

Table of Contents

Low Cost Cryptography

QUARK: A Lightweight Hash	1
<i>Jean-Philippe Aumasson, Luca Henzen, Willi Meier, and María Naya-Plasencia</i>	
PRINTCIPHER: A Block Cipher for IC-Printing	16
<i>Lars Knudsen, Gregor Leander, Azel Poschmann, and Matthew J.B. Robshaw</i>	
Sponge-Based Pseudo-Random Number Generators	33
<i>Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche</i>	

Efficient Implementations I

A High Speed Coprocessor for Elliptic Curve Scalar Multiplications over $\mathbb{F}_p$	48
<i>Nicolas Guillermín</i>	
Co-Z Addition Formulæ and Binary Ladders on Elliptic Curves	65
<i>Raveen R. Goundar, Marc Joye, and Atsuko Miyaji</i>	
Efficient Techniques for High-Speed Elliptic Curve Cryptography	80
<i>Patrick Longa and Catherine Gebotys</i>	

Side-Channel Attacks and Countermeasures I

Analysis and Improvement of the Random Delay Countermeasure of CHES 2009	95
<i>Jean-Sébastien Coron and Ilya Kizhvatov</i>	
New Results on Instruction Cache Attacks	110
<i>Onur Acıçmez, Billy Bob Brumley, and Philipp Grabher</i>	
Correlation-Enhanced Power Analysis Collision Attack	125
<i>Amir Moradi, Oliver Mischke, and Thomas Eisenbarth</i>	
Side-Channel Analysis of Six SHA-3 Candidates	140
<i>Olivier Benoît and Thomas Peyrin</i>	

Tamper Resistance and Hardware Trojans

Flash Memory ‘Bumping’ Attacks	158
<i>Sergei Skorobogatov</i>	
Self-referencing: A Scalable Side-Channel Approach for Hardware Trojan Detection	173
<i>Dongdong Du, Seetharam Narasimhan, Rajat Subhra Chakraborty, and Swarup Bhunia</i>	
When Failure Analysis Meets Side-Channel Attacks	188
<i>Jerome Di-Battista, Jean-Christophe Courrege, Bruno Rouzeyre, Lionel Torres, and Philippe Perdu</i>	

Efficient Implementations II

Fast Exhaustive Search for Polynomial Systems in $\mathbb{F}_2$	203
<i>Charles Bouillaguet, Hsieh-Chung Chen, Chen-Mou Cheng, Tung Chou, Ruben Niederhagen, Adi Shamir, and Bo-Yin Yang</i>	
256 Bit Standardized Crypto for 650 GE – GOST Revisited	219
<i>Axel Poschmann, San Ling, and Huaxiong Wang</i>	
Mixed Bases for Efficient Inversion in $\mathbb{F}_{((2^2)^2)^2}$ and Conversion Matrices of SubBytes of AES	234
<i>Yasuyuki Nogami, Kenta Nekado, Tetsumi Toyota, Naoto Hongo, and Yoshitaka Morikawa</i>	

SHA-3

Developing a Hardware Evaluation Method for SHA-3 Candidates	248
<i>Luca Henzen, Pietro Gendotti, Patrice Guillet, Enrico Pargaetzi, Martin Zoller, and Frank K. Gürkaynak</i>	
Fair and Comprehensive Methodology for Comparing Hardware Performance of Fourteen Round Two SHA-3 Candidates Using FPGAs	264
<i>Kris Gaj, Ekawat Homsirikamol, and Marcin Rogawski</i>	
Performance Analysis of the SHA-3 Candidates on Exotic Multi-core Architectures	279
<i>Joppe W. Bos and Deian Stefan</i>	
XBX: eXternal Benchmarking eXtension for the SUPERCOP Crypto Benchmarking Framework	294
<i>Christian Wenzel-Benner and Jens Gräf</i>	

Fault Attacks and Countermeasures

Public Key Perturbation of Randomized RSA Implementations	306
<i>Alexandre Berzati, Cécile Canovas-Dumas, and Louis Goubin</i>	
Fault Sensitivity Analysis	320
<i>Yang Li, Kazuo Sakiyama, Shigeto Gomisawa, Toshinori Fukunaga, Junko Takahashi, and Kazuo Ohta</i>	

PUFs and RNGs

An Alternative to Error Correction for SRAM-Like PUFs	335
<i>Maximilian Hofer and Christoph Boehm</i>	
New High Entropy Element for FPGA Based True Random Number Generators	351
<i>Michal Varchola and Milos Drutarovsky</i>	
The Glitch PUF: A New Delay-PUF Architecture Exploiting Glitch Shapes	366
<i>Daisuke Suzuki and Koichi Shimizu</i>	

New Designs

Garbled Circuits for Leakage-Resilience: Hardware Implementation and Evaluation of One-Time Programs	383
<i>Kimmo Järvinen, Vladimir Kolesnikov, Ahmad-Reza Sadeghi, and Thomas Schneider</i>	
ARMADILLO: A Multi-purpose Cryptographic Primitive Dedicated to Hardware	398
<i>Stéphane Badel, Nilay Dağtekin, Jorge Nakahara Jr., Khaled Ouafi, Nicolas Reffé, Pouyan Sepehrdad, Petr Sušil, and Serge Vaudenay</i>	

Side-Channel Attacks and Countermeasures II

Provably Secure Higher-Order Masking of AES	413
<i>Matthieu Rivain and Emmanuel Prouff</i>	
Algebraic Side-Channel Analysis in the Presence of Errors	428
<i>Yossef Oren, Mario Kirschbaum, Thomas Popp, and Avishai Wool</i>	
Coordinate Blinding over Large Prime Fields	443
<i>Michael Tunstall and Marc Joye</i>	

Author Index	457
------------------------	-----