1.	Record Nr.	UNINA9910616373503321
	Titolo	Advances in Cryptology – CRYPTO 2022 : 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15–18, 2022, Proceedings, Part IV / / edited by Yevgeniy Dodis, Thomas Shrimpton
	Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2022
	ISBN	9783031159855 3031159853
	Edizione	[1st ed. 2022.]
	Descrizione fisica	1 online resource (590 pages)
	Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 13510
	Disciplina	929 005.82
	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	Secret Sharing and Secure Multiparty Computation -- Unique Topics -- Symmetric Key Theory -- Zero Knowledge -- Secure Multiparty Computation III -- Threshold Signatures.
	Sommario/riassunto	The 4-volume sets LNCS 13507, 13508, 13509, 13510 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 proceedings 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. .