

1. Record Nr.	UNINA9910484994503321
Titolo	Advances in Cryptology – ASIACRYPT 2017 : 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part I // edited by Tsuyoshi Takagi, Thomas Peyrin
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2017
ISBN	3-319-70694-2
Edizione	[1st ed. 2017.]
Descrizione fisica	1 online resource (XXVI, 813 p. 121 illus.)
Collana	Security and Cryptology ; ; 10624
Disciplina	004
Soggetti	Data encryption (Computer science) Computer security Coding theory Information theory Management information systems Computer science Computers Computer science—Mathematics Cryptology Systems and Data Security Coding and Information Theory Management of Computing and Information Systems Theory of Computation Mathematics of Computing
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Post-Quantum Cryptography -- Symmetric Key Cryptanalysis -- Lattices -- Homomorphic Encryptions.-Access Control -- Oblivious Protocols -- Side Channel Analysis. .
Sommario/riassunto	The three-volume set LNCS 10624, 10625, 10626 constitutes the refereed proceedings of the 23rd International Conference on the Theory and Applications of Cryptology and Information Security,

ASIACRYPT 2017, held in Hong Kong, China, in December 2017. The 65 revised full papers were carefully selected from 243 submissions. They are organized in topical sections on Post-Quantum Cryptography; Symmetric Key Cryptanalysis; Lattices; Homomorphic Encryptions; Access Control; Oblivious Protocols; Side Channel Analysis; Pairing-based Protocols; Quantum Algorithms; Elliptic Curves; Block Chains; Multi-Party Protocols; Operating Modes Security Proofs; Cryptographic Protocols; Foundations; Zero-Knowledge Proofs; and Symmetric Key Designs.

---