1.	Record Nr.	UNINA9910508435903321
	Titolo	Theory of Cryptography : 19th International Conference, TCC 2021, Raleigh, NC, USA, November 8–11, 2021, Proceedings, Part I / / edited by Kobbi Nissim, Brent Waters
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2021
	ISBN	3-030-90459-8
	Edizione	[1st ed. 2021.]
	Descrizione fisica	1 online resource (799 pages)
	Collana	Security and Cryptology, , 2946-1863 ; ; 13042
	Disciplina	005.82
	Soggetti	Cryptography Data encryption (Computer science) Coding theory Information theory Computer engineering Computer networks Data protection Cryptology Coding and Information Theory Computer Engineering and Networks Computer Communication Networks Data and Information Security
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di bibliografia	Includes bibliographical references and index.
	Nota di contenuto	Secure Quantum Computation with Classical Communication -- Secure Software Leasing from Standard Assumptions -- Post-quantum Resettably-Sound Zero Knowledge -- Secure Software Leasing Without Assumptions -- The Round Complexity of Quantum Zero-Knowledge -- Rate-1 Quantum Fully Homomorphic Encryption -- Unifying Presampling via Concentration Bounds -- Quantum Key-length Extension -- Relationships between quantum IND-CPA notions -- Classical Binding for Quantum Commitments -- Unclonable Encryption, Revisited -- Somewhere Statistical Soundness, Post-Quantum Security,

and SNARGs -- Black-Box Impossibilities of Obtaining 2-Round Weak ZK and Strong WI from Polynomial Hardness -- Tight Security Bounds for Micali's SNARGs -- Acyclicity Programming for Sigma-Protocols.-Statistical ZAPs from Group-Based Assumptions -- Generalized Proofs of Knowledge with Fully Dynamic Setup -- Fully-succinct Publicly Verifiable Delegation from Constant-Size Assumptions -- On expected polynomial runtime in cryptography.-Information-Theoretically Secure MPC against Mixed Dynamic Adversaries -- Round-Efficient Byzantine Agreement and Multi-Party Computation with Asynchronous Fallback -- Two-Round Maliciously Secure Computation with Super-Polynomial Simulation -- Adaptive Security of Multi-Party Protocols, Revisited.-On Actively-Secure Elementary MPC Reductions -- Environmentally Friendly Composable Multi-Party Computation in the Plain Model from Standard (Timed) Assumptions.-.

Sommario/riassunto

The three-volume set LNCS 13042, LNCS 13043 and LNCS 13044 constitutes the refereed proceedings of the 19th International Conference on Theory of Cryptography, TCC 2021, held in Raleigh, NC, USA, in November 2021. The total of 66 full papers presented in this three-volume set was carefully reviewed and selected from 161 submissions. They cover topics on proof systems, attribute-based and functional encryption, obfuscation, key management and secure communication.