1. **Record Nr.**   UNINA9910616370103321

   Titolo   Advances in Cryptology – CRYPTO 2022 : 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15–18, 2022, Proceedings, Part II / / edited by Yevgeniy Dodis, Thomas Shrimpton

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

   ISBN   9783031159794
                          3031159799

   Edizione   [1st ed. 2022.]

   Descrizione fisica   1 online resource (830 pages)

   Collana   Lecture Notes in Computer Science, , 1611-3349 ; ; 13508

   Disciplina   652.8
                          005.82

   Soggetti   Cryptography
                          Data encryption (Computer science)
                          Cryptology

   Lingua di pubblicazione   Inglese

   Formato   Materiale a stampa

   Livello bibliografico   Monografia

   Nota di bibliografia   Includes bibliographical references and index.

   Nota di contenuto   Secure Messaging -- Lattice-Based Zero Knowledge -- Quantum Cryptography II -- Lattice-Based Signatures -- Blockchain -- Best Paper Awards -- Coding Theory -- Public Key Cryptography -- Signatures.

   Sommario/riassunto   This book constitutes the refereed proceedings of the 42nd Annual International Cryptology Conference, CRYPTO 2022, which was held in Santa Barbara, CA, USA, in August 2022. The total of 100 papers included in the 4-volume proceedings LNCS 13507, 13508, 13509, 13510, was reviewed and selected from 455 submissions. The papers were organized in the following topical sections: Cryptanalysis; randomness; quantum cryptography; advanced encryption systems; secure messaging; lattice-based zero knowledge; lattice-based signatures; blockchain; coding theory; public key cryptography; signatures, idealized models; lower bounds; secure hash functions; post-quantum cryptography; symmetric cryptanalysis; secret sharing and secure multiparty computation; unique topics; symmetric key theory; zero knowledge; and threshold signatures. .