1. Record Nr. UNISA996465626903316

Titolo	Theory of Cryptography [[electronic resource]] : 14th International Conference, TCC 2016-B, Beijing, China, October 31-November 3, 2016, Proceedings, Part II / / edited by Martin Hirt, Adam Smith
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2016
ISBN	3-662-53644-7
Edizione	[1st ed. 2016.]
Descrizione fisica	1 online resource (XV, 578 p. 32 illus.)
Collana	Security and Cryptology ; ; 9986
Disciplina	004
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 contenuto	Delegation and IP -- Delegating RAM Computations with Adaptive Soundness and Privacy -- Interactive Oracle Proofs -- Adaptive Succinct Garbled RAM, or How To Delegate Your Database.-Delegating RAM Computations -- Public-Key Encryption -- Standard Security Does Not Imply Indistinguishability Under Selective Opening -- Public-Key Encryption with Simulation-Based Selective-Opening Security and Compact Ciphertexts -- Towards Non-Black-Box Separations of Public Key Encryption and One Way Function -- Post-Quantum Security of the

Fujisaki-Okamoto and OAEP Transforms -- Multi-Key FHE from LWE, Revisited -- Obfuscation and Multilinear Maps -- Secure Obfuscation in a Weak Multilinear Map Model -- Virtual Grey-Boxes Beyond Obfuscation: A Statistical Security Notion for Cryptographic Agents -- Attribute-Based Encryption -- Deniable Attribute Based Encryption for Branching Programs from LWE -- Targeted Homomorphic Attribute-Based Encryption -- Semi-Adaptive Security and Bundling Functionalities Made Generic and Easy -- Functional Encryption -- From Cryptomania to Obfustopia through Secret-Key Functional Encryption -- Single-Key to Multi-Key Functional Encryption with Polynomial Loss -- Compactness vs Collusion Resistance in Functional Encryption -- Secret Sharing -- Threshold Secret Sharing Requires a Linear Size Alphabet -- How to Share a Secret, Infinitely -- New Models -- Designing Proof of Human-work Puzzles for Cryptocurrency and Beyond -- Access Control Encryption: Enforcing Information Flow with Cryptography.

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.