

- |    |                         |                                                                                   |
|----|-------------------------|-----------------------------------------------------------------------------------|
| 1. | Record Nr.              | UNISALENTO991003304299707536                                                      |
|    | Autore                  | Tartuferi, Salvatore                                                              |
|    | Titolo                  | Diario maceratese : 1794-1817 / Tartuferi Salvatore ; a cura di Marcello Sgattoni |
|    | Pubbl/distr/stampa      | Macerata : Litotipo Sangiuseppe, 1979                                             |
|    | Descrizione fisica      | 106 p. ; 24 cm                                                                    |
|    | Altri autori (Persone)  | Sgattoni, Marcello                                                                |
|    | Disciplina              | 945.673                                                                           |
|    | Soggetti                | Macerata Storia 1794-1817                                                         |
|    | Lingua di pubblicazione | Italiano                                                                          |
|    | Formato                 | Materiale a stampa                                                                |
|    | Livello bibliografico   | Monografia                                                                        |
- 
- |    |                        |                                                                                                                                                                                                                                                                                                                     |
|----|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2. | Record Nr.             | UNINA9910484779603321                                                                                                                                                                                                                                                                                               |
|    | Titolo                 | Theory of Cryptography : 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, , 2946-1863 ; ; 3876                                                                                                                                                                                                                                                                       |
|    | Altri autori (Persone) | HaleviShai<br>RabinTal                                                                                                                                                                                                                                                                                              |
|    | Disciplina             | 005.8                                                                                                                                                                                                                                                                                                               |
|    | Soggetti               | Cryptography<br>Data encryption (Computer science)<br>Algorithms<br>Computer science - Mathematics<br>Discrete mathematics<br>Operating systems (Computers)<br>Electronic data processing - Management<br>Computers and civilization<br>Cryptology<br>Discrete Mathematics in Computer Science<br>Operating 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 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-Composable 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. |
| Sommario/riassunto      | This book constitutes the refereed proceedings of the Third Theory of Cryptography Conference, TCC 2006, held in March 2006. The 31 revised full papers presented were carefully reviewed and selected from 91 submissions. The papers are organized in topical sections on zero-knowledge, primitives, assumptions and models, the bounded-retrieval model, privacy, secret sharing and multi-party computation, universally-composable security, one-way functions and friends, and pseudo-random functions and encryption.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |