Public Key Encryption
On the Broadcast and Validity-Checking Security of PKCS#1 v1.5 Encryption p. 1
How to Construct Interval Encryption from Binary Tree Encryption p. 19
Shrinking the Keys of Discrete-Log-Type Lossy Trapdoor Functions p. 35
Digital Signature
Trapdoor Sanitizable Signatures Made Easy p. 53
Generic Constructions for Verifiably Encrypted Signatures without Random Oracles or NIZKs p. 69
Redactable Signatures for Tree-Structured Data: Definitions and Constructions p. 87
Block Ciphers and Hash Functions
Impossible Differential Cryptanalysis on Feistel Ciphers with S P and S P S Round Functions p. 105
Multi-trail Statistical Saturation Attacks p. 123
Multiset Collision Attacks on Reduced-Round SNOW 3G and SNOW 3G p. 139
High Performance GHASH Function for Long Messages p. 154
Side-Channel Attacks
Principles on the Security of AES against First and Second-Order Differential Power Analysis p. 168
Adaptive Chosen-Message Side-Channel Attacks p. 186
Secure Multiplicative Masking of Power Functions p. 200
Zero Knowledge and Multi-party Protocols
Batch Groth-Sahai p. 218
Efficient and Secure Evaluation of Multivariate Polynomials and Applications p. 236
Efficient Implementation of the Orlandi Protocol p. 255
Improving the Round Complexity of Traitor Tracing Schemes p. 273
Key Management
Password Based Key Exchange Protocols on Elliptic Curves Which Conceal the Public Parameters p. 291
Okamoto-Tanaka Revisited: Fully Authenticated Diffie-Hellman with Minimal Overhead p. 309
Deniable Internet Key Exchange p. 329
Authentication and Identification
A New Human Identification Protocol and Coppersmith's Baby-Step Giant-Step Algorithm p. 349
Secure Sketch for Multiple Secrets p. 367
A Message Recognition Protocol Based on Standard Assumptions p. 384
Privacy and Anonymity
Affiliation-Hiding Key Exchange with Untrusted Group Authorities p. 402
Privacy-Preserving Group Discovery with Linear Complexity p. 420
Two New Efficient PIR-writing Protocols p. 438
Regulatory Compliant Oblivious RAM p. 456
RFID Security and Privacy
Revisiting Unpredictability-Based RFID Privacy Models p. 475

On RFID Privacy with Mutual Authentication and Tag Corruption p. 493
Internet Security
Social Network-Based Botnet Command-and-Control: Emerging Threats and Countermeasures p. 511
COP: A Step toward Children Online Privacy p. 529
A Hybrid Method to Detect Deflation Fraud in Cost-Per-Action Online Advertising p. 545
Author Index p. 563
Table of Contents provided by Blackwell's Book Services and R.R. Bowker. Used with permission.