1. Record Nr. UNISA996574258203316

Titolo	Advances in Cryptology - ASIACRYPT 2023 : 29th International Conference on the Theory and Application of Cryptology and Information Security, Guangzhou, China, December 4-8, 2023, Proceedings, Part VIII / / edited by Jian Guo and Ron Steinfeld
Pubbl/distr/stampa	Singapore : , : Springer, , [2023] ©2023
ISBN	9789819987429
Edizione	[First edition.]
Descrizione fisica	1 online resource (342 pages)
Collana	Lecture Notes in Computer Science Series ; ; Volume 14445
Disciplina	929.605
Soggetti	Computers
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Quantum cryptography -- key exchange -- symmetric-key design.
Sommario/riassunto	The eight-volume set LNCS 14438 until 14445 constitutes the proceedings of the 29th International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2023, held in Guangzhou, China, during December 4-8, 2023. The total of 106 full papers presented in these proceedings was carefully reviewed and selected from 375 submissions. The papers were organized in topical sections as follows: Part I: Secure Multi-party computation; threshold cryptography; . Part II: proof systems - succinctness and foundations; anonymity; Part III: quantum cryptanalysis; symmetric-key cryptanalysis; Part IV: cryptanalysis of post-quantum and public-key systems; side-channels; quantum random oracle model; Part V: functional encryption, commitments and proofs; secure messaging and broadcast; Part VI: homomorphic encryption; encryption with special functionalities; security proofs and security models; Part VII: post-quantum cryptography; Part VIII: quantum cryptography; key exchange; symmetric-key design.