

1. Record Nr.	UNINA9910484231003321
Titolo	Information Theoretic Security : 10th International Conference, ICITS 2017, Hong Kong, China, November 29 – December 2, 2017, Proceedings // edited by Junji Shikata
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2017
ISBN	3-319-72089-9
Edizione	[1st ed. 2017.]
Descrizione fisica	1 online resource (XII, 235 p. 31 illus.)
Collana	Security and Cryptology, , 2946-1863 ; ; 10681
Disciplina	005.8
Soggetti	Data protection Coding theory Information theory Computer networks Software engineering Computer science - Mathematics Mathematical statistics Computer vision Data and Information Security Coding and Information Theory Computer Communication Networks Software Engineering Probability and Statistics in Computer Science Computer Vision
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Quantum cryptography -- Quantum information theory -- Post-quantum cryptography (e.g. lattices and cryptography) -- Physical layer security -- Wiretap channels -- Adversarial channel models -- Cryptography from noisy channels -- Bounded storage models -- Network coding security -- Biometric security -- Randomness extraction -- Key and message rates -- Secret sharing -- Authentication codes -- Multiparty computations -- Information

theoretic reductions -- Implementation challenges.

Sommario/riassunto

This book constitutes the refereed proceedings of the 10th International Conference on Information Theoretic Security, ICITS 2017, held in Hong Kong, China, in November/December 2017. The 12 full papers were carefully reviewed and selected from 42 submissions. They are organized around the following topics: quantum cryptography; quantum information theory; post-quantum cryptography (e.g. lattices and cryptography); physical layer security; wiretap channels; adversarial channel models; cryptography from noisy channels; bounded storage models; network coding security; biometric security; randomness extraction; key and message rates; secret sharing; authentication codes; multiparty computations; information theoretic reductions; and implementation challenges.
