A Group Signature Scheme With Efficient Membership Revocation for Reasonable Groups p. 336

Convertible Nominative Signatures p. 348

Protocols
Protocols With Security Proofs for Mobile Applications p. 358
Secure Bilinear Diffie-Hellman Bits p. 370
Weak Property of Malleability in NTRUSign p. 379

Security Management
Information Security Risk Assessment, Aggregation, and Mitigation p. 391

Access Control and Authorisation
A Weighted Graph Approach to Authorization Delegation and Conflict Resolution p. 402
Authorization Mechanisms for Virtual Organizations in Distributed Computing Systems p. 414

Cryptosystems (II)
Unconditionally Secure Encryption Under Strong Attacks p. 427
ManTiCore: Encryption With Joint Cipher-State Authentication p. 440

Cryptanalysis (III)
On Security of XTR Public Key Cryptosystems Against Side Channel Attacks p. 454
On the Exact Flexibility of the Flexible Countermeasure Against Side Channel Attacks p. 466

Fault Attacks on Signature Schemes p. 478

Author Index p. 493

Table of Contents provided by Blackwell's Book Services and R.R. Bowker. Used with permission.