1. Record Nr. UNISA996205173203316

Titolo	Theory of Cryptography [[electronic resource]] : 11th International Conference, TCC 2014, San Diego, CA, USA, February 24-26, 2014, Proceedings / / edited by Yehuda Lindell
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2014
ISBN	3-642-54242-5
Edizione	[1st ed. 2014.]
Descrizione fisica	1 online resource (XVI, 739 p. 59 illus.)
Collana	Security and Cryptology ; ; 8349
Disciplina	005.8
Soggetti	Data encryption (Computer science) Computer security Computers Algorithms Computer science—Mathematics Cryptology Systems and Data Security Computation by Abstract Devices Algorithm Analysis and Problem Complexity Discrete Mathematics in Computer Science
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Virtual Black-Box Obfuscation for All Circuits via Generic Graded Encoding -- Obfuscation for Evasive Functions -- On Extractability Obfuscation -- Two-Round Secure MPC from Indistinguishability Obfuscation -- Chosen Ciphertext Security via Point Obfuscation -- Probabilistically Checkable Proofs of Proximity with Zero-Knowledge -- Achieving Constant Round Leakage-Resilient Zero-Knowledge -- Statistical Concurrent Non-malleable Zero Knowledge -- 4-Round Resettably-Sound Zero Knowledge -- Can Optimally-Fair Coin Tossing Be Based on One-Way Functions? -- On the Power of Public-Key Encryption in Secure Computation -- On the Impossibility of Basing Public-Coin One-Way Permutations on Trapdoor Permutations -- Towards Characterizing Complete Fairness in Secure Two-Party

Computation -- On the Cryptographic Complexity of the Worst Functions -- Constant-Round Black-Box Construction of Composable Multi-Party Computation Protocol -- One-Sided Adaptively Secure Two-Party Computation -- Multi-linear Secret-Sharing -- Broadcast Amplification -- Non-malleable Coding against Bit-Wise and Split-State Tampering -- Continuous Non-malleable Codes -- Locally Updatable and Locally Decodable Codes -- Leakage Resilient Fully Homomorphic Encryption -- Securing Circuits and Protocols against 1/ poly(k) Tampering Rate -- How to Fake Auxiliary Input -- Standard versus Selective Opening Security: Separation and Equivalence Results -- Dual System Encryption via Predicate Encodings -- (Efficient) Universally Composable Oblivious Transfer Using a Minimal Number of Stateless Tokens -- Lower Bounds in the Hardware Token Model -- Unified, Minimal and Selectively Randomizable Structure-Preserving Signatures -- On the Impossibility of Structure-Preserving Deterministic Primitives.

Sommario/riassunto

This book constitutes the refereed proceedings of the 11th Theory of Cryptography Conference, TCC 2014, held in San Diego, CA, USA, in February 2014. The 30 revised full papers presented were carefully reviewed and selected from 90 submissions. The papers are organized in topical sections on obfuscation, applications of obfuscation, zero knowledge, black-box separations, secure computation, coding and cryptographic applications, leakage, encryption, hardware-aided secure protocols, and encryption and signatures.