

1. Record Nr.	UNINA9910741170403321
Titolo	Advances in Cryptology – CRYPTO 2023 : 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20–24, 2023, Proceedings, Part V // edited by Helena Handschuh, Anna Lysyanskaya
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2023
ISBN	3-031-38554-3
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (XIX, 868 p. 126 illus., 23 illus. in color.)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14085
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Computer engineering Computer networks Computer networks - Security measures Coding theory Information theory Cryptology Computer Engineering and Networks Mobile and Network Security Coding and Information Theory Xifratge (Informàtica) Seguretat informàtica Congressos Llibres electrònics
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Sommario/riassunto	The five-volume set, LNCS 14081, 140825, 14083, 14084, and 14085 constitutes the refereed proceedings of the 43rd Annual International Cryptology Conference, CRYPTO 2023. The conference took place at Santa Barbara, USA, during August 19-24, 2023. The 124 full papers

presented in the proceedings were carefully reviewed and selected from a total of 479 submissions. The papers are organized in the following topical sections: Part I: Consensus, secret sharing, and multi-party computation; Part II: Succinctness; anonymous credentials; new paradigms and foundations; Part III: Cryptanalysis; side channels; symmetric constructions; isogenies; Part IV: Faster fully homomorphic encryption; oblivious RAM; obfuscation; secure messaging; functional encryption; correlated pseudorandomness; proof systems in the discrete-logarithm setting. .
