

1. Record Nr.	UNINA9910337842203321
Titolo	Advances in Cryptology – EUROCRYPT 2019 : 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19–23, 2019, Proceedings, Part III // edited by Yuval Ishai, Vincent Rijmen
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2019
ISBN	3-030-17659-2
Edizione	[1st ed. 2019.]
Descrizione fisica	1 online resource (XIX, 793 p. 1749 illus., 24 illus. in color.)
Collana	Security and Cryptology ; ; 11478
Disciplina	001.5436 005.824
Soggetti	Data encryption (Computer science) Software engineering Coding theory Information theory Computers and civilization Data mining Artificial intelligence Cryptology Software Engineering/Programming and Operating Systems Coding and Information Theory Computers and Society Data Mining and Knowledge Discovery Artificial Intelligence
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	ABE and CCA security -- Succinct arguments and secure messaging -- Obfuscation -- Block ciphers -- Differential privacy -- Bounds for symmetric cryptography -- Non-malleability -- Blockchain and consensus -- Homomorphic primitives -- Standards -- Searchable encryption and ORAM -- Proofs of work and space -- Secure computation -- Quantum, secure computation and NIZK, Lattice-based

cryptography -- Foundations -- Efficient secure computation --
Signatures -- Information-theoretic cryptography -- Cryptanalysis.

Sommario/riassunto

The three volume-set LNCS 11476, 11477, and 11478 constitute the thoroughly refereed proceedings of the 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2019, held in Darmstadt, Germany, in May 2019. The 76 full papers presented were carefully reviewed and selected from 327 submissions. The papers are organized into the following topical sections: ABE and CCA security; succinct arguments and secure messaging; obfuscation; block ciphers; differential privacy; bounds for symmetric cryptography; non-malleability; blockchain and consensus; homomorphic primitives; standards; searchable encryption and ORAM; proofs of work and space; secure computation; quantum, secure computation and NIZK, lattice-based cryptography; foundations; efficient secure computation; signatures; information-theoretic cryptography; and cryptanalysis.
