1. Record Nr. UNINA9910767521803321

Titolo	Theory of Cryptography : First Theory of Cryptography Conference, TCC 2004, Cambridge, MA, USA, February 19-21, 2004, Proceedings / / edited by Moni Naor
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2004
ISBN	1-280-30688-2 9786610306886 3-540-24638-X
Edizione	[1st ed. 2004.]
Descrizione fisica	1 online resource (XII, 532 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 2951
Disciplina	005.82
Soggetti	Data encryption (Computer science) Operating systems (Computers) Algorithms Computers and civilization Management information systems Computer science Cryptology Operating Systems Algorithm Analysis and Problem Complexity Computers and Society Management of Computing and Information Systems
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 at the end of each chapters and index.
Nota di contenuto	Notions of Reducibility between Cryptographic Primitives -- Indifferentiability, Impossibility Results on Reductions, and Applications to the Random Oracle Methodology -- On the Random-Oracle Methodology as Applied to Length-Restricted Signature Schemes -- Universally Composable Commitments Using Random Oracles -- Transformation of Digital Signature Schemes into Designated Confirmer Signature Schemes -- List-Decoding of Linear Functions and Analysis

of a Two-Round Zero-Knowledge Argument -- On the Possibility of One-Message Weak Zero-Knowledge -- Soundness of Formal Encryption in the Presence of Active Adversaries -- Rerandomizable and Replayable Adaptive Chosen Ciphertext Attack Secure Cryptosystems -- Alternatives to Non-malleability: Definitions, Constructions, and Applications -- A Note on Constant-Round Zero-Knowledge Proofs for NP -- Lower Bounds for Concurrent Self Composition -- Secret-Key Zero-Knowlegde and Non-interactive Verifiable Exponentiation -- A Quantitative Approach to Reductions in Secure Computation -- Algorithmic Tamper-Proof (ATP) Security: Theoretical Foundations for Security against Hardware Tampering -- Physically Observable Cryptography -- Efficient and Universally Composable Committed Oblivious Transfer and Applications -- A Universally Composable Mix-Net -- A General Composition Theorem for Secure Reactive Systems -- Unfair Noisy Channels and Oblivious Transfer -- Computational Collapse of Quantum State with Application to Oblivious Transfer -- Implementing Oblivious Transfer Using Collection of Dense Trapdoor Permutations -- Composition of Random Systems: When Two Weak Make One Strong -- Simpler Session-Key Generation from Short Random Passwords -- Constant-Round Oblivious Transfer in the Bounded Storage Model -- Hierarchical Threshold Secret Sharing -- On Compressing Encrypted Data without the Encryption Key -- On the Notion of Pseudo-Free Groups.

Sommario/riassunto

I thank Sha? Goldwasser for chairing this conference and making all the necessaryarrangementsatMIT.Sha? inturnistremendouslygratefultoJoanne Talbot who coordinated the conference facilities, hotels, Web page, budgets, and the conference chair relentlessly and without a single complaint. Thank you Joanne. I thank Mihir Bellare for chairing the Steering Committee of TCC and the members of the committee (see the list in the pages that follow) for helping out with many issues concerning the conference, including the proceedings and the TCC Web-site. Finally a big thanks is due to Oded Goldreich who initiated this endeavor and pushed hard for it. Rehovot, Israel Moni Naor December 2003 Program Chair TCC 2004 VII External Referees Masayuki Abe Daniel Gottesman Jesper Buus Nielsen Luis van Ahn Jens Groth Adriana Palacio Michael Backes Shai Halevi Erez Petrank Boaz Barak Danny Harnik Benny Pinkas Amos Beimel Alejandro Hevia Tal Rabin Mihir Bellare Thomas Jakobsen Oded Regev Alexandra Boldyreva Markus Jakobsson Amit Sahai Harry Buhrman Ari Juels Jean-Pierre Seifert Christian Cachin Jonathan Katz Adam Smith Jan Camenisch Hugo Krawczyk Martijn Stam Claude Cr´ epeau Eyal Kushilevitz Yael Tauman Kalai Anand Desai Yehuda Lindell Michael Waidner Yan Zong Ding Anna Lysyanskaya John Watrous Yevgeniy Dodis Tal Malkin Douglas Wikstr¨ om Marc Fischlin David Meyer Bogdan Warinschi Juan Garay Ashwin Nayak Stephanie Wehner Rosario Gennaro Gregory Neven Ke Yang TCC Steering Committee Mihir Bellare (Chair) UCSD, USA ? Ivan Damg? ard Arhus University, Denmark Oded Goldreich Weizmann Institute, Israel and Radcli?e Institute, USA Sha? Goldwasser MIT, USA and Weizmann Institute, Israel