

Contents

Deep Learning and Fault Based Attacks

Breaking Cryptographic Implementations Using Deep Learning Techniques . . .	3
<i>Housseem Maghrebi, Thibault Portigliatti, and Emmanuel Prouff</i>	
Cheap and Cheerful: A Low-Cost Digital Sensor for Detecting Laser Fault Injection Attacks	27
<i>Wei He, Jakub Breier, and Shivam Bhasin</i>	
Comprehensive Laser Sensitivity Profiling and Data Register Bit-Flips for Cryptographic Fault Attacks in 65 Nm FPGA	47
<i>Wei He, Jakub Breier, Shivam Bhasin, Dirmanto Jap, Hock Guan Ong, and Chee Lip Gan</i>	
Fault Based Almost Universal Forgeries on CLOC and SILC.	66
<i>Debapriya Basu Roy, Avik Chakraborti, Donghoon Chang, S.V. Dilip Kumar, Debdeep Mukhopadhyay, and Mridul Nandi</i>	

Applied Cryptography

Implementing Complete Formulas on Weierstrass Curves in Hardware.	89
<i>Pedro Maat C. Massolino, Joost Renes, and Lejla Batina</i>	
Partially Homomorphic Encryption Schemes over Finite Fields.	109
<i>Jian Liu, Sihem Mesnager, and Lusheng Chen</i>	
Light Weight Key Establishment Scheme for Wireless Sensor Networks	124
<i>Payingat Jilna and P.P. Deepthi</i>	
A Scalable and Systolic Architectures of Montgomery Modular Multiplication for Public Key Cryptosystems Based on DSPs	138
<i>Amine Mrabet, Nadia El-Mrabet, Ronan Lashermes, Jean-Baptiste Rigaud, Belgacem Bouallegue, Sihem Mesnager, and Mohsen Machhout</i>	

Iterative Ciphers

Spectral Characterization of Iterating Lossy Mappings	159
<i>Joan Daemen</i>	

Decomposed S-Boxes and DPA Attacks: A Quantitative Case Study Using PRINCE.	179
<i>Ravikumar Selvam, Dillibabu Shanmugam, Suganya Annadurai, and Jothi Rangasamy</i>	
GAIN: Practical Key-Recovery Attacks on Round-reduced PAEQ	194
<i>Dhiman Saha, Sourya Kakarla, Srinath Mandava, and Dipanwita Roy Chowdhury</i>	
Hardware Security	
Predictive Aging of Reliability of Two Delay PUFs	213
<i>Naghmeh Karimi, Jean-Luc Danger, Florent Lozac'h, and Sylvain Guilley</i>	
Towards Securing Low-Power Digital Circuits with Ultra-Low-Voltage Vdd Randomizers	233
<i>Dina Kamel, Guerric de Streel, Santos Merino Del Pozo, Kashif Nawaz, François-Xavier Standaert, Denis Flandre, and David Bol</i>	
Security	
Enabling Secure Web Payments with GNU Taler	251
<i>Jeffrey Burdges, Florian Dold, Christian Grothoff, and Marcello Stanisci</i>	
Malware Characterization Using Windows API Call Sequences	271
<i>Sanchit Gupta, Harshit Sharma, and Sarvjeet Kaur</i>	
VMI Based Automated Real-Time Malware Detector for Virtualized Cloud Environment	281
<i>M.A. Ajay Kumara and C.D. Jaidhar</i>	
Post-quantum Cryptology	
Solving Binary \mathcal{MQ} with Grover's Algorithm	303
<i>Peter Schwabe and Bas Westerbaan</i>	
Ring-LWE: Applications to Cryptography and Their Efficient Realization . . .	323
<i>Sujoy Sinha Roy, Angshuman Karmakar, and Ingrid Verbauwhede</i>	
NewHope on ARM Cortex-M.	332
<i>Erdem Alkim, Philipp Jakubeit, and Peter Schwabe</i>	

Leakage, Power and Fault Analysis

Towards Fair and Efficient Evaluations of Leaking Cryptographic Devices: Overview of the ERC Project CRASH, Part I (<i>Invited Talk</i>)	353
<i>François-Xavier Standaert</i>	
A Methodology for the Characterisation of Leakages in Combinatorial Logic	363
<i>Guido Bertoni and Marco Martinoli</i>	
Exploiting the Leakage: Analysis of Some Authenticated Encryption Schemes	383
<i>Donghoon Chang, Amit Kumar Chauhan, Naina Gupta, Arpan Jati, and Somitra Kumar Sanadhya</i>	
Breaking Kalyna 128/128 with Power Attacks	402
<i>Stephane Fernandes Medeiros, François Gérard, Nikita Veshchikov, Liran Lerman, and Olivier Markowitch</i>	
Fault Injection Attacks: Attack Methodologies, Injection Techniques and Protection Mechanisms: A Tutorial	415
<i>Shivam Bhasin and Debdeep Mukhopadhyay</i>	
Author Index	419

Security, Privacy, and Applied Cryptography Engineering
6th International Conference, SPACE 2016, Hyderabad,
India, December 14-18, 2016, Proceedings
Carlet, C.; Hasan, M.A.; Saraswat, V. (Eds.)
2016, XXIII, 420 p. 139 illus., Softcover
ISBN: 978-3-319-49444-9