1.	Record Nr.	UNINA9910349391703321
	Titolo	Advances in Cryptology – ASIACRYPT 2018 : 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2–6, 2018, Proceedings, Part III / / edited by Thomas Peyrin, Steven Galbraith
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2018
	ISBN	3-030-03332-5
	Edizione	[1st ed. 2018.]
	Descrizione fisica	1 online resource (XVI, 553 p. 78 illus., 17 illus. in color.)
	Collana	Security and Cryptology ; ; 11274
	Disciplina	005.8 005.824
	Soggetti	Data encryption (Computer science) Software engineering Computer communication systems Computers Cryptology Software Engineering/Programming and Operating Systems Computer Communication Networks Computing Milieux
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di contenuto	Multi-party Computation -- ORAM -- Real World Protocols -- Secret Sharing -- Isogeny Cryptography -- Foundations.
	Sommario/riassunto	The three-volume set of LNCS 11272, 11273, and 11274 constitutes the refereed proceedings of the 24th International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2018, held in Brisbane, Australia, in December 2018. The 65 revised full papers were carefully selected from 234 submissions. They are organized in topical sections on Post-Quantum Cryptanalysis; Encrypted Storage; Symmetric-Key Constructions; Lattice Cryptography; Quantum Symmetric Cryptanalysis; Zero-Knowledge; Public Key and Identity-Based Encryption; Side-Channels; Signatures; Leakage-Resilient Cryptography; Functional/Inner Product/Predicate Encryption;