1. Record Nr. UNINA9910376503503321

Autore	Young Michal
Titolo	SIGSOFT 2006 FSE-14 : proceedings of the 14th ACM SIGSOFT International Symposium on the Foundations of Software Engineering : November 5-11, 2006, Portland, Oregon, USA
Pubbl/distr/stampa	[Place of publication not identified], : ACM, 2006
Descrizione fisica	1 online resource (290 pages)
Collana	ACM Conferences
Soggetti	Engineering & Applied Sciences Computer Science
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph

2. Record Nr. UNINA9910357840803321

Titolo	Theory of Cryptography : 17th International Conference, TCC 2019, Nuremberg, Germany, December 1–5, 2019, Proceedings, Part II / / edited by Dennis Hofheinz, Alon Rosen
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2019
ISBN	3-030-36033-4
Edizione	[1st ed. 2019.]
Descrizione fisica	1 online resource (xiv, 578 pages) : illustrations
Collana	Security and Cryptology, , 2946-1863 ; ; 11892
Disciplina	005.82
Soggetti	Cryptography Data encryption (Computer science) Computer networks Application software Data structures (Computer science) Information theory Data protection Computers Cryptology Computer Communication Networks Computer and Information Systems Applications Data Structures and Information Theory Data and Information Security Computing Milieux
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Succinct Arguments in the Quantum Random Oracle Model -- Delegating Quantum Computation in the Quantum Random Oracle Model -- Tighter proofs of CCA security in the quantum random oracle model -- Attribute Based Encryption for Deterministic Finite Automata from DLIN -- CPA-to-CCA Transformation for KDM Security -- New Approaches to Traitor Tracing with Embedded Identities -- A Unified and Composable Take on Ratcheting -- Continuously Non-Malleable

Secret Sharing for General Access Structures -- Interactive Non-Malleable Codes -- Stronger Lower Bounds for Online ORAM -- Adaptively Secure Garbling Schemes for Parallel Computations -- Statistical Difference Beyond the Polarizing Regime -- Estimating Gaps in Martingales and Applications to Coin-Tossing: Constructions & Hardness -- Fully Homomorphic NIZK and NIWI Proofs -- Lower and Upper Bounds on the Randomness Complexity of Private Computations of AND -- Leveraging Linear Decryption: Rate-1 Fully-Homomorphic Encryption and Time-Lock Puzzles -- Compressible FHE with Applications to PIR -- Permuted Puzzles and Cryptographic Hardness -- Linear-Size Constant-Query IOPs for Delegating Computation -- On the (In)security of Kilian-Based SNARGs -- Incrementally Verifiable Computation via Incremental PCPs.

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.