

Table of Contents

Signatures

A New RSA-Based Signature Scheme	1
<i>Sven Schäge and Jörg Schwenk</i>	
Fair Blind Signatures without Random Oracles	16
<i>Georg Fuchsbaauer and Damien Vergnaud</i>	
Fair Partially Blind Signatures	34
<i>Markus Rückert and Dominique Schröder</i>	

Attacks

Parallel Shortest Lattice Vector Enumeration on Graphics Cards	52
<i>Jens Hermans, Michael Schneider, Johannes Buchmann, Frederik Vercauteren, and Bart Preneel</i>	
Flexible Partial Enlargement to Accelerate Gröbner Basis Computation over $\mathbb{F}_2$	69
<i>Johannes Buchmann, Daniel Cabarcas, Jintai Ding, and Mohamed Saied Emam Mohamed</i>	
Factoring RSA Modulus Using Prime Reconstruction from Random Known Bits	82
<i>Subhamoy Maitra, Santanu Sarkar, and Sourav Sen Gupta</i>	

Protocols

Proofs of Restricted Shuffles	100
<i>Björn Terehus and Douglas Wikström</i>	
Batch Range Proof for Practical Small Ranges	114
<i>Kun Peng and Feng Bao</i>	
Optimistic Fair Priced Oblivious Transfer	131
<i>Alfredo Rial and Bart Preneel</i>	

Networks

Information-Theoretically Secure Key-Insulated Multireceiver Authentication Codes	148
<i>Takenobu Seito, Tadashi Aikawa, Junji Shikata, and Tsutomu Matsumoto</i>	

Simple and Communication Complexity Efficient Almost Secure and Perfectly Secure Message Transmission Schemes	166
<i>Yvo Desmedt, Stelios Erotokritou, and Reihaneh Safavi-Naini</i>	

Communication Efficient Perfectly Secure VSS and MPC in Asynchronous Networks with Optimal Resilience	184
<i>Arpita Patra, Ashish Choudhury, and C. Pandu Rangan</i>	

Elliptic Curves

Avoiding Full Extension Field Arithmetic in Pairing Computations	203
<i>Craig Costello, Colin Boyd, Juan Manuel González Nieto, and Kenneth Koon-Ho Wong</i>	

ECC2K-130 on Cell CPUs	225
<i>Joppe W. Bos, Thorsten Kleinjung, Ruben Niederhagen, and Peter Schwabe</i>	

Side-Channel Attacks and Fault Attacks

Practical Improvements of Profiled Side-Channel Attacks on a Hardware Crypto-Accelerator	243
<i>M. Abdelaziz Elaabid and Sylvain Guilley</i>	

Differential Fault Analysis of HC-128	261
<i>Aleksandar Kircanski and Amr M. Youssef</i>	

Fresh Re-keying: Security against Side-Channel and Fault Attacks for Low-Cost Devices	279
<i>Marcel Medwed, François-Xavier Standaert, Johann Großschädl, and Francesco Regazzoni</i>	

Public-Key Encryption

Strong Cryptography from Weak Secrets: Building Efficient PKE and IBE from Distributed Passwords	297
<i>Xavier Boyen, Céline Chevalier, Georg Fuchsbauer, and David Pointcheval</i>	

Efficient Unidirectional Proxy Re-Encryption	316
<i>Sherman S.M. Chow, Jian Weng, Yanjiang Yang, and Robert H. Deng</i>	

Public-Key Encryption with Non-interactive Opening: New Constructions and Stronger Definitions	333
<i>David Galindo, Benoît Libert, Marc Fischlin, Georg Fuchsbauer, Anja Lehmann, Mark Manulis, and Dominique Schröder</i>	

Keys and PUFs

Flexible Group Key Exchange with On-demand Computation of Subgroup Keys	351
<i>Michel Abdalla, Céline Chevalier, Mark Manulis, and David Pointcheval</i>	
Quantum Readout of Physical Unclonable Functions	369
<i>Boris Škorić</i>	

Ciphers and Hash Functions

Parallelizing the Camellia and SMS4 Block Ciphers	387
<i>Huihui Yap, Khoongming Khoo, and Axel Poschmann</i>	
Improved Linear Differential Attacks on CubeHash	407
<i>Shahram Khazaei, Simon Knellwolf, Willi Meier, and Deian Stefan</i>	
Cryptanalysis of the 10-Round Hash and Full Compression Function of SHA-3	419
<i>Praveen Gauravaram, Gaëtan Leurent, Florian Mendel, María Naya-Plasencia, Thomas Peyrin, Christian Rechberger, and Martin Schläpfer</i>	
Author Index	437