Network/Computer Security
Impacts of Security Protocols on Real-Time Multimedia Communications p. 1
An Improvement on Privacy and Authentication in GSM p. 14
Encrypted Watermarks and Linux Laptop Security p. 27
Inconsistency Detection of Authorization Policies in Distributed Component Environment p. 39
Public Key Schemes I
Custodian-Hiding Verifiable Encryption p. 51
Proving Key Usage p. 65
Public Key Encryption with Conjunctive Field Keyword Search p. 73
Intrusion Detection I
A Probabilistic Method for Detecting Anomalous Program Behavior p. 87
Service Discrimination and Audit File Reduction for Effective Intrusion Detection p. 99
IDS False Alarm Filtering Using KNN Classifier p. 114
Watermarking/Anti-spamming
Content-Based Synchronization Using the Local Invariant Feature for Robust Watermarking p. 122
Some Fitting of Naive Bayesian Spam Filtering for Japanese Environment p. 135
Public Key Schemes II
Efficient Authenticated Key Agreement Protocol for Dynamic Groups p. 144
A Ring Signature Scheme Using Bilinear Pairings p. 160
Verifiable Pairing and Its Applications p. 170
Intrusion Detection II
Improving the Performance of Signature-Based Network Intrusion Detection Sensors by Multi-threading p. 188
An Effective Placement of Detection Systems for Distributed Attack Detection in Large Scale Networks p. 204
Application of Content Computing in Honeyfarm p. 211
Digital Rights Management
License Protection with a Tamper-Resistant Token p. 223
An Adaptive Approach to Hardware Alteration for Digital Rights Management p. 238
Dynamic Fingerprinting over Broadcast Using Revocation Scheme p. 251
Practical Pay-TV Scheme Using Traitor Tracing Scheme for Multiple Channels p. 264
e-Commerce Security
Vulnerability of a Mobile Payment System Proposed at WISA 2002 p. 278
Fair Offline Payment Using Verifiable Encryption p. 286
A Limited-Use Key Generation Scheme for Internet Transactions p. 302
Efficient Implementation
Efficient Representation and Software Implementation of Resilient Maiorana-McFarland S-boxes p. 317
Signed Digit Representation with NAF and Balanced Ternary Form and Efficient Exponentiation in GF(q p. 332
Novel Efficient Implementations of Hyperelliptic Curve Cryptosystems Using Degenerate Divisors p. 345
Hyperelliptic Curve Coprocessors on a FPGA p. 360
Anonymous Communication Key-Exchange Protocol Using Pre-agreed Session-ID p. 375
A New k-Anonymous Message Transmission Protocol p. 388
Onions Based on Universal Re-encryption - Anonymous Communication Immune Against Repetitive Attack p. 400
Side-Channel Attacks Side Channel Cryptanalysis on SEED p. 411
Secure and Efficient AES Software Implementation for Smart Cards p. 425
Practical Template Attacks p. 440
Evaluation and Improvement of the Tempest Fonts p. 457
Author Index p. 471

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