Title:	Developments in Device-Independent Quantum Key Distribution
Authors:	Singh, Jasmeet
Keywords:	Device-Independent Quantum Quantum cryptography quantum encryption
Issue Date:	May-2020
Publisher:	IISERM
Abstract:	Quantum cryptography, also known as quantum encryption, exploits the principles of quantum mechanics to encrypt messages in a way such that it is not possible to be read by anyone except the recipient to which it is sent. It utilizes the advantage of quantum's multiple states, coupled with its "no change theory", to achieve secure encryption, which means it cannot be unknowingly interrupted. The fundamental idea behind the security of quantum cryptography comes from the no-cloning theo- rem. Whenever an eavesdropper tries to gain information by attacking the quantum channel, she would end up disturbing the state. One of the best-known examples of quantum cryptography is quantum key distri- bution. Quantum key distribution (QKD) is a cryptographic task that allows two distant parties, Alice and Bob, to exchange secret keys and communicate securely over an untrusted quantum channel (which can be affected by an eavesdropper, Eve), provided they have access to an authenticated classical channel. The basic idea is that, Eve cannot gain any information from the states transmitted from Alice to Bob. Any attempt by her to try and learn information about the key being established, causes discrepancies, leading to Alice and Bob to notice. Once the key is established, it is then typically used for encrypted communication using classical techniques. The security of the traditional device-dependent quantum key distribution (DD-QKD) protocols is based on several assumptions, the most prominent being that honest users are able to control their devices completely and accurately. Most of these protocols do not consider the fact that the measuring devices cannot be trusted, which causes hidden danger resulting in unsafe quantum communication. The goal of device-independent quantum key distribution (DI-QKD) is to provide a relaxation, even to the fundamental assumption of devices being truthful. In fact, in this case, no assumption is made on the internal working of the devices. The security is based only on the observable behaviour of the devices, i.e. the probabilities of the measurement results given the choice of measurement. This thesis is an attempt to explore the realm quantum key distribution in the context of device-independence.
URI:	http://hdl.handle.net/123456789/1417
Appears in Collections:	MS-15

Files in This Item:

File	Size	Format	
MS15064.pdf	1.11 MB	Adobe PDF	View/Open

Show full item record