1. Record Nr. UNINA9910483918103321

Titolo	Advances in Cryptology -- CRYPTO 2014 : 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part I / / edited by Juan A. Garay, Rosario Gennaro
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2014
ISBN	3-662-44371-6
Edizione	[1st ed. 2014.]
Descrizione fisica	1 online resource (XVIII, 574 p. 52 illus.)
Collana	Security and Cryptology ; ; 8616
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	Symmetric Encryption and PRFs -- Formal Methods -- Hash Functions -- Groups and Maps -- Lattices.- Asymmetric Encryption and Signatures -- Side Channels and Leakage Resilience -- Obfuscation -- FHE.
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.