1. Record Nr. UNINA9910447246303321

Titolo	Theory of Cryptography : 18th International Conference, TCC 2020, Durham, NC, USA, November 16–19, 2020, Proceedings, Part III / / edited by Rafael Pass, Krzysztof Pietrzak
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2020
ISBN	3-030-64381-6
Edizione	[1st ed. 2020.]
Descrizione fisica	1 online resource (XII, 673 p. 395 illus., 11 illus. in color.)
Collana	Security and Cryptology, , 2946-1863 ; ; 12552
Disciplina	005.82
Soggetti	Cryptography Data encryption (Computer science) Application software Computer networks - Security measures Data protection Computer networks Computer systems Cryptology Computer and Information Systems Applications Mobile and Network Security Data and Information Security Computer Communication Networks Computer System Implementation
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Universal Composition with Global Subroutines: Capturing Global Setup within plain UC -- Security analysis of SPAKE2+ -- Schrödinger's Pirate: How To Trace a Quantum Decoder -- Quantum Encryption with Certified Deletion -- Secure Quantum Extraction Protocols -- Non-interactive Classical Verification of Quantum Computation -- Classical Verification of Quantum Computations with Efficient Verifier -- Coupling of Random Systems -- Towards Defeating Backdoored Random Oracles: Indifferentiability with Bounded Adaptivity -- Zero-

Communication Reductions -- Lower Bounds on the Time/Memory Tradeoff of Function Inversion -- Super-Linear Time-Memory Trade-Offs for Symmetric Encryption -- Algebraic Distinguishers: From Discrete Logarithms to Decisional Uber Assumptions -- On the Security of Time-Lock Puzzles and Timed Commitments -- Expected-Time Cryptography: Generic Techniques and Applications to Concrete Soundness -- On the Complexity of Arithmetic Secret Sharing -- Robust Secret Sharing with AlmostOptimal Share Size and Security Against Rushing Adversaries -- The Share Size of Secret-Sharing Schemes for Almost All Access Structures and Graphs -- Transparent Error Correcting in a Computationally Bounded World -- New Techniques in Replica Encodings with Client Setup.

Sommario/riassunto

This three-volume set, LNCS 12550, 12551, and 12552, constitutes the refereed proceedings of the 18th International Conference on Theory of Cryptography, TCCC 2020, held in Durham, NC, USA, in November 2020. The total of 71 full papers presented in this three-volume set was carefully reviewed and selected from 167 submissions. Amongst others they cover the following topics: study of known paradigms, approaches, and techniques, directed towards their better understanding and utilization; discovery of new paradigms, approaches and techniques that overcome limitations of the existing ones, formulation and treatment of new cryptographic problems; study of notions of security and relations among them; modeling and analysis of cryptographic algorithms; and study of the complexity assumptions used in cryptography. Due to the Corona pandemic this event was held virtually.