

1. Record Nr.	UNISA996418441303316
Autore	Arnon-Friedman Rotem
Titolo	Device-independent quantum information processing : a simplified analysis // Rotem Arnon-Friedman
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2020] ©2020
ISBN	3-030-60231-1
Edizione	[1st ed. 2020.]
Descrizione fisica	1 online resource (XVI, 217 p. 13 illus., 6 illus. in color.)
Collana	Springer Theses
Disciplina	005.824
Soggetti	Quantum communication - Security measures Quantum computers Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Introduction -- Preliminaries: Basics and Notation -- Preliminaries: Device-independent Concepts -- Introduction to the Showcases -- Single-round Box -- Multi-round Box -- Working Under the IID Assumption -- Reductions to IID: Parallel Interaction -- Reductions to IID: Sequential Interaction -- Showcase: Non-signalling Parallel Repetition -- Showcase: Device-independent Quantum Cryptography -- Outlook -- Appendix.
Sommario/riassunto	Device-independent quantum cryptography is a method for exchanging secret messages over potentially insecure quantum communication channels, such as optical fibers. In contrast to conventional quantum cryptography, security is guaranteed even if the devices used by the communication partners, such as photon sources and detectors, deviate from their theoretical specifications. This is of high practical relevance, for attacks to current implementations of quantum cryptography exploit exactly such deviations. Device-independent cryptography is however technologically so demanding that it looked as if experimental realizations are out of reach. In her thesis, Rotem Arnon-Friedman presents powerful information-theoretic methods to prove the security of device-independent quantum cryptography. Based on them, she is able to establish security in a parameter regime that

may be experimentally achievable in the near future. Rotem Arnon-Friedman's thesis thus provides the theoretical foundations for an experimental demonstration of device-independent quantum cryptography. .
