Table of Contents

Block Ciphers

Essential Algebraic Structure within the AES 1
Sean Murphy and Matthew J.B. Robshaw

Blockwise-Adaptive Attackers: Revisiting the (In)Security of Some Provably Secure Encryption Modes: CBC, GEM, IACBC 17
Antoine Joux, Gwenaëlle Martinet, and Frédéric Valette

Tweakable Block Ciphers 31
Moses Liskov, Ronald L. Rivest, and David Wagner

Multi-user Oriented Cryptosystems

The LSD Broadcast Encryption Scheme 47
Dani Halevy and Adi Shamir

Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials 61
Jan Camenisch and Anna Lysyanskaya

Foundations and Methodology

Provably Secure Steganography (Extended Abstract) 77
Nicholas J. Hopper, John Langford, and Luis von Ahn

Flaws in Applying Proof Methodologies to Signature Schemes 93
Jacques Stern, David Pointcheval, John Malone-Lee, and Nigel P. Smart

Separating Random Oracle Proofs from Complexity Theoretic Proofs: The Non-committing Encryption Case 111
Jesper Buus Nielsen

Security of Practical Protocols

On the Security of RSA Encryption in TLS 127
Jakob Jonsson and Burton S. Kaliski Jr.

Security Analysis of IKE's Signature-Based Key-Exchange Protocol 143
Ran Canetti and Hugo Krawczyk

GQ and Schnorr Identification Schemes: Proofs of Security against Impersonation under Active and Concurrent Attacks 162
Mihir Bellare and Adriana Palacio

Secure Multiparty Computation

On 2-Round Secure Multiparty Computation 178
Rosario Gennaro, Yuval Ishai, Eyal Kushilevitz, and Tal Rabin

Private Computation – k-Connected versus 1-Connected Networks 194
Markus Bläser, Andreas Jakoby, Maciej Liśkiewicz, and Bodo Siebert

Public-Key Encryption

Analysis and Improvements of NTRU Encryption Paddings 210
Phong Q. Nguyen and David Pointcheval

Universal Padding Schemes for RSA 226
Jean-Sébastien Coron, Marc Joye, David Naccache, and Pascal Paillier

Cryptanalysis of Unbalanced RSA with Small CRT-Exponent 242
Alexander May

Information Theory and Secret Sharing

Hyper-encryption against Space-Bounded Adversaries
from On-Line Strong Extractors 257
Chi-Jen Lu

Optimal Black-Box Secret Sharing over Arbitrary Abelian Groups 272
Ronald Cramer and Serge Fehr

Cipher Design and Analysis

A Generalized Birthday Problem (Extended Abstract) 288
David Wagner

(Not So) Random Shuffles of RC4 304
Ilya Mironov

Black-Box Analysis of the Block-Cipher-Based Hash-Function
Constructions from PGV 320
John Black, Phillip Rogaway, and Thomas Shrimpton

Elliptic Curves and Abelian Varieties

Supersingular Abelian Varieties in Cryptology 336
Karl Rubin and Alice Silverberg

Efficient Algorithms for Pairing-Based Cryptosystems 354
Paulo S.L.M. Barreto, Hae Y. Kim, Ben Lynn, and Michael Scott

Computing Zeta Functions of Hyperelliptic Curves over Finite Fields of Characteristic 2 369
Frederik Vercauteren

Password-Based Authentication

Threshold Password-Authenticated Key Exchange (Extended Abstract) . . . 385
Philip MacKenzie, Thomas Shrimpton, and Markus Jakobsson

Distributed Cryptosystems

A Threshold Pseudorandom Function Construction and Its Applications . . 401
Jesper Buus Nielsen

Efficient Computation Modulo a Shared Secret with Application to the Generation of Shared Safe-Prime Products 417
Joy Algesheimer, Jan Camenisch, and Victor Shoup

Pseudorandomness and Applications

Hidden Number Problem with the Trace and Bit Security of XTR and LUC 433
Wen-Ching W. Li, Mats Näslund, and Igor E. Shparlinski

Expanding Pseudorandom Functions; or: From Known-Plaintext Security to Chosen-Plaintext Security 449
Ivan Damgård and Jesper Buus Nielsen

Variations on Signatures and Authentication

Threshold Ring Signatures and Applications to Ad-hoc Groups 465
Emmanuel Bresson, Jacques Stern, and Michael Szydlo

Deniable Ring Authentication 481
Moni Naor

SiBIR: Signer-Base Intrusion-Resilient Signatures 499
Gene Itkis and Leonid Reyzin

Stream Ciphers and Boolean Functions

Cryptanalysis of Stream Ciphers with Linear Masking 515
Don Coppersmith, Shai Halevi, and Charanjit Jutla

The Filter-Combiner Model for Memoryless Synchronous Stream Ciphers . 533
Palash Sarkar

A Larger Class of Cryptographic Boolean Functions via a Study of the Maiorana-McFarland Construction 549
Claude Carlet

Commitment Schemes

Linear VSS and Distributed Commitments Based on Secret Sharing and Pairwise Checks ... 565
Serge Fehr and Ueli Maurer

Perfect Hiding and Perfect Binding Universally Composable Commitment Schemes with Constant Expansion Factor ... 581
Ivan Damgård and Jesper Buus Nielsen

Signature Schemes

Unique Signatures and Verifiable Random Functions from the DH-DDH Separation ... 597
Anna Lysyanskaya

Security Proof for Partial-Domain Hash Signature Schemes ... 613
Jean-Sébastien Coron

Author Index ... 627