1. Record Nr. UNISA996465707303316

Titolo	Advances in Cryptology – EUROCRYPT 2016 [[electronic resource]] : 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part I / / edited by Marc Fischlin, Jean-Sébastien Coron
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2016
ISBN	3-662-49890-1
Edizione	[1st ed. 2016.]
Descrizione fisica	1 online resource (XXVIII, 853 p. 155 illus.)
Collana	Security and Cryptology ; ; 9665
Disciplina	005.8
Soggetti	Data encryption (Computer science) Algorithms Computer security Management information systems Computer science Computer science—Mathematics Cryptology Algorithm Analysis and Problem Complexity Systems and Data Security Management of Computing and Information Systems Discrete Mathematics in Computer Science
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	(Pseudo)randomness -- LPN/LWE -- Cryptanalysis -- Masking -- Fully homomorphic encryption -- Number theory -- Hash functions -- Multilinear maps -- Message authentification codes -- Attacks on SSL/TLS -- Real-world protocols -- Robust designs -- Lattice reduction.
Sommario/riassunto	The two-volume proceedings LNCS 9665 + LNCS 9666 constitutes the thoroughly refereed proceedings of the 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2016, held in Vienna, Austria, in May 2016.

The 62 full papers included in these volumes were carefully reviewed and selected from 274 submissions. The papers are organized in topical sections named: (pseudo)randomness; LPN/LWE; cryptanalysis; masking; fully homomorphic encryption; number theory; hash functions; multilinear maps; message authentification codes; attacks on SSL/TLS; real-world protocols; robust designs; lattice reduction; latticed-based schemes; zero-knowledge; pseudorandom functions; multi-party computation; separations; protocols; round complexity; commitments; lattices; leakage; in differentiability; obfuscation; and automated analysis, functional encryption, and non-malleable codes.