

1. Record Nr.	UNISA996465492903316
Titolo	Advances in Cryptology – ASIACRYPT 2016 [[electronic resource]] : 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I // edited by Jung Hee Cheon, Tsuyoshi Takagi
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2016
ISBN	3-662-53887-3
Edizione	[1st ed. 2016.]
Descrizione fisica	1 online resource (XXIV, 941 p. 217 illus.)
Collana	Security and Cryptology ; ; 10031
Disciplina	005.8
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 bibliografia	Includes bibliographical references and index.
Nota di contenuto	Mathematical Analysis -- AES and White-Box -- Hash Function; Randomness -- Authenticated Encryption -- Block Cipher -- SCA and Leakage Resilience -- Zero Knowledge -- Post Quantum Cryptography -- Provable Security -- Digital Signature -- Functional and Homomorphic Cryptography -- ABE and IBE -- Foundation --

Sommario/riassunto

The two-volume set LNCS 10031 and LNCS 10032 constitutes the refereed proceedings of the 22nd International Conference on the Theory and Applications of Cryptology and Information Security, ASIACRYPT 2016, held in Hanoi, Vietnam, in December 2016. The 67 revised full papers and 2 invited talks presented were carefully selected from 240 submissions. They are organized in topical sections on Mathematical Analysis; AES and White-Box; Hash Function; Randomness; Authenticated Encryption; Block Cipher; SCA and Leakage Resilience; Zero Knowledge; Post Quantum Cryptography; Provable Security; Digital Signature; Functional and Homomorphic Cryptography; ABE and IBE; Foundation; Cryptographic Protocol; Multi-Party Computation.
