1. Record Nr.   UNISA996465407103316

   Titolo   Advances in Cryptology - CRYPTO 2000 [[electronic resource]] : 20th
                             Annual International Cryptology Conference, Santa Barbara, California,
                             USA, August 20-24, 2000. Proceedings / / edited by Mihir Bellare

   Pubbl/distr/stampa   Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer,
                             , 2000

   ISBN   3-540-44598-6

   Edizione   [1st ed. 2000.]

   Descrizione fisica   1 online resource (XI, 543 p.)

   Collana   Lecture Notes in Computer Science, , 0302-9743 ; ; 1880

   Disciplina   005.8/2

   Soggetti   Computer communication systems
                             Data encryption (Computer science)
                             Algorithms
                             Management information systems
                             Computer science
                             Computer mathematics
                             Computer Communication Networks
                             Cryptology
                             Algorithm Analysis and Problem Complexity
                             Management of Computing and Information Systems
                             Computational Mathematics and Numerical Analysis

   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   XTR and NTRU -- The XTR Public Key System -- A Chosen-Ciphertext
                             Attack against NTRU -- Privacy for Databases -- Privacy Preserving
                             Data Mining -- Reducing the Servers Computation in Private
                             Information Retrieval: PIR with Preprocessing -- Secure Distributed
                             Computation and Applications -- Parallel Reducibility for Information-
                             Theoretically Secure Computation -- Optimistic Fair Secure
                             Computation -- A Cryptographic Solution to a Game Theoretic Problem
                             -- Algebraic Cryptosystems -- Differential Fault Attacks on Elliptic
                             Curve Cryptosystems -- Quantum Public-Key Cryptosystems -- New
                             Public-Key Cryptosystem Using Braid Groups -- Message
                             Authentication -- Key Recovery and Forgery Attacks on the MacDES