

1. Record Nr.	UNINA9910647383603321
Titolo	Advances in cryptology - ASIACRYPT 2022 : 28th international conference on the theory and application of cryptology and information security, Taipei, Taiwan, December 5-9, 2022, proceedings, part I // edited by Shweta Agrawal and Dongdai Lin
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2023] ©2023
ISBN	3-031-22963-0
Edizione	[1st ed. 2022.]
Descrizione fisica	1 online resource (846 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 13791
Disciplina	005.8
Soggetti	Computer security Data encryption (Computer science)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Award Papers -- Functional and Witness Encryption -- Symmetric Key Cryptanalysis -- Multiparty Computation -- Real World Protocols -- Blockchains and Cryptocurrencies. .
Sommario/riassunto	The four-volume proceedings LNCS 13791, 13792, 13793, and 13794 constitute the proceedings of the 28th International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2022, held in Taipei, Taiwan, during December 5-9, 2022. The total of 98 full papers presented in these proceedings was carefully reviewed and selected from 364 submissions. The papers were organized in topical sections as follows: Part I: Award papers; functional and witness encryption; symmetric key cryptanalysis; multiparty computation; real world protocols; and blockchains and cryptocurrencies. Part II: Isogeny based cryptography; homomorphic encryption; NIZK and SNARKs; non interactive zero knowledge; and symmetric cryptography. Part III: Practical cryptography; advanced encryption; zero knowledge; quantum algorithms; lattice cryptoanalysis. Part IV: Signatures; commitments; theory; cryptoanalysis; and quantum cryptography.