1. Record Nr. UNINA9910482979803321

Titolo	Theory of Cryptography : Fifth Theory of Cryptography Conference, TCC 2008, New York, USA, March 19-21, 2008, Proceedings / / edited by Ran Canetti
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2008
ISBN	3-540-78524-8
Edizione	[1st ed. 2008.]
Descrizione fisica	1 online resource (XII, 645 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 4948
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Algorithms Computer science - Mathematics Discrete mathematics Data protection Electronic data processing - Management Computers and civilization Cryptology Discrete Mathematics in Computer Science Data and Information Security IT Operations Computers and Society
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Technical Session 1 -- Incrementally Verifiable Computation or Proofs of Knowledge Imply Time/Space Efficiency -- On Seed-Incompressible Functions -- Technical Session 2 -- Asymptotically Efficient Lattice-Based Digital Signatures -- Basing Weak Public-Key Cryptography on Strong One-Way Functions -- Technical Session 3 -- Which Languages Have 4-Round Zero-Knowledge Proofs? -- How to Achieve Perfect Simulation and A Complete Problem for Non-interactive Perfect Zero-Knowledge -- General Properties of Quantum Zero-Knowledge Proofs

-- Technical Session 4 -- The Layered Games Framework for Specifications and Analysis of Security Protocols -- Universally Composable Multi-party Computation with an Unreliable Common Reference String -- Efficient Protocols for Set Intersection and Pattern Matching with Security Against Malicious and Covert Adversaries -- Fast Private Norm Estimation and Heavy Hitters -- Technical Session 5 -- Matroids Can Be Far from Ideal Secret Sharing -- Perfectly-Secure MPC with Linear Communication Complexity -- MPC vs. SFE: Perfect Security in a Unified Corruption Model -- Invited Talk -- Bridging Game Theory and Cryptography: Recent Results and Future Directions -- Technical Session 6 -- Verifiably Secure Devices -- Lower Bounds on Implementing Robust and Resilient Mediators -- Cryptography and Game Theory: Designing Protocols for Exchanging Information -- Technical Session 7 -- Equivocal Blind Signatures and Adaptive UC-Security -- P-signatures and Noninteractive Anonymous Credentials -- Technical Session 8 -- Multi-property Preserving Combiners for Hash Functions -- OT-Combiners via Secure Computation -- Semi-honest to Malicious Oblivious Transfer—The Black-Box Way -- Black-Box Construction of a Non-malleable Encryption Scheme from Any Semantically Secure One -- Technical Session 9.-A Linear Lower Bound on the Communication Complexity of Single-Server Private Information Retrieval -- Randomness Extraction Via ?-Biased Masking in the Presence of a Quantum Attacker -- Technical Session 10 -- An Equivalence Between Zero Knowledge and Commitments -- Interactive and Noninteractive Zero Knowledge are Equivalent in the Help Model -- Technical Session 11 -- The Round-Complexity of Black-Box Zero-Knowledge: A Combinatorial Characterization -- On Constant-Round Concurrent Zero-Knowledge -- Technical Session 12 -- Concurrent Non-malleable Commitments from Any One-Way Function -- Faster and Shorter Password-Authenticated Key Exchange -- Technical Session 13 -- Saving Private Randomness in One-Way Functions and Pseudorandom Generators -- Degradation and Amplification of Computational Hardness.

Sommario/riassunto

This book constitutes the refereed proceedings of the Fifth Theory of Cryptography Conference, TCC 2008, held in New York, USA, March 19-21, 2008. The 33 revised full papers presented were carefully reviewed and selected from 81 submissions. The papers are organized in 16 sessions dealing with the paradigms, approaches and techniques used to conceptualize, define and provide solutions to natural cryptographic problems.