

| | |
|-------------------------|--|
| 1. Record Nr. | UNISA996466092503316 |
| Titolo | Financial Cryptography and Data Security [[electronic resource]] : 10th International Conference, FC 2006 Anguilla, British West Indies, February 27 - March 2, 2006, Revised Selected Papers // edited by Giovanni Di Crescenzo, Avi Rubin |
| Pubbl/distr/stampa | Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2006 |
| ISBN | 3-540-46256-2 |
| Edizione | [1st ed. 2006.] |
| Descrizione fisica | 1 online resource (XI, 327 p.) |
| Collana | Security and Cryptology ; ; 4107 |
| Disciplina | 005.82 |
| Soggetti | Data encryption (Computer science) Operating systems (Computers) Management information systems Computer science Computers and civilization Computer communication systems Algorithms Cryptology Operating Systems Management of Computing and Information Systems Computers and Society Computer Communication Networks Algorithm Analysis and Problem Complexity |
| 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 | Authentication and Fraud Detection -- Phoolproof Phishing Prevention -- A Protocol for Secure Public Instant Messaging -- Using Automated Banking Certificates to Detect Unauthorised Financial Transactions -- Privacy -- Privacy in Encrypted Content Distribution Using Private Broadcast Encryption -- A Private Stable Matching Algorithm -- Private Policy Negotiation -- Reputation and Mix-Nets -- Uncheatable Reputation for Distributed Computation Markets -- An Efficient Publicly |

Verifiable Mix-Net for Long Inputs -- Auditable Privacy: On Tamper-Evident Mix Networks -- Short Papers -- A Practical Implementation of Secure Auctions Based on Multiparty Integer Computation -- Defeating Malicious Servers in a Blind Signatures Based Voting System -- Pairing Based Threshold Cryptography Improving on Libert-Quisquater and Baek-Zheng -- Credit Transfer for Market-Based Infrastructure -- A Note on Chosen-Basis Decisional Diffie-Hellman Assumptions -- Cryptanalysis of a Partially Blind Signature Scheme or How to Make \$100 Bills with \$1 and \$2 Ones -- Conditional Financial Cryptography -- A Generic Construction for Token-Controlled Public Key Encryption -- Timed-Release and Key-Insulated Public Key Encryption -- Conditional Encrypted Mapping and Comparing Encrypted Numbers -- Revisiting Oblivious Signature-Based Envelopes -- Payment Systems -- Provably Secure Electronic Cash Based on Blind Multisignature Schemes -- Efficient Provably Secure Restrictive Partially Blind Signatures from Bilinear Pairings -- Privacy-Protecting Coupon System Revisited -- Efficient Protocols -- Efficient Broadcast Encryption Scheme with Log-Key Storage -- Efficient Correlated Action Selection -- Efficient Cryptographic Protocols Realizing E-Markets with Price Discrimination.
