Table of Contents

Hash Functions

Second Preimage Attack on 5-Pass HAVAL and Partial Key-Recovery Attack on HMAC/NMAC-5-Pass HAVAL 1
Gaoli Wang and Shaohui Wang

Cryptanalysis of Vortex 14
Jean-Philippe Aumasson, Orr Dunkelman, Florian Mendel, Christian Rechberger, and Søren S. Thomsen

Two Passes of Tiger Are Not One-Way 29
Florian Mendel

Block Ciphers

Generic Attacks on Feistel Networks with Internal Permutations 41
Joana Treger and Jacques Patarin

Distinguishers for Ciphers and Known Key Attack against Rijndael with Large Blocks 60
Marine Minier, Raphael C.-W. Phan, and Benjamin Pousse

Asymmetric Encryption

Reducing Key Length of the McEliece Cryptosystem 77
Thierry P. Berger, Pierre-Louis Cayrel, Philippe Gaborit, and Ayoub Otmani

Cryptanalysis of RSA Using the Ratio of the Primes 98
Abderrahmane Nitaj

Digital Signatures

New RSA-Based (Selectively) Convertible Undeniable Signature Schemes 116
Le Trieu Phong, Kaoru Kurosawa, and Wakaha Ogata

A Schnorr-Like Lightweight Identity-Based Signature Scheme 135
David Galindo and Flavio D. Garcia

On the Theoretical Gap between Group Signatures with and without Unlinkability 149
Go Ohtake, Arisa Fujii, Goichiro Hanaoka, and Kazuto Ogawa

Practical Threshold Signatures with Linear Secret Sharing Schemes 167
İlker Nadi Bozkurt, Kamer Kaya, and Ali Aydın Selçuk

Asymmetric Encryption and Anonymity

Certified Encryption Revisited 179
Pooya Farshim and Bogdan Warinschi

Threshold Attribute-Based Signatures and Their Application to Anonymous Credential Systems 198
Siamak F. Shahandashti and Reihaneh Safavi-Naini

Anonymity from Public Key Encryption to Undeniable Signatures 217
Laila El Aimani

Key Agreement Protocols

Security Analysis of Standard Authentication and Key Agreement Protocols Utilising Timestamps 235
Manuel Barbosa and Pooya Farshim

Password-Authenticated Group Key Agreement with Adaptive Security and Contributiveness 254
Michel Abdalla, Dario Catalano, Céline Chevalier, and David Pointcheval

Cryptographic Protocols

Unifying Zero-Knowledge Proofs of Knowledge 272
Ueli Maurer

Co-sound Zero-Knowledge with Public Keys 287
Carmine Ventre and Ivan Visconti

Another Look at Extended Private Information Retrieval Protocols 305
Julien Bringer and Hervé Chabanne

Constructing Universally Composable Oblivious Transfers from Double Trap-Door Encryptions 323
Huafei Zhu and Feng Bao

Efficient Implementations

Exponent Recoding and Regular Exponentiation Algorithms 334
Marc Joye and Michael Tunstall

Efficient Acceleration of Asymmetric Cryptography on Graphics Hardware 350
Owen Harrison and John Waldron

Fast Elliptic-Curve Cryptography on the Cell Broadband Engine 368
Neil Costigan and Peter Schwabe

On Modular Decomposition of Integers 386
Billy Bob Brumley and Kaisa Nyberg

Implementation Attacks

Breaking KeeLoq in a Flash: On Extracting Keys at Lightning Speed 403
Markus Kasper, Timo Kasper, Amir Moradi, and Christof Paar

An Improved Fault Based Attack of the Advanced Encryption Standard 421
Debdeep Mukhopadhyay

Author Index 435