

Table of Contents

Side Channels I

Template Attacks in Principal Subspaces	1
<i>C. Archambeau, E. Peeters, F.-X. Standaert, J.-J. Quisquater</i>	
Templates vs. Stochastic Methods	15
<i>Benedikt Gierlichs, Kerstin Lemke-Rust, Christof Paar</i>	
Towards Security Limits in Side-Channel Attacks	30
<i>F.-X. Standaert, E. Peeters, C. Archambeau, J.-J. Quisquater</i>	

Low Resources

HIGHT: A New Block Cipher Suitable for Low-Resource Device	46
<i>Deukjo Hong, Jaechul Sung, Seokhie Hong, Jongin Lim, Sangjin Lee, Bon-Seok Koo, Changhoon Lee, Donghoon Chang, Jesang Lee, Kitae Jeong, Hyun Kim, Jongsung Kim, Seongtaek Chee</i>	

Invited Talk I

Integer Factoring Utilizing PC Cluster	60
<i>Kazumaro Aoki</i>	

Hardware Attacks and Countermeasures I

Optically Enhanced Position-Locked Power Analysis	61
<i>Sergei Skorobogatov</i>	
Pinpointing the Side-Channel Leakage of Masked AES Hardware Implementations	76
<i>Stefan Mangard, Kai Schramm</i>	
A Generalized Method of Differential Fault Attack Against AES Cryptosystem	91
<i>Amir Moradi, Mohammad T. Manzuri Shalmani, Mahmoud Salmasizadeh</i>	

Special Purpose Hardware

Breaking Ciphers with COPACOBANA – A Cost-Optimized Parallel
Code Breaker 101
*Sandeep Kumar, Christof Paar, Jan Pelzl, Gerd Pfeiffer,
Manfred Schimpler*

Implementing the Elliptic Curve Method of Factoring
in Reconfigurable Hardware 119
*Kris Gaj, Soonhak Kwon, Patrick Baier, Paul Kohlbrenner,
Hoang Le, Mohammed Khaleeluddin, Ramakrishna Bachimanchi*

Efficient Algorithms for Embedded Processors

Implementing Cryptographic Pairings on Smartcards 134
Michael Scott, Neil Costigan, Wesam Abdulwahab

SPA-Resistant Scalar Multiplication on Hyperelliptic Curve
Cryptosystems Combining Divisor Decomposition Technique
and Joint Regular Form 148
Toru Akishita, Masanobu Katagi, Izuru Kitamura

Fast Generation of Prime Numbers on Portable Devices: An Update 160
Marc Joye, Pascal Paillier

Side Channels II

A Proposition for Correlation Power Analysis Enhancement 174
*Thanh-Ha Le, Jessy Clédière, Cécile Canovas, Bruno Robisson,
Christine Servièrre, Jean-Louis Lacoume*

High-Resolution Side-Channel Attack Using Phase-Based Waveform
Matching 187
*Naofumi Homma, Sei Nagashima, Yuichi Imai, Takafumi Aoki,
Akashi Satoh*

Cache-Collision Timing Attacks Against AES 201
Joseph Bonneau, Ilya Mironov

Provably Secure S-Box Implementation Based on Fourier Transform 216
Emmanuel Prouff, Christophe Giraud, Sébastien Aumônier

Invited Talk II

The Outer Limits of RFID Security 231
Ari Juels

Hardware Attacks and Countermeasures II

Three-Phase Dual-Rail Pre-charge Logic	232
<i>Marco Bucci, Luca Giancane, Raimondo Luzzi, Alessandro Trifiletti</i>	
Dual-Rail Random Switching Logic: A Countermeasure to Reduce Side Channel Leakage	242
<i>Zhimin Chen, Yujie Zhou</i>	
Security Evaluation of DPA Countermeasures Using Dual-Rail Pre-charge Logic Style	255
<i>Daisuke Suzuki, Minoru Sasaki</i>	

Efficient Hardware I

Instruction Set Extensions for Efficient AES Implementation on 32-bit Processors	270
<i>Stefan Tillich, Johann Großschädl</i>	
NanoCMOS-Molecular Realization of Rijndael	285
<i>Massoud Masoumi, Farshid Raissi, Mahmoud Ahmadian</i>	
Improving SHA-2 Hardware Implementations	298
<i>Ricardo Chaves, Georgi Kuzmanov, Leonel Sousa, Stamatis Vassiliadis</i>	

Trusted Computing

Offline Hardware/Software Authentication for Reconfigurable Platforms	311
<i>Eric Simpson, Patrick Schaumont</i>	

Side Channels III

Why One Should Also Secure RSA Public Key Elements	324
<i>Eric Brier, Benoît Chevallier-Mames, Mathieu Ciet, Christophe Clavier</i>	
Power Attack on Small RSA Public Exponent	339
<i>Pierre-Alain Fouque, Sébastien Kunz-Jacques, Gwenaëlle Martinet, Frédéric Muller, Frédéric Valette</i>	
Unified Point Addition Formulæ and Side-Channel Attacks	354
<i>Douglas Stebila, Nicolas Thériault</i>	

Hardware Attacks and Countermeasures III

Read-Proof Hardware from Protective Coatings 369
 *Pim Tuyls, Geert-Jan Schrijen, Boris Škorić, Jan van Geloven,
 Nynke Verhaegh, Rob Wolters*

Path Swapping Method to Improve DPA Resistance of Quasi Delay
Insensitive Asynchronous Circuits 384
 Fraidy Bouesse, Gilles Sicard, Marc Renaudin

Automated Design of Cryptographic Devices Resistant to Multiple
Side-Channel Attacks 399
 Konrad Kulikowski, Alexander Smirnov, Alexander Taubin

Invited Talk III

Challenges for Trusted Computing 414
 Ahmad-Reza Sadeghi

Efficient Hardware II

Superscalar Coprocessor for High-Speed Curve-Based Cryptography 415
 K. Sakiyama, L. Batina, B. Preneel, I. Verbauwhede

Hardware/Software Co-design of Elliptic Curve Cryptography
on an 8051 Microcontroller 430
 *Manuel Koschuch, Joachim Lechner, Andreas Weitzer,
 Johann Großschädl, Alexander Szekely, Stefan Tillich,
 Johannes Wolkerstorfer*

FPGA Implementation of Point Multiplication on Koblitz Curves
Using Kleinian Integers 445
 *V.S. Dimitrov, K.U. Järvinen, M.J. Jacobson Jr., W.F. Chan,
 Z. Huang*

Author Index 461