1.	Record Nr.	UNISA996465967103316
	Titolo	Advances in Cryptology – CRYPTO 2016 [[electronic resource]] : 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II / / edited by Matthew Robshaw, Jonathan Katz
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2016
	ISBN	3-662-53008-2
	Edizione	[1st ed. 2016.]
	Descrizione fisica	1 online resource (XIII, 703 p. 94 illus.)
	Collana	Security and Cryptology ; ; 9815
	Disciplina	005.82
	Soggetti	Data encryption (Computer science)
		Computer security
		Algorithms
		Management information systems
		Computer science
		Computer science—Mathematics
		Cryptology
		Systems and Data Security
		Algorithm Analysis and Problem Complexity
		Management of Computing and Information Systems
		Discrete Mathematics in Computer Science
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Includes index.
	Nota di contenuto	Provable security for symmetric cryptography -- Asymmetric cryptography and cryptanalysis -- Cryptography in theory and practice -- Compromised systems -- Symmetric cryptanalysis -- Algorithmic number theory -- Symmetric primitives -- Asymmetric cryptography -- Symmetric cryptography -- Cryptanalytic tools -- Hardware-oriented cryptography -- Secure computation and protocols -- Obfuscation -- Quantum techniques -- Spooky encryption -- IBE, ABE, and functional encryption -- Automated tools and synthesis -- Zero knowledge -- Theory.

Sommario/riassunto The three volume-set, LNCS 9814, LNCS 9815, and LNCS 9816, constitutes the refereed proceedings of the 36th Annual International Cryptology Conference, CRYPTO 2016, held in Santa Barbara, CA, USA, in August 2016. The 70 revised full papers presented were carefully reviewed and selected from 274 submissions. The papers are organized in the following topical sections: provable security for symmetric cryptography; asymmetric cryptography and cryptanalysis; cryptography in theory and practice; compromised systems; symmetric cryptanalysis; algorithmic number theory; symmetric primitives; asymmetric cryptography; symmetric cryptography; cryptanalytic tools; hardware-oriented cryptography; secure computation and protocols; obfuscation; quantum techniques; spooky encryption; IBE, ABE, and functional encryption; automated tools and synthesis; zero knowledge; theory.