Authentication and Key Exchange

Time and Space Efficient Algorithms for Two-Party Authenticated Data Structures p. 1
New Construction of Group Secret Handshakes Based on Pairings p. 16
nPAKE\[^{+}\]: A Hierarchical Group Password-Authenticated Key Exchange Protocol Using Different Passwords p. 31
An Efficient Password-Only Two-Server Authenticated Key Exchange System p. 44

Digital Signatures

Formal Definition and Construction of Nominative Signature p. 57
Short Group Signature Without Random Oracles p. 69
(Convertible) Undeniable Signatures Without Random Oracles p. 83

Applications

A New Dynamic Accumulator for Batch Updates p. 98
Preventing Unofficial Information Propagation p. 113
A Novel Method for Micro-Aggregation in Secure Statistical Databases Using Association and Interaction p. 126
Privacy Protection on Multiple Sensitive Attributes p. 141

Watermarking

Audio Watermarking Algorithm Based on Centroid and Statistical Features p. 153
A Semi-blind Watermarking Based on Discrete Wavelet Transform p. 164

Fast Implementations

On the Design of Fast Prefix-Preserving IP Address Anonymization Scheme p. 177
High Speed Modular Divider Based on GCD Algorithm p. 189
MDH: A High Speed Multi-phase Dynamic Hash String Matching Algorithm for Large-Scale Pattern Set p. 201
Compact and Secure Design of Masked AES S-Box p. 216

Applied Cryptography

Boudot’s Range-Bounded Commitment Scheme Revisited p. 230
Toward Practical Anonymous Rerandomizable RCCA Secure Encryptions p. 239
Secure Multiparty Computation of DNF p. 254

Cryptanalysis

Square Like Attack on Camellia p. 269
Differential Fault Analysis on CLEFIA p. 284
Extending FORK-256 Attack to the Full Hash Function p. 296
Attacking Reduced-Round Versions of the SMS4 Block Cipher in the Chinese WAPI Standard p. 306

Formal Analysis

A Framework for Game-Based Security Proofs p. 319
Modeling Agreement Problems in the Universal Composability Framework p. 350
System Security I

A System Architecture for History-Based Access Control for XML Documents p. 362
Power Efficient Hardware Architecture of SHA-1 Algorithm for Trusted Mobile Computing p. 375
Auth-SL - A System for the Specification and Enforcement of Quality-Based Authentication Policies p. 386
System Security II
A Novel Approach for Untrusted Code Execution p. 398
Detection and Diagnosis of Control Interception p. 412
BIOS Security Analysis and a Kind of Trusted BIOS p. 427
Collecting Autonomous Spreading Malware Using High-Interaction Honeypots p. 438
Network Security
DDoS Attack Detection Algorithms Based on Entropy Computing p. 452
Firewall for Dynamic IP Address in Mobile IPv6 p. 467
Application of the PageRank Algorithm to Alarm Graphs (Extended Abstract) p. 480
Drive-By Pharming p. 495
Author Index p. 507

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