1. Record Nr. UNINA9910647396603321

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 IV / / edited by Shweta Agrawal, Dongdai Lin
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2022
ISBN	3-031-22972-X
Edizione	[1st ed. 2022.]
Descrizione fisica	1 online resource (667 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 13794
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Computer networks Coding theory Information theory Computer engineering Data protection Computer networks - Security measures Cryptology Computer Communication Networks Coding and Information Theory Computer Engineering and Networks Security Services Mobile and Network Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Signatures -- Commitments -- Theory -- Cryptoanalysis -- Quantum Cryptography.
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.