1. Record Nr.   UNINA9910637739203321

   Titolo   Theory of Cryptography : 20th International Conference, TCC 2022, Chicago, IL, USA, November 7–10, 2022, Proceedings, Part II / / edited by Eike Kiltz, Vinod Vaikuntanathan

   Pubbl/distr/stampa Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2022

   ISBN   3-031-22365-9

   Edizione   [1st ed. 2022.]

   Descrizione fisica 1 online resource (813 pages)

   Collana   Lecture Notes in Computer Science, , 1611-3349 ; ; 13748

   Disciplina   652.8
                     005.82

   Soggetti   Cryptography
                     Data encryption (Computer science)
                     Computer networks
                     Data structures (Computer science)
                     Information theory
                     Computer engineering
                     Data protection
                     Cryptology
                     Computer Communication Networks
                     Data Structures and Information Theory
                     Computer Engineering and Networks
                     Security Services
                     Data and Information Security

   Lingua di pubblicazione Inglese

   Formato   Materiale a stampa

   Livello bibliografico Monografia

   Nota di bibliografia Includes bibliographical references and index.

   Nota di contenuto Encryption -- Multi-party computation -- Protocols: key agreement and commitments -- Theory: sampling and friends -- Lattices -- Anonymity, Verfiability and robustness.

   Sommario/riassunto The three-volume set LNCS 13747, LNCS 13748 and LNCS 13749 constitutes the refereed proceedings of the 20th International Conference on Theory of Cryptography, TCC 2022, held in Chicago, IL, USA, in November 2022. The total of 60 full papers presented in this three-volume set was carefully reviewed and selected from 139

submissions. They cover topics on post-quantum cryptography; interactive proofs; quantum cryptography; secret-sharing and applications; succinct proofs; identity-based encryption and functional encryption; attribute-based encryption and functional encryption; encryption; multi-party computation; protocols: key agreement and commitments; theory: sampling and friends; lattices; anonymity, verfiability and robustness; ORAM, OT and PIR; and theory.