1.	Record Nr.	UNINA9910483156103321
	Titolo	Advances in Cryptology – CRYPTO 2017 : 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20–24, 2017, Proceedings, Part I / / edited by Jonathan Katz, Hovav Shacham
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2017
	ISBN	3-319-63688-X
	Edizione	[1st ed. 2017.]
	Descrizione fisica	1 online resource (XV, 793 p. 120 illus.)
	Collana	Security and Cryptology, , 2946-1863 ; ; 10401
	Disciplina	005.82
	Soggetti	Cryptography
		Data encryption (Computer science)
		Data protection
		Computer networks
		Computers and civilization
		Electronic data processing - Management
		Computers - Law and legislation
		Information technology - Law and legislation
		Cryptology
		Data and Information Security
		Computer Communication Networks
		Computers and Society
		IT Operations
		Legal Aspects of Computing
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Sommario/riassunto	The three volume-set, LNCS 10401, LNCS 10402, and LNCS 10403, constitutes the refereed proceedings of the 37th Annual International Cryptology Conference, CRYPTO 2017, held in Santa Barbara, CA, USA, in August 2017. The 72 revised full papers presented were carefully reviewed and selected from 311 submissions. The papers are organized in the following topical sections: functional encryption; foundations;

two-party computation; bitcoin; multiparty computation; award papers; obfuscation; conditional disclosure of secrets; OT and ORAM; quantum; hash functions; lattices; signatures; block ciphers; authenticated encryption; public-key encryption, stream ciphers, lattice crypto; leakage and subversion; symmetric-key crypto, and real-world crypto.