

1. Record Nr.	UNISA996466369503316
Titolo	Applied Cryptography and Network Security [[electronic resource] ] : 5th International Conference, ACNS 2007, Zhuhai, China, June 5-8, 2007, Proceedings // edited by Jonathan Katz, Moti Yung
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2007
ISBN	1-280-94923-6 9786610949236 3-540-72738-8
Edizione	[1st ed. 2007.]
Descrizione fisica	1 online resource (508 p.)
Collana	Security and Cryptology ; ; 4521
Disciplina	005.8
Soggetti	Computer networks Cryptography Data encryption (Computer science) Data protection Application software Computers and civilization Electronic data processing—Management Computer Communication Networks Cryptology Data and Information Security Computer and Information Systems Applications Computers and Society IT Operations
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Signature Schemes I -- Generic Transformation to Strongly Unforgeable Signatures -- Efficient Generic On-Line/Off-Line Signatures Without Key Exposure -- Merkle Signatures with Virtually Unlimited Signature Capacity -- Computer and Network Security -- Midpoints Versus Endpoints: From Protocols to Firewalls -- An Adversary Aware and Intrusion Detection Aware Attack Model Ranking Scheme -- Analyzing

an Electronic Cash Protocol Using Applied Pi Calculus -- Cryptanalysis -- Cryptanalysis of the TRMC-4 Public Key Cryptosystem -- Estimating the Prime-Factors of an RSA Modulus and an Extension of the Wiener Attack -- A Timing Attack on Blakley's Modular Multiplication Algorithm, and Applications to DSA -- Protecting AES Software Implementations on 32-Bit Processors Against Power Analysis -- Group-Oriented Security -- Constant-Round Authenticated Group Key Exchange with Logarithmic Computation Complexity -- Preventing Collusion Attacks on the One-Way Function Tree (OFT) Scheme -- Bayesian Methods for Practical Traitor Tracing -- Cryptographic Protocols -- A New Protocol for Conditional Disclosure of Secrets and Its Applications -- An Unconditionally Secure Protocol for Multi-Party Set Intersection -- Privacy-Preserving Set Union -- Anonymous Authentication -- Universal Accumulators with Efficient Nonmembership Proofs -- Unlinkable Secret Handshakes and Key-Private Group Key Management Schemes -- Identity-Based Cryptography -- Identity-Based Proxy Re-encryption -- A More Natural Way to Construct Identity-Based Identification Schemes -- Tweaking TBE/IBE to PKE Transforms with Chameleon Hash Functions -- Certified E-Mail Protocol in the ID-Based Setting -- Security in Wireless, Ad-Hoc, and Peer-to-Peer Networks -- Efficient Content Authentication in Peer-to-Peer Networks -- An Identity-Based Signcryption Scheme for Multi-domain Ad Hoc Networks -- Efficient Self-healing Key Distribution with Revocation for Wireless Sensor Networks Using One Way Key Chains -- BAP: Broadcast Authentication Using Cryptographic Puzzles -- Efficient Implementation -- Compressed XTR -- Sliding Window Method for NTRU -- Signature Schemes II -- Efficient Certificateless Signature Schemes -- Security Mediated Certificateless Signatures -- Gradually Convertible Undeniable Signatures.

---