1.

Record Nr.	UNISA996466115003316
Titolo	Theory of Cryptography [[electronic resource]] : Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March 4-7, 2006, Proceedings / / edited by Shai Halevi, Tal Rabin
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2006
ISBN	3-540-32732-0
Edizione	[1st ed. 2006.]
Descrizione fisica	1 online resource (XII, 620 p.)
Collana	Security and Cryptology ; ; 3876
Disciplina	005.8
Soggetti	Data encryption (Computer science) Algorithms Computer science—Mathematics Operating systems (Computers) Management information systems Computer science Computers and civilization Cryptology Algorithm Analysis and Problem Complexity Discrete Mathematics in Computer Science Operating Systems Management of Computing and Information Systems Computers and Society
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	Zero-Knowledge -- Concurrent Zero Knowledge Without Complexity Assumptions -- Interactive Zero-Knowledge with Restricted Random Oracles -- Non-interactive Zero-Knowledge from Homomorphic Encryption -- Primitives -- Ring Signatures: Stronger Definitions, and Constructions Without Random Oracles -- Efficient Blind and Partially Blind Signatures Without Random Oracles -- Key Exchange Using Passwords and Long Keys -- Mercurial Commitments: Minimal Assumptions and Efficient Constructions -- Assumptions and Models

-- Efficient Collision-Resistant Hashing from Worst-Case Assumptions on Cyclic Lattices -- On Error Correction in the Exponent -- On the Relation Between the Ideal Cipher and the Random Oracle Models -- The Bounded-Retrieval Model -- Intrusion-Resilience Via the Bounded-Storage Model -- Perfectly Secure Password Protocols in the Bounded Retrieval Model -- Privacy -- Polylogarithmic Private Approximations and Efficient Matching -- Calibrating Noise to Sensitivity in Private Data Analysis -- Secret Sharing and Multi-party Computation (I) -- Unconditionally Secure Constant-Rounds Multi-party Computation for Equality, Comparison, Bits and Exponentiation -- Efficient Multi-party Computation with Dispute Control -- Round-Optimal and Efficient Verifiable Secret Sharing -- Universally-Composible Security -- Generalized Environmental Security from Number Theoretic Assumptions -- Games and the Impossibility of Realizable Ideal Functionality -- Universally Composable Symbolic Analysis of Mutual Authentication and Key-Exchange Protocols -- Resource Fairness and Composability of Cryptographic Protocols -- One-Way Functions and Friends -- Finding Pessiland -- Pseudorandom Generators from One-Way Functions: A Simple Construction for Any Hardness -- On the Complexity of Parallel Hardness Amplification for One-Way Functions -- Secret Sharing and Multi-party Computation (II) -- On Matroids and Non-ideal Secret Sharing -- Secure Computation with Partial Message Loss -- Communication Efficient Secure Linear Algebra -- Threshold and Proactive Pseudo-Random Permutations -- Pseudo-Random Functions and Encryption -- PRF Domain Extension Using DAGs -- Chosen-Ciphertext Security from Tag-Based Encryption -- Separating Sources for Encryption and Secret Sharing.