

Table of Contents

Malicious Code on Java Card Smartcards: Attacks and Countermeasures.....	1
<i>Wojciech Mostowski and Erik Poll</i>	
Static Program Analysis for Java Card Applets	17
<i>Vasilios Almaliotis, Alexandros Loizidis, Panagiotis Katsaros, Panagiotis Louridas, and Diomidis Spinellis</i>	
On Practical Information Flow Policies for Java-Enabled Multiapplication Smart Cards	32
<i>Dorina Ghindici and Isabelle Simplot-Ryl</i>	
New Differential Fault Analysis on AES Key Schedule: Two Faults Are Enough	48
<i>Chong Hee Kim and Jean-Jacques Quisquater</i>	
DSA Signature Scheme Immune to the Fault Cryptanalysis.....	61
<i>Maciej Nikodem</i>	
A Black Hen Lays White Eggs: Bipartite Multiplier Out of Montgomery One for On-Line RSA Verification	74
<i>Masayuki Yoshino, Katsuyuki Okeya, and Camille Vuillaume</i>	
Ultra-Lightweight Implementations for Smart Devices – Security for 1000 Gate Equivalents	89
<i>Carsten Rolfes, Axel Poschmann, Gregor Leander, and Christof Paar</i>	
Fast Hash-Based Signatures on Constrained Devices	104
<i>Sebastian Rohde, Thomas Eisenbarth, Erik Dahmen, Johannes Buchmann, and Christof Paar</i>	
Fraud Detection and Prevention in Smart Card Based Environments Using Artificial Intelligence.....	118
<i>Wael William Zakhari Malek, Keith Mayes, and Kostas Markantonakis</i>	
The Trusted Execution Module: Commodity General-Purpose Trusted Computing	133
<i>Victor Costan, Luis F.G. Sarmenta, Marten van Dijk, and Srinivas Devadas</i>	
Management of Multiple Cards in NFC-Devices	149
<i>Gerald Madlmayr, Oliver Dillinger, Josef Langer, and Josef Scharinger</i>	

Coupon Recalculation for the GPS Authentication Scheme	162
<i>Georg Hofferek and Johannes Wolkerstorfer</i>	
Provably Secure Grouping-Proofs for RFID Tags	176
<i>Mike Burmester, Breno de Medeiros, and Rossana Motta</i>	
Secure Implementation of the Stern Authentication and Signature Schemes for Low-Resource Devices	191
<i>Pierre-Louis Cayrel, Philippe Gaborit, and Emmanuel Prouff</i>	
A Practical DPA Countermeasure with BDD Architecture	206
<i>Toru Akishita, Masanobu Katagi, Yoshikazu Miyato, Asami Mizuno, and Kyoji Shibutani</i>	
SCARE of an Unknown Hardware Feistel Implementation	218
<i>Denis Réal, Vivien Dubois, Anne-Marie Guilloux, Frédéric Valette, and Mhamed Drissi</i>	
Evaluation of Java Card Performance	228
<i>Samia Bouzefrane, Julien Cordry, Hervé Meunier, and Pierre Paradinas</i>	
Application of Network Smart Cards to Citizens Identification Systems	241
<i>Joaquin Torres, Mildrey Carbonell, Jesus Tellez, and Jose M. Sierra</i>	
SmartPRO: A Smart Card Based Digital Content Protection for Professional Workflow	255
<i>Alain Durand, Marc Éluard, Sylvain Lelievre, and Christophe Vincent</i>	
A Practical Attack on the MIFARE Classic	267
<i>Gerhard de Koning Gans, Jaap-Henk Hoepman, and Flavio D. Garcia</i>	
A Chemical Memory Snapshot	283
<i>Jörn-Marc Schmidt</i>	
Recent Advances in Electronic Cash Design	290
<i>Aline Gouget</i>	
Author Index	295