1. Record Nr. UNINA9910349391903321

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 I / / edited by Thomas Peyrin, Steven Galbraith
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2018
ISBN	3-030-03326-0
Edizione	[1st ed. 2018.]
Descrizione fisica	1 online resource (XXIV, 659 p. 120 illus., 50 illus. in color.)
Collana	Security and Cryptology ; ; 11272
Disciplina	005.82 005.824
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 bibliografia	Includes bibliographical references and index.
Nota di contenuto	Post-Quantum Cryptanalysis -- Encrypted Storage -- Symmetric-Key Constructions -- Lattice Cryptography -- Quantum Symmetric Cryptanalysis -- Zero-Knowledge.
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; Multi-party Computation; ORQM; Real World Protocols; Secret Sharing; Isogeny Cryptography; and Foundations.