A STUDY ON QUANTUM CRYPTOGRAPHIC PROTOCOLS IN THE DEVICE-INDEPENDENT PARADIGM

Abstract

Quantum cryptography (QC) ensures the security of a cryptographic protocol by the fundamental laws of quantum mechanics, such as quantum no-cloning theorem and the Heisenberg uncertainty principle. Although it pledges the unconditional security, but the practical implementations confronted some attacks in which information gets leaked via side-channel. The device-independent paradigm was proposed to avert these types of attacks and prove the security with a minimal number of assumptions. In this thesis, we have investigated the device-independent security of two quantum cryptographic primitives, such as, quantum private query and quantum secret sharing.

In Chapter 2, we have presented a device-independent quantum private query using the idea of local CHSH game. We have shown that the user can gain some extra information by manipulating the source. To remove the trust from the source, we have introduced the device-independent testing phase, performed locally by the database provider. The security of this testing phase is guaranteed by the well-known statistical lemma, called Serfling lemma.

In Chapter 3, a measurement-device-independent quantum private query is proposed using qutrits (a three-dimensional quantum state). We have compared the security properties of the proposed protocol with a protocol using qubits. We have observed an enhanced database privacy but a vulnerable user privacy in the qutrit protocol than a qubit.

Chapters 4 and 5 deal with the proposals quantum secret sharing schemes. In Chapter 4, we have proposed a device-independent quantum secret sharing scheme in arbitrary even dimensions. The device-independent testing criteria is defined by the optimal winning probability of a multipartite higher dimensional linear game using quantum strategy. The security of the scheme depends on a property of an entangled state, which states that an entangled state cannot be arbitrarily shared. In Chapter 5, we have proposed a (t, n)-threshold d-level quantum secret sharing scheme using quantum Fourier transformation. The security of the proposed scheme is defended against all possible attacks. Finally, Chapter 6 deals with the key findings of the thesis and some possible future directions.

Keywords: Quantum Private Query; Quantum Secret Sharing; Nonlocality; Device-Independence; Measurement-Device-Independence; Security analysis.