1.

Record Nr.	UNISA996635666303316
Autore	Chung Kai-Min
Titolo	Advances in Cryptology – ASIACRYPT 2024 : 30th International Conference on the Theory and Application of Cryptology and Information Security, Kolkata, India, December 9–13, 2024, Proceedings, Part VI / / edited by Kai-Min Chung, Yu Sasaki
Pubbl/distr/stampa	Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2025
ISBN	9789819609383
	9819609380
Edizione	[1st ed. 2025.]
Descrizione fisica	1 online resource (508 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 15489
Altri autori (Persone)	SasakiYu
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
Nota di contenuto	Secure Multiparty Computation -- Blockchain Protocols -- Information-theoretic Cryptography.
Sommario/riassunto	The 9 volume set LNCS 15484-15492 constitutes the refereed proceedings of the 30th International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2024, which took place in Kolkata, India, during December 9–13, 2024. The 127 full papers included in the proceedings were carefully reviewed and selected from 433 submissions. They were organized in topical sections as follows: Advances Primitives; homomorphic encryption;

digital signatures; public-key cryptography; pairing-based cryptography, threshold cryptography; isogeny-based cryptography; post-quantum cryptography; secure data structures; lattice-based cryptography; lattice assumptions; key exchange protocols; succinct arguments; verifiable computation, zero-knowledge protocols; secure multiparty computation; blockchain protocols; information theoretic cryptography; secret sharing; security against physical attacks; cryptanalysis on symmetric-key schemes; cryptanalysis on public-key schemes; fault attacks and side-channel analysis; cryptanalysis on various problems; quantum cryptanalysis; quantum cryptography; symmetric-key cryptography.