

1. Record Nr.	UNINA9910484996803321
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 III // edited by Tsuyoshi Takagi, Thomas Peyrin
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2017
ISBN	3-319-70700-0
Edizione	[1st ed. 2017.]
Descrizione fisica	1 online resource (XVIII, 473 p. 57 illus.)
Collana	Security and Cryptology, , 2946-1863 ; ; 10626
Disciplina	005.82
Soggetti	Cryptography Data encryption (Computer science) Data protection Coding theory Information theory Electronic data processing - Management Computer science Computer science - Mathematics Cryptology Data and Information Security Coding and Information Theory IT Operations Theory of Computation Mathematics of Computing
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Cryptographic Protocols -- Foundations -- Zero-Knowledge Proofs -- Symmetric Key Designs.
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.
