1. Record Nr. UNINA9910483213803321

Titolo	Advances in Cryptology – CRYPTO 2013 : 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I / / edited by Ran Canetti, Juan A. Garay
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2013
ISBN	3-642-40041-8
Edizione	[1st ed. 2013.]
Descrizione fisica	1 online resource (XVIII, 590 p. 83 illus.)
Collana	Security and Cryptology, , 2946-1863 ; ; 8042
Disciplina	005.82
Soggetti	Cryptography Data encryption (Computer science) Data protection Algorithms Computer science - Mathematics Discrete mathematics Computer science Cryptology Data and Information Security Discrete Mathematics in Computer Science Computer Science
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Lattices and FHE -- Foundations of Hardness -- Cryptanalysis -- New Directions -- Leakage Resilience -- Symmetric Encryption and PRFs -- Key Exchange -- Multi Linear Maps -- Ideal Ciphers.
Sommario/riassunto	The two volume-set, LNCS 8042 and LNCS 8043, constitutes the refereed proceedings of the 33rd Annual International Cryptology Conference, CRYPTO 2013, held in Santa Barbara, CA, USA, in August 2013. The 61 revised full papers presented in LNCS 8042 and LNCS 8043 were carefully reviewed and selected from numerous submissions. Two abstracts of the invited talks are also included in the proceedings. The papers are organized in topical sections on lattices

and FHE; foundations of hardness; cryptanalysis; MPC - new directions; leakage resilience; symmetric encryption and PRFs; key exchange; multi linear maps; ideal ciphers; implementation-oriented protocols; number-theoretic hardness; MPC - foundations; codes and secret sharing; signatures and authentication; quantum security; new primitives; and functional encryption.