

1. Record Nr.	UNINA9910349415203321
Titolo	Advances in Cryptology – CRYPTO 2018 : 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part I // edited by Hovav Shacham, Alexandra Boldyreva
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2018
ISBN	9783319968841 331996884X
Edizione	[1st ed. 2018.]
Descrizione fisica	1 online resource (XXIII, 823 p. 133 illus.)
Collana	Security and Cryptology, , 2946-1863 ; ; 10991
Disciplina	005.82
Soggetti	Cryptography Data encryption (Computer science) Coding theory Information theory Computer science - Mathematics Mathematical statistics Software engineering Cryptology Coding and Information Theory Probability and Statistics in Computer Science Software Engineering
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Secure messaging -- Implementations and physical attacks prevention -- Authenticated and format-preserving encryption -- Cryptoanalysis -- Searchable encryption and differential privacy -- Secret sharing -- Encryption -- Symmetric cryptography -- Proofs of work and proofs of Stake -- Proof tools -- Key exchange -- Symmetric cryptoanalysis -- Hashes and random oracles -- Trapdoor functions -- Round optimal MPC -- Foundations -- Lattices -- Lattice-based ZK -- Efficient MPC -- Quantum cryptography -- MPC -- Garbling -- Information-theoretic MPC -- Oblivious transfer -- Non-malleable codes -- Zero knowledge

-- Obfuscation.

Sommario/riassunto

The three volume-set, LNCS 10991, LNCS 10992, and LNCS 10993, constitutes the refereed proceedings of the 38th Annual International Cryptology Conference, CRYPTO 2018, held in Santa Barbara, CA, USA, in August 2018. The 79 revised full papers presented were carefully reviewed and selected from 351 submissions. The papers are organized in the following topical sections: secure messaging; implementations and physical attacks prevention; authenticated and format-preserving encryption; cryptoanalysis; searchable encryption and differential privacy; secret sharing; encryption; symmetric cryptography; proofs of work and proofs of stake; proof tools; key exchange; symmetric cryptoanalysis; hashes and random oracles; trapdoor functions; round optimal MPC; foundations; lattices; lattice-based ZK; efficient MPC; quantum cryptography; MPC; garbling; information-theoretic MPC; oblivious transfer; non-malleable codes; zero knowledge; and obfuscation.