

Table of Contents

Invited Paper

Privacy-Preserving Speaker Authentication	1
<i>Manas Pathak, Jose Portelo, Bhiksha Raj, and Isabel Trancoso</i>	

Cryptography and Cryptanalysis

Differential Attacks on Reduced RIPEMD-160	23
<i>Florian Mendel, Tomislav Nad, Stefan Scherz, and Martin Schl��ffer</i>	
Revisiting Difficulty Notions for Client Puzzles and DoS Resilience	39
<i>Bogdan Groza and Bogdan Warinschi</i>	
On Optimal Bounds of Small Inverse Problems and Approximate GCD Problems with Higher Degree	55
<i>Noboru Kunihiro</i>	

Mobility

Strong Authentication with Mobile Phone	70
<i>Sanna Suoranta, Andr�� Andrade, and Tuomas Aura</i>	
Measuring SSL Indicators on Mobile Browsers: Extended Life, or End of the Road?	86
<i>Chaitrali Amrutkar, Patrick Traynor, and Paul C. van Oorschot</i>	

Cards and Sensors

Domain-Specific Pseudonymous Signatures for the German Identity Card	104
<i>Jens Bender, ��zg��r Dagdelen, Marc Fischlin, and Dennis K��gler</i>	
Solutions for the Storage Problem of McEliece Public and Private Keys on Memory-Constrained Platforms	120
<i>Falko Strenzke</i>	
100% Connectivity for Location Aware Code Based KPD in Clustered WSN: Merging Blocks	136
<i>Samiran Bag, Aritra Dhar, and Pinaki Sarkar</i>	

Software Security

Learning Fine-Grained Structured Input for Memory Corruption
Detection 151
Lei Zhao, Debin Gao, and Lina Wang

Dynamic Anomaly Detection for More Trustworthy Outsourced
Computation 168
*Sami Alsouri, Jan Sinschek, Andreas Sewe, Eric Bodden,
Mira Mezini, and Stefan Katzenbeisser*

An Empirical Study of Dangerous Behaviors in Firefox Extensions 188
*Jiangang Wang, Xiaohong Li, Xuhui Liu, Xinshu Dong,
Junjie Wang, Zhenkai Liang, and Zhìyong Feng*

Processing Encrypted Data

Collaboration-Preserving Authenticated Encryption for Operational
Transformation Systems 204
*Michael Clear, Karl Reid, Desmond Ennis, Arthur Hughes, and
Hitesh Tewari*

Selective Document Retrieval from Encrypted Database..... 224
Christoph Bösch, Qiang Tang, Pieter Hartel, and Willem Jonker

Additively Homomorphic Encryption with a Double Decryption
Mechanism, Revisited 242
Andreas Peter, Max Kronberg, Wilke Trei, and Stefan Katzenbeisser

Authentication and Identification

Secure Hierarchical Identity-Based Identification without Random
Oracles 258
Atsushi Fujioka, Taichi Saito, and Keita Xagawa

Efficient Two-Move Blind Signatures in the Common Reference String
Model 274
E. Ghadafi and N.P. Smart

New Directions in Access Control

Compliance Checking for Usage-Constrained Credentials in Trust
Negotiation Systems..... 290
Jinwei Hu, Khaled M. Khan, Yun Bai, and Yan Zhang

A Quantitative Approach for Inexact Enforcement of Security
Policies 306
Peter Drábik, Fabio Martinelli, and Charles Morisset

OSDM: An Organizational Supervised Delegation Model for RBAC	322
<i>Nezar Nassr, Nidal Aboudagga, and Eric Steegmans</i>	

GPU for Security

GPU-Acceleration of Block Ciphers in the OpenSSL Cryptographic Library	338
<i>Johannes Gilger, Johannes Barnickel, and Ulrike Meyer</i>	

A Highly-Efficient Memory-Compression Approach for GPU-Accelerated Virus Signature Matching	354
<i>Ciprian Pungila and Viorel Negru</i>	

Models for Risk and Revocation

Intended Actions: Risk Is Conflicting Incentives	370
<i>Lisa Rajbhandari and Einar Snekkenes</i>	

On the Self-similarity Nature of the Revocation Data	387
<i>Carlos Gañán, Jorge Mata-Díaz, Jose L. Muñoz, Oscar Esparza, and Juanjo Alins</i>	

Author Index	401
------------------------	-----