1. Record Nr. UNISA996465951303316

Titolo	Theory of Cryptography [[electronic resource]] : Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10-12. 2005, Proceedings / / edited by Joe Kilian
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2005
ISBN	3-540-30576-9
Edizione	[1st ed. 2005.]
Descrizione fisica	1 online resource (XII, 628 p.)
Collana	Security and Cryptology ; ; 3378
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	Hardness Amplification and Error Correction -- Optimal Error Correction Against Computationally Bounded Noise -- Hardness Amplification of Weakly Verifiable Puzzles -- On Hardness Amplification of One-Way Functions -- Graphs and Groups -- Cryptography in Subgroups of -- Efficiently Constructible Huge Graphs That Preserve First Order Properties of Random Graphs -- Simulation and Secure Computation -- Comparing Two Notions of Simulatability -- Relaxing Environmental Security: Monitored Functionalities and

Client-Server Computation -- Handling Expected Polynomial-Time Strategies in Simulation-Based Security Proofs -- Security of Encryption -- Adaptively-Secure, Non-interactive Public-Key Encryption -- Adaptive Security of Symbolic Encryption -- Chosen-Ciphertext Security of Multiple Encryption -- Steganography and Zero Knowledge -- Public-Key Steganography with Active Attacks -- Upper and Lower Bounds on Black-Box Steganography -- Fair-Zero Knowledge -- Secure Computation I -- How to Securely Outsource Cryptographic Computations -- Secure Computation of the Mean and Related Statistics -- Keyword Search and Oblivious Pseudorandom Functions -- Secure Computation II -- Evaluating 2-DNF Formulas on Ciphertexts -- Share Conversion, Pseudorandom Secret-Sharing and Applications to Secure Computation -- Toward Privacy in Public Databases -- Quantum Cryptography and Universal Composability -- The Universal Composable Security of Quantum Key Distribution -- Universally Composable Privacy Amplification Against Quantum Adversaries -- A Universally Composable Secure Channel Based on the KEM-DEM Framework -- Cryptographic Primitives and Security -- Sufficient Conditions for Collision-Resistant Hashing -- The Relationship Between Password-Authenticated Key Exchange and Other Cryptographic Primitives -- On the Relationships Between Notions of Simulation-Based Security -- Encryption and Signatures -- A New Cramer-Shoup Like Methodology for Group Based Provably Secure Encryption Schemes -- Further Simplifications in Proactive RSA Signatures -- Proof of Plaintext Knowledge for the Ajtai-Dwork Cryptosystem -- Information Theoretic Cryptography -- Entropic Security and the Encryption of High Entropy Messages -- Error Correction in the Bounded Storage Model -- Characterizing Ideal Weighted Threshold Secret Sharing.

Sommario/riassunto

TCC 2005, the 2nd Annual Theory of Cryptography Conference, was held in Cambridge,Massachusetts,onFebruary10–12,2005. Theconferencereceived84 submissions, ofwhichtheprogramcommitteeselected32forpresentation.These proceedings contain the revised versions of the submissions that were presented at the conference. These revisions have not been checked for correctness, and the authors bear full responsibility for the contents of their papers. The conference program also included a panel discussion on the future of theoretical cryptography and its relationship to the real world (whatever that is). It also included the traditional “rump session,” featuring short, informal talks on late-breaking research news. Much as hatters of old faced mercury-induced neurological damage as an occupational hazard, computer scientists will on rare occasion be a? icted with egocentrism, probably due to prolonged CRT exposure. Thus, you must view withpityandnotcontemptmyunalloyedelationathavingmynameonthefront cover of this LNCS volume, and my deep-seated conviction that I fully deserve the fame and riches that will surely come of it. However, having in recent years switched over to an LCD monitor, I would like to acknowledge some of the many who contributed to this conference. First thanks are due to the many researchers from all over the world who submitted their work to this conference. Lacking shrimp and chocolate-covered strawberries, TCC has to work hard to be a good conference. As a community, I think we have.