1. Record Nr. UNISA996466239003316

Titolo	Cryptology and Network Security [[electronic resource]] : 5th International Conference, CANS 2006, Suzhou, China, December 8-10, 2006, Proceedings / / edited by David Pointcheval, Yi Mu, Kefei Chen
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2006
ISBN	3-540-49463-4
Edizione	[1st ed. 2006.]
Descrizione fisica	1 online resource (XIII, 384 p.)
Collana	Security and Cryptology ; ; 4301
Disciplina	005.8
Soggetti	Data encryption (Computer science) Computer security Management information systems Computer science Computers and civilization Computer communication systems Algorithms Cryptology Systems and Data Security Management of Computing and Information Systems Computers and Society Computer Communication Networks Algorithm Analysis and Problem Complexity
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	International conference proceedings.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Encryption -- Concrete Chosen-Ciphertext Secure Encryption from Subgroup Membership Problems -- Efficient Identity-Based Encryption with Tight Security Reduction -- Key Exchange -- A Diffie-Hellman Key Exchange Protocol Without Random Oracles -- Authenticated Group Key Agreement for Multicast -- Authenticated and Communication Efficient Group Key Agreement for Clustered Ad Hoc Networks -- Authentication and Signatures -- Efficient Mutual Data Authentication Using Manually Authenticated Strings -- Achieving Multicast Stream

Authentication Using MDS Codes -- Shorter Verifier-Local Revocation Group Signatures from Bilinear Maps -- Proxy Signatures -- Security Model of Proxy-Multi Signature Schemes -- Efficient ID-Based One-Time Proxy Signature and Its Application in E-Cheque -- Cryptanalysis -- Side Channel Attacks and Countermeasures on Pairing Based Cryptosystems over Binary Fields -- Improved Collision Attack on Reduced Round Camellia -- Stealing Secrets with SSL/TLS and SSH – Kleptographic Attacks -- Implementation -- Bitslice Implementation of AES -- A Fast Algorithm for Determining the Linear Complexity of Periodic Sequences over GF(3) -- Steganalysis and Watermarking -- Steganalysis Based on Differential Statistics -- Watermarking Essential Data Structures for Copyright Protection -- Boolean Functions and Stream Ciphers -- A Note of Perfect Nonlinear Functions -- Chaotic Keystream Generator Using Coupled NDFs with Parameter Perturbing -- Intrusion Detection -- Cooperative Intrusion Detection for Web Applications -- Finding TCP Packet Round-Trip Time for Intrusion Detection: Algorithm and Analysis -- Smart Architecture for High-Speed Intrusion Detection and Prevention Systems -- A Multi-agent Cooperative Model and System for Integrated Security Monitoring -- Disponibility and Reliability -- Detecting DDoS Attacks Based on Multi-stream Fused HMM in Source-End Network -- An Immune-Based Model for Service Survivability -- X2BT Trusted Reputation System: A Robust Mechanism for P2P Networks.