1. Record Nr. UNINA9910357840603321

Titolo	Theory of Cryptography : 17th International Conference, TCC 2019, Nuremberg, Germany, December 1–5, 2019, Proceedings, Part I / / edited by Dennis Hofheinz, Alon Rosen
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2019
ISBN	3-030-36030-X
Edizione	[1st ed. 2019.]
Descrizione fisica	1 online resource (611 pages)
Collana	Security and Cryptology ; ; 11891
Disciplina	005.82
Soggetti	Data encryption (Computer science) Computer communication systems Application software Data structures (Computer science) Computer security Computers Cryptology Computer Communication Networks Information Systems Applications (incl. Internet) Data Structures and Information Theory Systems and Data Security Computing Milieux
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Algebraically Structured LWE, Revisited -- Lattice Trapdoors and IBE from Middle-Product LWE -- Matrix PRFs: Constructions, Attacks, and Applications to Obfuscation -- Obfuscated Fuzzy Hamming Distance and Conjunctions from Subset Product Problems -- A Black-Box Construction of Fully-Simulatable, Round-Optimal Oblivious Transfer from Strongly Uniform Key Agreement -- Synchronous Consensus with Optimal Asynchronous Fallback Guarantees -- Predicate Encryption from Bilinear Maps and One-Sided Probabilistic Rank -- Optimal Bounded-Collusion Secure Functional Encryption -- From FE Combiners

to Secure MPC and Back -- (Pseudo) Random Quantum States with Binary Phase -- General Linear Group Action on Tensors: A Candidate for Post-Quantum Cryptography -- Composable and Finite Computational Security of Quantum Message Transmission -- On Fully Secure MPC with Solitary Output -- Secure Computation with Preprocessing via Function Secret Sharing -- Efficient Private PEZ Protocols for Symmetric Functions -- The Function-Inversion Problem: Barriers and Opportunities -- On the Complexity of Collision Resistant Hash Functions: New and Old Black-Box Separations -- Characterizing Collision and Second-Preimage Resistance in Linicrypt -- Efficient Information-Theoretic Secure Multiparty Computation over Z/pkZ via Galois Rings -- Is Information-Theoretic Topology-Hiding Computation Possible -- Channels of Small Log-Ratio Leakage and Characterization of Two-Party Differentially Private Computation -- On Perfectly Secure 2PC in the OT-Hybrid Model.

Sommario/riassunto

The two-volume set LNCS 11891 and 11892 constitutes the proceedings of the 17th International Conference on Theory of Cryptography, TCC 2019, held in Nuremberg, Germany, in December 2019. The 43 full papers presented were carefully reviewed and selected from 147 submissions. The Theory of Cryptography Conference deals with the paradigms, approaches, and techniques used to conceptualize natural cryptographic problems and provide algorithmic solutions to them and much more.