

Table of Contents

Practical Side-Channel Analysis

Exploiting the Difference of Side-Channel Leakages	1
<i>Michael Hutter, Mario Kirschbaum, Thomas Plos, Jörn-Marc Schmidt, and Stefan Mangard</i>	
Attacking an AES-Enabled NFC Tag: Implications from Design to a Real-World Scenario	17
<i>Thomas Korak, Thomas Plos, and Michael Hutter</i>	

Invited Talk I

700+ Attacks Published on Smart Cards: The Need for a Systematic Counter Strategy	33
<i>Mathias Wagner</i>	

Secure Design

An Interleaved EPE-Immune PA-DPL Structure for Resisting Concentrated EM Side Channel Attacks on FPGA Implementation	39
<i>Wei He, Eduardo de la Torre, and Teresa Riesgo</i>	
An Architectural Countermeasure against Power Analysis Attacks for FSR-Based Stream Ciphers	54
<i>Shohreh Sharif Mansouri and Elena Dubrova</i>	
Conversion of Security Proofs from One Leakage Model to Another: A New Issue	69
<i>Jean-Sébastien Coron, Christophe Giraud, Emmanuel Prouff, Soline Renner, Matthieu Rivain, and Praveen Kumar Vadnala</i>	

Side-Channel Attacks on RSA

Attacking Exponent Blinding in RSA without CRT	82
<i>Sven Bauer</i>	
A New Scan Attack on RSA in Presence of Industrial Countermeasures	89
<i>Jean Da Rolt, Amitabh Das, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre, and Ingrid Verbauwhede</i>	
RSA Key Generation: New Attacks	105
<i>Camille Vuillaume, Takashi Endo, and Paul Wooderson</i>	

Fault Attacks

A Fault Attack on the LED Block Cipher	120
<i>Philipp Jovanovic, Martin Kreuzer, and Ilia Polian</i>	
Differential Fault Analysis of Full LBlock	135
<i>Liang Zhao, Takashi Nishide, and Kouichi Sakurai</i>	
Contactless Electromagnetic Active Attack on Ring Oscillator Based True Random Number Generator	151
<i>Pierre Bayon, Lilian Bossuet, Alain Aubert, Viktor Fischer, François Poucheret, Bruno Robisson, and Philippe Maurine</i>	

Invited Talk II

A Closer Look at Security in Random Number Generators Design	167
<i>Viktor Fischer</i>	

Side-Channel Attacks on ECC

Same Values Power Analysis Using Special Points on Elliptic Curves ...	183
<i>Cédric Murdica, Sylvain Guilley, Jean-Luc Danger, Philippe Hoogvorst, and David Naccache</i>	
The Schindler-Ittoh-attack in Case of Partial Information Leakage	199
<i>Alexander Krüger</i>	

Different Methods in Side-Channel Analysis

Butterfly-Attack on Skein's Modular Addition	215
<i>Michael Zohner, Michael Kasper, and Marc Stöttinger</i>	
MDASCA: An Enhanced Algebraic Side-Channel Attack for Error Tolerance and New Leakage Model Exploitation	231
<i>Xinjie Zhao, Fan Zhang, Shize Guo, Tao Wang, Zhijie Shi, Huiying Liu, and Keke Ji</i>	
Intelligent Machine Homicide: Breaking Cryptographic Devices Using Support Vector Machines	249
<i>Annelie Heuser and Michael Zohner</i>	

Author Index	265
--------------------	-----