Public Key Crypto Applications
Universal \([\eta][\text{subscript} T]\) Pairing Algorithm over Arbitrary Extension Degree p. 1
Convertible Undeniable Proxy Signatures: Security Models and Efficient Construction p. 16
Biometrics/Information Hiding
Implementation of BioAPI Conformance Test Suite Using BSP Testing Model p. 48
Information Hiding in Software with Mixed Boolean-Arithmetic Transforms p. 61
Geometrically Invariant Image Watermarking in the DWT Domain p. 76
Secure Hardware
Implementation of LSM-Based RBAC Module for Embedded System p. 91
Iteration Bound Analysis and Throughput Optimum Architecture of SHA-256 (384, 512) for Hardware Implementations p. 102
A Compact Architecture for Montgomery Elliptic Curve Scalar Multiplication Processor p. 115
Secure Systems
Windows Vault: Prevention of Virus Infection and Secret Leakage with Secure OS and Virtual Machine p. 128
An Architecture Providing Virtualization-Based Protection Mechanisms Against Insider Attacks p. 142
Detecting Motifs in System Call Sequences p. 157
Wireless and Mobile Security
Comparative Studies in Key Disagreement Correction Process on Wireless Key Agreement System p. 173
Breaking 104 Bit WEP in Less Than 60 Seconds p. 188
Efficient Implementation of the Pairing on Mobilephones Using BREW p. 203
Application Security/Secure Systems
Security Analysis of MISTY1 p. 215
A Generic Method for Secure SBox Implementation p. 227
On the Security of a Popular Web Submission and Review Software (WSaR) for Cryptology Conferences p. 245
Access Control/DB Security
Authorization Constraints Specification of RBAC p. 266
Dynamic Access Control Research for Inter-operation in Multi-domain Environment Based on Risk p. 277
Smart Cards/Secure Systems
Longer Randomly Blinded RSA Keys May Be Weaker Than Shorter Ones p. 303
Differential Power Analysis of HMAC Based on SHA-2, and Countermeasures p. 317
Provably Secure Countermeasure Resistant to Several Types of Power Attack for ECC p. 333
Anonymity and P2P Security
Risk &amp; Distortion Based K-Anonymity p. 345
Optimizing Quality Levels and Development Costs for Developing an Integrated Information Security System p. 359