1. Record Nr. UNISA996198258503316

Titolo	Advances in Cryptology -- CRYPTO 2014 [[electronic resource]] : 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part II / / edited by Juan A. Garay, Rosario Gennaro
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2014
ISBN	3-662-44381-3
Edizione	[1st ed. 2014.]
Descrizione fisica	1 online resource (XVIII, 532 p. 53 illus.)
Collana	Security and Cryptology ; ; 8617
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 bibliografia	Includes bibliographical references and index.
Nota di contenuto	Quantum Cryptography -- Foundations of Hardness -- Obfuscation. - Number-Theoretic Hardness -- Side Channels and Leakage Resilience -- Information-Theoretic Security -- Key Exchange and Secure Communication -- Zero Knowledge -- Composable Security -- Secure Computation – Foundations -- Secure Computation – Implementations.
Sommario/riassunto	The two volume-set, LNCS 8616 and LNCS 8617, constitutes the refereed proceedings of the 34th Annual International Cryptology Conference, CRYPTO 2014, held in Santa Barbara, CA, USA, in August 2014. The 60 revised full papers presented in LNCS 8616 and LNCS 8617 were carefully reviewed and selected from 227 submissions. The papers are organized in topical sections on symmetric encryption and PRFs; formal methods; hash functions; groups and maps; lattices; asymmetric encryption and signatures; side channels and leakage resilience; obfuscation; FHE; quantum cryptography; foundations of

hardness; number-theoretic hardness; information-theoretic security; key exchange and secure communication; zero knowledge; composable security; secure computation - foundations; secure computation - implementations.