1.	Record Nr.	UNISA996207295603316
	Titolo	Information Theoretic Security [[electronic resource]] : 8th International Conference, ICITS 2015, Lugano, Switzerland, May 2-5, 2015. Proceedings / / edited by Anja Lehmann, Stefan Wolf
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2015
	ISBN	3-319-17470-3
	Edizione	[1st ed. 2015.]
	Descrizione fisica	1 online resource (XIV, 297 p. 29 illus.)
	Collana	Security and Cryptology ; ; 9063
	Disciplina	005.82
	Soggetti	Computer security Data encryption (Computer science) Coding theory Information theory Systems and Data Security Cryptology Coding and Information Theory
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Includes index.
	Nota di contenuto	Practical Sharing of Quantum Secrets over Untrusted Channels -- Generalizing Efficient Multiparty Computation -- Round-Optimal Perfectly Secret Message Transmission with Linear Communication Complexity -- On Zero-Knowledge with Strict Polynomial-Time Simulation and Extraction from Differing-Input Obfuscation for Circuits -- Unifying Leakage Classes: Simulatable Leakage and Pseudoentropy -- On the Orthogonal Vector Problem and the Feasibility of Unconditionally Secure Leakage-Resilient Computation -- Metric Pseudoentropy: Characterizations, Transformations and Applications -- Nonuniform Indistinguishability and Unpredictability Hardcore Lemmas: New Proofs and Applications to Pseudoentropy -- Gambling, Computational Information and Encryption Security -- Query-Complexity Amplification for Random Oracles -- The Chaining Lemma and Its Application -- Weakening the Isolation Assumption of Tamper-Proof Hardware Tokens -- Limited View Adversary Codes: Bounds,

Constructions and Applications -- Locally Decodable Codes for Edit Distance -- The Multivariate Hidden Number Problem -- Lattice Point Enumeration on Block Reduced Bases -- Adaptive Key Recovery Attacks on NTRU-Based Somewhat Homomorphic Encryption Schemes.

Sommario/riassunto

This book constitutes the thoroughly refereed proceedings of the 8th International Conference on Information Theoretic Security, ICITS 2015, held in Lugano, Switzerland, in May 2015. The 17 full papers presented in this volume were carefully reviewed and selected from 57 submissions. The papers cover a variety of topics at the intersection of cryptography, information theory, and quantum physics.