1. Record Nr. UNINA9910647383903321

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 II / / edited by Shweta Agrawal, Dongdai Lin
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2022
ISBN	9783031229664 3031229665
Edizione	[1st ed. 2022.]
Descrizione fisica	1 online resource (720 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 13792
Disciplina	016.391 005.8
Soggetti	Cryptography Data encryption (Computer science) Computer networks Coding theory Information theory Application software User interfaces (Computer systems) Human-computer interaction Data protection Cryptology Computer Communication Networks Coding and Information Theory Computer and Information Systems Applications User Interfaces and Human Computer Interaction Security Services
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Isogeny Based Cryptography -- Homomorphic Encryption -- NIZK and SNARKs -- Non Interactive Zero Knowledge -- and Symmetric 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.