1.	Record Nr.	UNINA9910483089103321
	Titolo	Information Theoretic Security : 7th International Conference, ICITS 2013, Singapore, November 28-30, 2013, Proceedings / / edited by Carles Padró
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2014
	ISBN	3-319-04268-8
	Edizione	[1st ed. 2014.]
	Descrizione fisica	1 online resource (XII, 259 p. 29 illus.)
	Collana	Security and Cryptology ; ; 8317
	Classificazione	DAT 465f SS 4800
	Disciplina	005.8
	Soggetti	Computer security Data encryption (Computer science) Coding theory Information theory E-commerce Management information systems Computer science Computers and civilization Systems and Data Security Cryptology Coding and Information Theory e-Commerce/e-business Management of Computing and Information Systems Computers and Society Kongress2013.Singapur
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Bibliographic Level Mode of Issuance: Monograph
	Nota di bibliografia	Includes bibliographical references and index.
	Nota di contenuto	How to Construct Strongly Secure Network Coding Scheme -- Secure two-party computation: a visual way -- Measure-independent Characterization of Contrast Optimal Visual Cryptography Schemes -- On (k; n) visual cryptography scheme with t essential parties -- New Lower Bounds for Privacy in Communication Protocols -- On the

Transmit Beamforming for MIMO Wiretap Channels: Large-System Analysis -- Information Theoretic Security for Encryption Based on Conditional Renyi Entropies -- Insider-proof encryption with applications for quantum key distribution -- Superposition Attacks on Cryptographic Protocols -- Overcoming Weak Expectations via the Renyi Entropy and the Expanded Computational Entropy -- Modulus Computational Entropy -- Broadcast (and Round) Efficient Verifiable Secret Sharing -- Leakage Resilience of the Blom's Key Distribution Scheme -- Detection of Algebraic Manipulation in the Presence of Leakage.

| Sommario/riassunto | This book constitutes the proceedings of the 7th International Conference on Information Theoretic Security, ICITS 2013, held in Singapore in November 2013. The 14 papers presented in this volume were carefully reviewed and selected from 49 submissions. Topics of interest are: unconditional security, quantum cryptography, authentication codes, wiretap channels, randomness extraction, codes and cryptography, lattices and cryptography, secret sharing, multiparty Computation, bounded storage model, oblivious transfer, nonlocality and nonsignaling, quantum information theory, network coding security, physical models and assumptions, physical layer security. |