

Table of Contents

Software Implementations

Faster and Timing-Attack Resistant AES-GCM	1
<i>Emilia Käsper and Peter Schwabe</i>	
Accelerating AES with Vector Permute Instructions	18
<i>Mike Hamburg</i>	
SSE Implementation of Multivariate PKCs on Modern x86 CPUs	33
<i>Anna Inn-Tung Chen, Ming-Shing Chen, Tien-Ren Chen, Chen-Mou Cheng, Jintai Ding, Eric Li-Hsiang Kuo, Frost Yu-Shuang Lee, and Bo-Yin Yang</i>	
MicroEliece: McEliece for Embedded Devices	49
<i>Thomas Eisenbarth, Tim Güneysu, Stefan Heyse, and Christof Paar</i>	

Invited Talk 1

Physical Unclonable Functions and Secure Processors	65
<i>Srini Devadas</i>	

Side Channel Analysis of Secret Key Cryptosystems

Practical Electromagnetic Template Attack on HMAC	66
<i>Pierre-Alain Fouque, Gaëtan Leurent, Denis Réal, and Frédéric Valette</i>	
First-Order Side-Channel Attacks on the Permutation Tables Countermeasure	81
<i>Emmanuel Prouff and Robert McEvoy</i>	
Algebraic Side-Channel Attacks on the AES: Why Time also Matters in DPA	97
<i>Mathieu Renauld, François-Xavier Standaert, and Nicolas Veyrat-Charvillon</i>	
Differential Cluster Analysis	112
<i>Lejla Batina, Benedikt Gierlichs, and Kerstin Lemke-Rust</i>	

Side Channel Analysis of Public Key Cryptosystems

Known-Plaintext-Only Attack on RSA-CRT with Montgomery Multiplication	128
<i>Martin Hlaváč</i>	

A New Side-Channel Attack on RSA Prime Generation	141
<i>Thomas Finke, Max Gebhardt, and Werner Schindler</i>	

Side Channel and Fault Analysis Countermeasures

An Efficient Method for Random Delay Generation in Embedded Software	156
<i>Jean-Sébastien Coron and Ilya Kizhvatov</i>	

Higher-Order Masking and Shuffling for Software Implementations of Block Ciphers	171
<i>Matthieu Rivain, Emmanuel Prouff, and Julien Doget</i>	

A Design Methodology for a DPA-Resistant Cryptographic LSI with RSL Techniques	189
<i>Minoru Saeki, Daisuke Suzuki, Koichi Shimizu, and Akashi Satoh</i>	

A Design Flow and Evaluation Framework for DPA-Resistant Instruction Set Extensions	205
<i>Francesco Regazzoni, Alessandro Cevrero, François-Xavier Standaert, Stephane Badel, Theo Kluter, Philip Brisk, Yusuf Leblebici, and Paolo Ienne</i>	

Invited Talk 2

Crypto Engineering: Some History and Some Case Studies (Extended Abstract)	220
<i>Christof Paar</i>	

Pairing-Based Cryptography

Hardware Accelerator for the Tate Pairing in Characteristic Three Based on Karatsuba-Ofman Multipliers	225
<i>Jean-Luc Beuchat, Jérémie Detrey, Nicolas Estibals, Eiji Okamoto, and Francisco Rodríguez-Henríquez</i>	

Faster $\mathbb{F}_p$ -Arithmetic for Cryptographic Pairings on Barreto-Naehrig Curves	240
<i>Junfeng Fan, Frederik Vercauteren, and Ingrid Verbauwhede</i>	

Designing an ASIP for Cryptographic Pairings over Barreto-Naehrig Curves	254
<i>David Kammler, Diandian Zhang, Peter Schwabe, Hanno Scharwaechter, Markus Langenberg, Dominik Auras, Gerd Ascheid, and Rudolf Mathar</i>	

New Ciphers and Efficient Implementations

KATAN and KTANTAN – A Family of Small and Efficient Hardware-Oriented Block Ciphers	272
<i>Christophe De Cannière, Orr Dunkelman, and Miroslav Knežević</i>	
Programmable and Parallel ECC Coprocessor Architecture: Tradeoffs between Area, Speed and Security	289
<i>Xu Guo, Junfeng Fan, Patrick Schaumont, and Ingrid Verbauwhede</i>	
Elliptic Curve Scalar Multiplication Combining Yao's Algorithm and Double Bases	304
<i>Nicolas Méloni and M. Anwar Hasan</i>	

TRNGs and Device Identification

The Frequency Injection Attack on Ring-Oscillator-Based True Random Number Generators	317
<i>A. Theodore Markettos and Simon W. Moore</i>	
Low-Overhead Implementation of a Soft Decision Helper Data Algorithm for SRAM PUFs	332
<i>Roel Maes, Pim Tuyls, and Ingrid Verbauwhede</i>	
CDs Have Fingerprints Too	348
<i>Ghaith Hammouri, Aykutlu Dana, and Berk Sunar</i>	

Invited Talk 3

The State-of-the-Art in IC Reverse Engineering	363
<i>Randy Torrance and Dick James</i>	

Hot Topic Session: Hardware Trojans and Trusted ICs

Trojan Side-Channels: Lightweight Hardware Trojans through Side-Channel Engineering	382
<i>Lang Lin, Markus Kasper, Tim Güneysu, Christof Paar, and Wayne Burleson</i>	
MERO: A Statistical Approach for Hardware Trojan Detection	396
<i>Rajat Subhra Chakraborty, Francis Wolff, Somnath Paul, Christos Papachristou, and Swarup Bhunia</i>	

Theoretical Aspects

On Tamper-Resistance from a Theoretical Viewpoint: The Power of Seals	411
<i>Paulo Mateus and Serge Vaudenay</i>	

Mutual Information Analysis: How, When and Why?	429
<i>Nicolas Veyrat-Charvillon and François-Xavier Standaert</i>	

Fault Analysis

Fault Attacks on RSA Signatures with Partially Unknown Messages	444
<i>Jean-Sébastien Coron, Antoine Joux, Ilya Kizhvatov, David Naccache, and Pascal Paillier</i>	

Differential Fault Analysis on DES Middle Rounds	457
<i>Matthieu Rivain</i>	

Author Index	471
-------------------------------	-----