1.	Record Nr.	UNISA996215840103316
	Titolo	Advances in Cryptology -- CRYPTO 2015 [[electronic resource]] : 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I / / edited by Rosario Gennaro, Matthew Robshaw
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2015
	ISBN	3-662-47989-3
	Edizione	[1st ed. 2015.]
	Descrizione fisica	1 online resource (XVIII, 787 p. 108 illus.)
	Collana	Security and Cryptology ; ; 9215
	Disciplina	005.82
	Soggetti	Data encryption (Computer science)
		Computer security
		Algorithms
		Computer science—Mathematics
		Cryptology
		Systems and Data Security
		Algorithm Analysis and Problem Complexity
		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	Lattice-based cryptography -- Cryptanalytic insights -- Modes and constructions -- Multilinear maps and IO -- Pseudorandomness -- Block cipher cryptanalysis -- Integrity -- Assumptions -- Hash functions and stream cipher cryptanalysis -- Implementations -- Multiparty computation -- Zero-knowledge -- Theory -- Signatures -- Non-signaling and information-theoretic crypto -- Attribute-based encryption -- New primitives -- Fully homomorphic/functional encryption.
	Sommario/riassunto	The two volume-set, LNCS 9215 and LNCS 9216, constitutes the refereed proceedings of the 35th Annual International Cryptology Conference, CRYPTO 2015, held in Santa Barbara, CA, USA, in August 2015. The 74 revised full papers presented were carefully reviewed and selected from 266 submissions. The papers are organized in the

following topical sections: lattice-based cryptography; cryptanalytic insights; modes and constructions; multilinear maps and IO; pseudorandomness; block cipher cryptanalysis; integrity; assumptions; hash functions and stream cipher cryptanalysis; implementations; multiparty computation; zero-knowledge; theory; signatures; non-signaling and information-theoretic crypto; attribute-based encryption; new primitives; and fully homomorphic/functional encryption.