

Table of Contents

Smart Card Applications

Design, Installation and Execution of a Security Agent for Mobile Stations

*William G. Sirett, John A. MacDonald, Keith Mayes,
Konstantinos Markantonakis* 1

Towards a Secure and Practical Multifunctional Smart Card

Idir Bakdi 16

Implementing Cryptography on TFT Technology for Secure Display Applications

Petros Oikonomakos, Jacques Fournier, Simon Moore 32

A Smart Card-Based Mental Poker System

Jordi Castellà-Roca, Josep Domingo-Ferrer, Francesc Sebé 48

A Smart Card Solution for Access Control and Trust Management for Nomadic Users

*Daniel Díaz Sánchez, Andrés Marín Lopez,
Florina Almenárez Mendoza* 62

Smart Cards and Residential Gateways: Improving OSGi Services with Java Cards

*Juan Jesús Sánchez Sánchez, Daniel Díaz Sánchez,
José Alberto Vigo Segura, Natividad Martínez Madrid,
Ralf Seepold* 78

Zero Footprint Secure Internet Authentication Using Network Smart Card

Asad M. Ali 91

An Optimistic NBAC-Based Fair Exchange Method for Arbitrary Items

Masayuki Terada, Kensaku Mori, Sadayuki Hongo 105

Side Channel Attacks

Generic Cryptanalysis of Combined Countermeasures with Randomized BSD Representations

Tae Hyun Kim, Dong-Guk Han, Katsuyuki Okeya, Jongin Lim 119

Amplifying Side-Channel Attacks with Techniques from Block Cipher
Cryptanalysis
Raphael C.-W. Phan, Sung-Ming Yen 135

Power Analysis to ECC Using Differential Power Between Multiplication
and Squaring
Toru Akishita, Tsuyoshi Takagi 151

Smart Card Networking

Designing Smartcards for Emerging Wireless Networks
Pascal Urien, Mesmin Dandjinou 165

Smartcard Firewalls Revisited
Henrich C. Pöhls, Joachim Posegga 179

Multi-stage Packet Filtering in Network Smart Cards
HongQian Karen Lu 192

Cryptographic Protocols

Anonymous Authentication with Optional Shared Anonymity
Revocation and Linkability
Martin Schaffer, Peter Schartner 206

SEA: A Scalable Encryption Algorithm for Small Embedded
Applications
*François-Xavier Standaert, Gilles Piret, Neil Gershenfeld,
Jean-Jacques Quisquater* 222

Low-Cost Cryptography for Privacy in RFID Systems
Benoît Calmels, Sébastien Canard, Marc Girault, Hervé Sibert 237

Optimal Use of Montgomery Multiplication on Smart Cards
Arnaud Boscher, Robert Naciri 252

Off-Line Group Signatures with Smart Cards
Jean-Bernard Fischer, Emmanuel Prouff 263

RFID Security

Analysis of Power Constraints for Cryptographic Algorithms in
Mid-Cost RFID Tags
Tobias Lohmann, Matthias Schneider, Christoph Ruland 278

Noisy Tags: A Pretty Good Key Exchange Protocol for RFID Tags <i>Claude Castelluccia, Gildas Avoine</i>	289
--	-----

MARP: Mobile Agent for RFID Privacy Protection <i>Soo-Cheol Kim, Sang-Soo Yeo, Sung Kwon Kim</i>	300
---	-----

Formal Methods

Certifying Native Java Card API by Formal Refinement <i>Quang-Huy Nguyen, Boutheina Chetali</i>	313
--	-----

A Low-Footprint Java-to-Native Compilation Scheme Using Formal Methods <i>Alexandre Courbot, Mariela Pavlova, Gilles Grimaud, Jean-Jacques Vandewalle</i>	329
---	-----

Automatic Test Generation on a (U)SIM Smart Card <i>Céline Bigot, Alain Faivre, Christophe Gaston, Julien Simon</i>	345
--	-----

Author Index	359
--------------------	-----