Less is More: Dimensionality Reduction from a Theoretical Perspective. | 22 |
| <i>Nicolas Bruneau, Sylvain Guilley, Annelie Heuser, Damien Marion, and Olivier Rioul</i> | |
| Blind Source Separation from Single Measurements Using Singular Spectrum Analysis | 42 |
| <i>Santos Merino Del Pozo and François-Xavier Standaert</i> | |

Cryptographic Hardware Implementations

| | |
|---|-----|
| Highly Efficient $GF(2^8)$ Inversion Circuit Based on Redundant GF Arithmetic and Its Application to AES Design | 63 |
| <i>Rei Ueno, Naofumi Homma, Yukihiro Sugawara, Yasuyuki Nogami, and Takafumi Aoki</i> | |
| NaCl's Crypto_box in Hardware. | 81 |
| <i>Michael Hutter, Jürgen Schilling, Peter Schwabe, and Wolfgang Wieser</i> | |
| Lightweight Coprocessor for Koblitz Curves: 283-Bit ECC Including Scalar Conversion with only 4300 Gates | 102 |
| <i>Sujoy Sinha Roy, Kimmo Järvinen, and Ingrid Verbauwhede</i> | |
| Single Base Modular Multiplication for Efficient Hardware RNS Implementations of ECC | 123 |
| <i>Karim Bigou and Arnaud Tisserand</i> | |

Homomorphic Encryption in Hardware

| | |
|---|-----|
| Accelerating Homomorphic Evaluation on Reconfigurable Hardware. | 143 |
| <i>Thomas Pöppelmann, Michael Naehrig, Andrew Putnam, and Adrian Macias</i> | |
| Modular Hardware Architecture for Somewhat Homomorphic Function Evaluation. | 164 |
| <i>Sujoy Sinha Roy, Kimmo Järvinen, Frederik Vercauteren, Vassil Dimitrov, and Ingrid Verbauwhede</i> | |

| | |
|---|-----|
| Accelerating LTV Based Homomorphic Encryption in Reconfigurable Hardware | 185 |
| <i>Yarkin Doröz, Erdinç Öztürk, Erkay Savaş, and Berk Sunar</i> | |

Side-Channel Attacks on Public Key Cryptography

| | |
|---|-----|
| Stealing Keys from PCs Using a Radio: Cheap Electromagnetic Attacks on Windowed Exponentiation | 207 |
| <i>Daniel Genkin, Lev Pachmanov, Itamar Pipman, and Eran Tromer</i> | |

| | |
|---|-----|
| Exclusive Exponent Blinding May Not Suffice to Prevent Timing Attacks on RSA | 229 |
| <i>Werner Schindler</i> | |

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

Cipher Design and Cryptanalysis

| | |
|--|-----|
| Improved Cryptanalysis of the DECT Standard Cipher | 269 |
| <i>Iwen Coisel and Ignacio Sanchez</i> | |

| | |
|--|-----|
| Practical Key Recovery for Discrete-Logarithm Based Authentication Schemes from Random Nonce Bits | 287 |
| <i>Aurélie Bauer and Damien Vergnaud</i> | |

| | |
|--|-----|
| The Simeck Family of Lightweight Block Ciphers | 307 |
| <i>Gangqiang Yang, Bo Zhu, Valentin Suder, Mark D. Aagaard, and Guang Gong</i> | |

| | |
|--|-----|
| TriviA: A Fast and Secure Authenticated Encryption Scheme | 330 |
| <i>Avik Chakraborti, Anupam Chattopadhyay, Muhammad Hassan, and Mridul Nandi</i> | |

True Random Number Generators and Entropy Estimations

| | |
|--|-----|
| A Physical Approach for Stochastic Modeling of TERO-Based TRNG | 357 |
| <i>Patrick Haddad, Viktor Fischer, Florent Bernard, and Jean Nicolai</i> | |

| | |
|---|-----|
| Predictive Models for Min-entropy Estimation | 373 |
| <i>John Kelsey, Kerry A. McKay, and Meltem Sönmez Turan</i> | |

Side-Channel Analysis and Fault Injection Attacks

| | |
|---|-----|
| Improved Side-Channel Analysis of Finite-Field Multiplication | 395 |
| <i>Sonia Belaïd, Jean-Sébastien Coron, Pierre-Alain Fouque, Benoît Gérard, Jean-Gabriel Kammerer, and Emmanuel Prouff</i> | |
| Evaluation and Improvement of Generic-Emulating DPA Attacks | 416 |
| <i>Weijia Wang, Yu Yu, Junrong Liu, Zheng Guo, François-Xavier Standaert, Dawu Gu, Sen Xu, and Rong Fu</i> | |
| Transient-Steady Effect Attack on Block Ciphers | 433 |
| <i>Yanting Ren, An Wang, and Liji Wu</i> | |

Higher-Order Side-Channel Attacks

| | |
|--|-----|
| Assessment of Hiding the Higher-Order Leakages in Hardware: What Are the Achievements Versus Overheads? | 453 |
| <i>Amir Moradi and Alexander Wild</i> | |
| Multi-variate High-Order Attacks of Shuffled Tables Recomputation | 475 |
| <i>Nicolas Bruneau, Sylvain Guilley, Zakaria Najm, and Yannick Tégli</i> | |
| Leakage Assessment Methodology: A Clear Roadmap for Side-Channel Evaluations | 495 |
| <i>Tobias Schneider and Amir Moradi</i> | |

Physically Unclonable Functions and Hardware Trojans

| | |
|--|-----|
| Secure Key Generation from Biased PUFs | 517 |
| <i>Roel Maes, Vincent van der Leest, Erik van der Sluis, and Frans Willems</i> | |
| The Gap Between Promise and Reality: On the Insecurity of XOR Arbiter PUFs | 535 |
| <i>Georg T. Becker</i> | |
| End-To-End Design of a PUF-Based Privacy Preserving Authentication Protocol | 556 |
| <i>Aydin Aysu, Ege Gulcan, Daisuke Moriyama, Patrick Schaumont, and Moti Yung</i> | |
| Improved Test Pattern Generation for Hardware Trojan Detection Using Genetic Algorithm and Boolean Satisfiability | 577 |
| <i>Sayandeep Saha, Rajat Subhra Chakraborty, Srinivasa Shashank Nuthakki, Anshul, and Debdeep Mukhopadhyay</i> | |

Side-Channel Attacks in Practice

| | |
|---|-----|
| DPA, Bitslicing and Masking at 1 GHz | 599 |
| <i>Josep Balasch, Benedikt Gierlichs, Oscar Reparaz, and Ingrid Verbauwhede</i> | |
| SoC It to EM: ElectroMagnetic Side-Channel Attacks on a Complex System-on-Chip | 620 |
| <i>J. Longo, E. De Mulder, D. Page, and M. Tunstall</i> | |
| Finding the AES Bits in the Haystack: Reverse Engineering and SCA Using Voltage Contrast | 641 |
| <i>Christian Kison, Jürgen Frinken, and Christof Paar</i> | |

Lattice-Based Implementations

| | |
|---|-----|
| Efficient Ring-LWE Encryption on 8-Bit AVR Processors | 663 |
| <i>Zhe Liu, Hwajeong Seo, Sujoy Sinha Roy, Johann Großschädl, Howon Kim, and Ingrid Verbauwhede</i> | |
| A Masked Ring-LWE Implementation | 683 |
| <i>Oscar Reparaz, Sujoy Sinha Roy, Frederik Vercauteren, and Ingrid Verbauwhede</i> | |
| 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