1. **Record Nr.**   UNISA996418302103316

   Titolo   Theory of cryptography : 18th International Conference, TCC 2020, Durham, NC, USA, November 16-19, 2020, proceedings, part II / / Rafael Pass, Krzysztof Pietrzak (Eds.)

   Pubbl/distr/stampa   Cham, Switzerland : , : Springer, , [2020]
                              Â©2020

   ISBN   3-030-64378-6

   Edizione   [1st ed. 2020.]

   Descrizione fisica   1 online resource (XII, 715 p. 139 illus., 25 illus. in color.)

   Collana   Lecture Notes in Computer Science ; ; 12551

   Disciplina   005.82

   Soggetti   Data encryption (Computer science)

   Lingua di pubblicazione   Inglese

   Formato   Materiale a stampa

   Livello bibliografico   Monografia

   Nota di contenuto   Proof-Carrying Data from Accumulation Schemes -- Linear-Time Arguments with Sublinear Verification from Tensor Codes -- Barriers for Succinct Arguments in the Random Oracle Model -- Accumulators in (and Beyond) Generic Groups: Non-Trivial Batch Verification Requires Interaction -- Batch Verification and Proofs of Proximity with Polylog Overhead -- Batch Verification for Statistical Zero Knowledge Proofs -- Public-Coin Zero-Knowledge Arguments with (almost) Minimal Time and Space Overheads -- On the Price of Concurrency in Group Ratcheting Protocols -- Stronger Security and Constructions of Multi-Designated Verifier Signatures -- Continuous Group Key Agreement with Active Security -- Round Optimal Secure Multiparty Computation from Minimal Assumptions -- Reusable Two-Round MPC from DDH -- Mr NISC: Multiparty Reusable Non-Interactive Secure Computation -- Secure Massively Parallel Computation for Dishonest Majority -- Towards Multiparty Computation Withstanding Coercion of All Parties -- Synchronous Constructive Cryptography -- Topology-Hiding Communication from Minimal Assumptions. -- Information-Theoretic 2-Round MPC without Round Collapsing: Adaptive Security, and More -- On Statistical Security in Two-Party Computation -- The Resiliency of MPC with Low Interaction: The Revisiting Fairness in MPC: Polynomial Number of Parties and General Adversarial Structures -- On the Power of an Honest Majority in Three-Party Computation Without Broadcast --

A Secret-Sharing Based MPC Protocol for Boolean Circuits with Good Amortized Complexity -- On the Round Complexity of the Shuffle Model.

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.