1.	Record Nr.	UNINA9910484384403321
	Titolo	Information Theoretic Security : Third International Conference, ICITS 2008, Calgary, Canada, August 10-13, 2008, Proceedings / / edited by Reihaneh Safavi-Naini
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2008
	ISBN	3-540-85093-7
	Edizione	[1st ed. 2008.]
	Descrizione fisica	1 online resource (XI, 249 p.)
	Collana	Security and Cryptology, , 2946-1863 ; ; 5155
	Disciplina	004
	Soggetti	Cryptography Data encryption (Computer science) Coding theory Information theory Data protection Algorithms Computer networks Electronic data processing - Management Cryptology Coding and Information Theory Data and Information Security Computer Communication Networks IT Operations
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Includes index.
	Nota di bibliografia	Includes bibliographical references and index.
	Nota di contenuto	Secure and Reliable Communication I -- Partially Connected Networks: Information Theoretically Secure Protocols and Open Problems (Invited Talk) -- Almost Secure 1-Round Message Transmission Scheme with Polynomial-Time Message Decryption -- Quantum Information and Communication -- Interactive Hashing: An Information Theoretic Tool (Invited Talk) -- Distributed Relay Protocol for Probabilistic Information-Theoretic Security in a Randomly-Compromised Network -- Networks and Devices -- Strong Secrecy for Wireless Channels

	(Invited Talk) -- Efficient Key Predistribution for Grid-Based Wireless Sensor Networks -- Does Physical Security of Cryptographic Devices Need a Formal Study? (Invited Talk) -- Mulitparty Computation -- A Single Initialization Server for Multi-party Cryptography -- Statistical Security Conditions for Two-Party Secure Function Evaluation -- Information Hiding and Tracing -- Upper Bounds for Set Systems with the Identifiable Parent Property -- Coding Theory and Security -- Oblivious Transfer Based on the McEliece Assumptions -- List Error-Correction with Optimal Information Rate (Invited Talk) -- Quantum Computation -- Theory of Quantum Key Distribution: The Road Ahead (Invited Talk) -- Susceptible Two-Party Quantum Computations -- Secure and Reliable Communication II -- Perfectly Reliable and Secure Communication Tolerating Static and Mobile Mixed Adversary -- Key Refreshing in Wireless Sensor Networks -- Efficient Traitor Tracing from Collusion Secure Codes -- Foundation -- Revisiting the Karnin, Greene and Hellman Bounds -- Simple Direct Reduction of String (1,2)-OT to Rabin’s OT without Privacy Amplification -- The Complexity of Distinguishing Distributions (Invited Talk) -- Encryption -- Some Information Theoretic Arguments for Encryption: Non-malleability and Chosen-CiphertextSecurity (Invited Talk) -- A Proof of Security in O(2 n) for the Xor of Two Random Permutations.
Sommario/riassunto	This book constitutes the proceedings of the Third International Conference on Information Theoretic Security, held in Calgary, Canada, in August 2008. The 14 papers presented in this volume were carefully reviewed and selected from 43 submissions. There were nine invited speeches to the conference. The topics covered are secure and reliable communication; quantum information and communication; networks and devices; multiparty computation; information hiding and tracing; coding theory and security; quantum computation; foundation; and encryption.