A Review of the SESAME Development
The Security of Public Key Cryptosystems Based on Integer Factorization
A Uniform Approach to Securing Unix Applications Using SESAME
Integrated Management of Network and Host Based Security Mechanisms
Covert Distributed Computing Using Java Through Web Spoofing
Differential Cryptanalysis of a Block Cipher
On Private-Key Cryptosystems Based on Product Codes
Key Schedules of Iterative Block Ciphers
Low-Cost Secure Server Connection with Limited-Privilege Clients
A Solution to Open Standard of PKI
Comparison of Commitment Schemes Used in Mix-Mediated Anonymous Communication for Preventing Pool-Mode Attacks
Correlation Attacks on Up/Down Cascades
A Stream Cipher Based on Linear Feedback over GF(2^{8})
A Probabilistic Correlation Attack on the Shrinking Generator
Bounds and Constructions for A[3]-code with Multi-senders
Rotation-Symmetric Functions and Fast Hashing
How to Improve the Nonlinearity of Bijective S-Boxes
Object Modeling of Cryptographic Algorithms with UML
Adapting an Electronic Purse for Internet Payments
LITESET: A Light-Weight Secure Electronic Transaction Protocol
Applications of Linearised and Sub-linearised Polynomials to Information Security
Protocol Failures Related to Order of Encryption and Signature: Computation of Discrete Logarithms in RSA Groups
Protection Against EEPROM Modification Attacks
Trends in Quantum Cryptography in Czech Republic
A High Level Language for Conventional Access Control Models
Fast Access Control Decisions from Delegation Certificate Databases
Meta Objects for Access Control: Role-Based Principals
A Dynamically Typed Access Control Model
Efficient Identity-Based Conference Key Distribution Protocols
A Formal Model for Systematic Design of Key Establishment Protocols
Key Establishment Protocols for Secure Mobile Communications: A Selective Survey
Detecting Key-Dependencies
Secret Sharing in Multilevel and Compartmented Groups
On Construction of Cumulative Secret Sharing Schemes
A Comment on the Efficiency of Secret Sharing Scheme over any Finite Abelian Group
A User Identification System Using Signature Written with Mouse
On Zhang's Nonrepudiable Proxy Signature Schemes
Author Index