1.	Record Nr.	UNISA996203611203316
	Titolo	Advances in Cryptology – EUROCRYPT 2014 [[electronic resource]] : 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014, Proceedings / / edited by Phong Q. Nguyen, Elisabeth Oswald
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2014
	ISBN	3-642-55220-X
	Edizione	[1st ed. 2014.]
	Descrizione fisica	1 online resource (XIV, 714 p. 77 illus.) : online resource
	Collana	Security and Cryptology ; ; 8441
	Disciplina	005.82
	Soggetti	Data encryption (Computer science) Algorithms Computer security Cryptology Algorithm Analysis and Problem Complexity Systems and Data Security
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Bibliographic Level Mode of Issuance: Monograph
	Nota di bibliografia	Includes bibliographical references and index.
	Nota di contenuto	Public key cryptanalysis -- Identity-based encryption -- Key derivation and quantum computing -- Secret-key analysis and implementations -- Obfuscation and multi linear maps -- Authenticated encryption -- Symmetric encryption -- Multi-party encryption -- Side-channel attacks -- Signatures and public-key encryption -- Functional encryption -- Foundations -- Multi-party computation.
	Sommario/riassunto	This book constitutes the proceedings of the 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2014, held in Copenhagen, Denmark, in May 2014. The 38 full papers included in this volume were carefully reviewed and selected from 197 submissions. They deal with public key cryptanalysis, identity-based encryption, key derivation and quantum computing, secret-key analysis and implementations, obfuscation and multi linear maps, authenticated encryption, symmetric encryption, multi-party encryption, side-channel attacks, signatures and public-