

| | |
|-------------------------|--|
| 1. Record Nr. | UNISA996465886203316 |
| Titolo | Theory of Cryptography [[electronic resource]] : Sixth Theory of Cryptography Conference, TCC 2009, San Francisco, CA, USA, March 15-17, 2009, Proceedings / / edited by Omer Reingold |
| Pubbl/distr/stampa | Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2009 |
| ISBN | 3-642-00457-1 |
| Edizione | [1st ed. 2009.] |
| Descrizione fisica | 1 online resource (XI, 615 p.) |
| Collana | Security and Cryptology ; ; 5444 |
| Classificazione | DAT 465f SS 4800 |
| Disciplina | 005.82 |
| Soggetti | Data encryption (Computer science) Algorithms Computer science—Mathematics Computer security Management information systems Computer science Computers and civilization Cryptology Algorithm Analysis and Problem Complexity Discrete Mathematics in Computer Science Systems and Data Security Management of Computing and Information Systems Computers and Society Kongress. San Francisco (Calif., 2009) |
| 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 | An Optimally Fair Coin Toss -- Complete Fairness in Multi-party Computation without an Honest Majority -- Fairness with an Honest Minority and a Rational Majority -- Purely Rational Secret Sharing (Extended Abstract) -- Some Recent Progress in Lattice-Based Cryptography -- Non-malleable Obfuscation -- Simulation-Based |

Concurrent Non-malleable Commitments and Decommitments --
Proofs of Retrievability via Hardness Amplification -- Security
Amplification for Interactive Cryptographic Primitives -- Composability
and On-Line Deniability of Authentication -- Authenticated Adversarial
Routing -- Adaptive Zero-Knowledge Proofs and Adaptively Secure
Oblivious Transfer -- On the (Im)Possibility of Key Dependent
Encryption -- On the (Im)Possibility of Arthur-Merlin Witness Hiding
Protocols -- Secure Computability of Functions in the IT Setting with
Dishonest Majority and Applications to Long-Term Security --
Complexity of Multi-party Computation Problems: The Case of 2-Party
Symmetric Secure Function Evaluation -- Realistic Failures in Secure
Multi-party Computation -- Secure Arithmetic Computation with No
Honest Majority -- Universally Composable Multiparty Computation
with Partially Isolated Parties -- Oblivious Transfer from Weak Noisy
Channels -- Composing Quantum Protocols in a Classical Environment
-- LEGO for Two-Party Secure Computation -- Simple, Black-Box
Constructions of Adaptively Secure Protocols -- Black-Box
Constructions of Two-Party Protocols from One-Way Functions --
Chosen-Ciphertext Security via Correlated Products -- Hierarchical
Identity Based Encryption with Polynomially Many Levels -- Predicate
Privacy in Encryption Systems -- Simultaneous Hardcore Bits and
Cryptography against Memory Attacks -- The Differential Privacy
Frontier (Extended Abstract) -- How Efficient Can Memory Checking Be?
-- Goldreich's One-Way Function Candidate and Myopic Backtracking
Algorithms -- Secret Sharing and Non-Shannon Information
Inequalities -- Weak Verifiable Random Functions -- Efficient Oblivious
Pseudorandom Function with Applications to Adaptive OT and Secure
Computation of Set Intersection -- Towards a Theory of Extractable
Functions.

Sommario/riassunto

This book constitutes the refereed proceedings of the Sixth Theory of Cryptography Conference, TCC 2009, held in San Francisco, CA, USA, March 15-17, 2009. The 33 revised full papers presented together with two invited talks were carefully reviewed and selected from 109 submissions. The papers are organized in 10 sessions dealing with the paradigms, approaches and techniques used to conceptualize, define and provide solutions to natural cryptographic problems.
