1. Record Nr. UNISA996465612703316

Titolo	Theory of Cryptography [[electronic resource]] : 14th International Conference, TCC 2016-B, Beijing, China, October 31-November 3, 2016, Proceedings, Part I / / edited by Martin Hirt, Adam Smith
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2016
ISBN	3-662-53641-2
Edizione	[1st ed. 2016.]
Descrizione fisica	1 online resource (XVI, 692 p. 85 illus.)
Collana	Security and Cryptology ; ; 9985
Disciplina	005.82
Soggetti	Data encryption (Computer science) Computer security Algorithms Computer science—Mathematics Management information systems Computer science Computer communication systems Cryptology Systems and Data Security Algorithm Analysis and Problem Complexity Discrete Mathematics in Computer Science Management of Computing and Information Systems Computer Communication Networks
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	TCC Test-of-Time Award -- From Indifferentiability to Constructive Cryptography (and Back) -- Foundations -- Fast Pseudorandom Functions Based on Expander Graphs -- 3-Message Zero Knowledge Against Human Ignorance -- The GGM Function Family is a Weakly One-Way Family of Functions -- On the (In)security of SNARKs in the Presence of Oracles -- Leakage Resilient One-Way Functions: The Auxiliary-Input Setting -- Simulating Auxiliary Inputs, Revisited -- Unconditional Security -- Pseudoentropy: Lower-bounds for Chain

rules and Transformations -- Oblivious Transfer from Any Non-Trivial Elastic Noisy Channel via Secret Key Agreement -- Simultaneous Secrecy and Reliability Amplification for a General Channel Model -- Proof of Space from Stacked Expanders -- Perfectly Secure Message Transmission in Two Rounds -- Foundations of Multi-Party Protocols -- Almost-Optimally Fair Multiparty Coin-Tossing with Nearly Three-Quarters Malicious -- Binary AMD Circuits from Secure Multiparty Computation -- Composable Security in the Tamper-Proof Hardware Model under Minimal Complexity -- Composable Adaptive Secure Protocols without Setup under Polytime Assumptions -- Adaptive Security of Yao's Garbled Circuits -- Round Complexity and Efficiency of Multi-Party Computation -- Efficient Secure Multiparty Computation with Identifiable Abort -- Secure Multiparty RAM Computation in Constant Rounds -- Constant-Round Maliciously Secure Two-Party Computation in the RAM Model -- More Efficient Constant-Round Multi-Party Computation from BMR and SHE -- Cross&Clean: Amortized Garbled Circuits With Constant Overhead -- Differential Privacy -- Separating Computational and Statistical Differential Privacy in the Client-Server Model -- Concentrated Differential Privacy: Simplifications, Extensions, and Lower Bounds -- Strong Hardness of Privacy from Weak Traitor Tracing. .

Sommario/riassunto

The two-volume set LNCS 9985 and LNCS 9986 constitutes the refereed proceedings of the 14th International Conference on Theory of Cryptography, TCC 2016-B, held in Beijing, China, in November 2016. The total of 45 revised full papers presented in the proceedings were carefully reviewed and selected from 113 submissions. The papers were organized in topical sections named: TCC test-of-time award; foundations; unconditional security; foundations of multi-party protocols; round complexity and efficiency of multi-party computation; differential privacy; delegation and IP; public-key encryption; obfuscation and multilinear maps; attribute-based encryption; functional encryption; secret sharing; new models.