1.	Record Nr.	UNISA996574258503316
	Autore	Guo Jian
	Titolo	Advances in Cryptology – ASIACRYPT 2023 [[electronic resource]] : 29th International Conference on the Theory and Application of Cryptology and Information Security, Guangzhou, China, December 4–8, 2023, Proceedings, Part III / / edited by Jian Guo, Ron Steinfeld
	Pubbl/distr/stampa	Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2023
	ISBN	9789819987276
		9789819987269
	Edizione	[1st ed. 2023.]
	Descrizione fisica	1 online resource (485 pages)
	Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14440
	Altri autori (Persone)	SteinfeldRon
	Disciplina	005.824
	Soggetti	Cryptography
		Data encryption (Computer science)
		Computer networks
		Application software
		Data protection
		Computer networks - Security measures
		Cryptology
		Computer Communication Networks
		Computer and Information Systems Applications
		Security Services
		Mobile and Network Security
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	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.