1. Record Nr. UNINA9910483850803321

Titolo	Cryptology and network security : 6th international conference, CANS 2007, Singapore, December 8-10, 2007 : proceedings / / Feng Bao [and three others] (editors)
Pubbl/distr/stampa	Berlin, Germany ; ; New York, New York : , : Springer, , [2007] ©2007
ISBN	3-540-76969-2
Edizione	[1st ed. 2007.]
Descrizione fisica	1 online resource (XII, 286 p.)
Collana	Security and Cryptology ; ; 4856
Classificazione	DAT 461f
Disciplina	005.8
Soggetti	Computer networks - Security measures Cryptography
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Signatures -- Mutative Identity-Based Signatures or Dynamic Credentials Without Random Oracles -- A Generic Construction for Universally-Convertible Undeniable Signatures -- Fast Digital Signature Algorithm Based on Subgraph Isomorphism -- Efficient ID-Based Digital Signatures with Message Recovery -- Network Security -- Achieving Mobility and Anonymity in IP-Based Networks -- Perfectly Secure Message Transmission in Directed Networks Tolerating Threshold and Non Threshold Adversary -- Forward-Secure Key Evolution in Wireless Sensor Networks -- A Secure Location Service for Ad Hoc Position-Based Routing Using Self-signed Locations -- An Intelligent Network-Warning Model with Strong Survivability -- Running on Karma – P2P Reputation and Currency Systems -- Secure Keyword Search and Private Information Retrieval -- Generic Combination of Public Key Encryption with Keyword Search and Public Key Encryption -- Extended Private Information Retrieval and Its Application in Biometrics Authentications -- Public Key Encryption -- Strongly Secure Certificateless Public Key Encryption Without Pairing -- Intrusion Detection -- Modeling Protocol Based Packet Header Anomaly Detector for Network and Host Intrusion Detection Systems -- Email Security -- How to Secure Your Email Address Book and Beyond -- Denial of Service Attacks -- Toward Non-parallelizable Client Puzzles --

	Authentication -- Anonymity 2.0 – X.509 Extensions Supporting Privacy-Friendly Authentication.
Sommario/riassunto	This book constitutes the refereed proceedings of the 6th International Conference on Cryptology and Network Security, CANS 2007, held in Singapore, in December 2007. The 17 revised full papers presented were carefully reviewed and selected from 68 submissions. The papers are organized in topical sections on signatures, network security, secure keyword search and private information retrieval, public key encryption, intrusion detection, email security, denial of service attacks, and authentication.