Abstract

The aim of this dissertation is to describe selected issues of quantum information processing in terms of investigating their physical limitations. In each case, we try to eliminate their negative consequences. As examples of limitations, we consider: relations between resources and their limited quantities, the physical nature of the generation and detection of photons, or the number of measurements we can carry out.

The first chapter describes the historical outline, concentrating mainly on themes which will be developed in the following chapters.

The next chapter is dedicated as a reminder of the basic definitions and concepts on which the work is based. This chapter is divided into two parts. The first is devoted to classical information theory whereas the second focuses on the basic properties of quantum description. The scope of material in this chapter is limited to the needs of subsequent analyzes.

The next chapters, which form the essential part of the work, are primarily based on the results published in the following papers:

[A] *Security of QKD protocols against detector blinding attacks*
arXiv:1504.00939 [quant-ph] (2015)

[B] *Activation of entanglement in teleportation*
J. Phys. A: Math. Theor. 46 435301 (2013)

[C] *Optimal pumping strength for BBM92 key distribution protocol*
Int. J. Quantum Inform. 14, 1650049 (2016)

[D] *Entanglement witnesses with variable number of local measurements*
Phys. Rev. A 88, 022304 (2013),

where I am co-writter.

In chapter three we consider problems of quantum cryptographic key distribution. The chapter begins with a theoretical introduction and description of the physical mechanism that enables photons to be detected. This description is performed on the example of an APD detector (avalanche photo-diode). Then the theoretical model is built, where the control over the devices is taken over by a third party. Two types of two attacks are tested: PP (Capture / Forward) and OP (Late Measurement).

In chapter four we examine the nature of the physical constraint on the (relationship) correspondance/relation/connection between classical communication and quantum entanglement. We study teleportation of d-level quantum states (qudits). The average fidelity of the teleportation process is analyzed, depending on the type of constraint imposed. After the analysis, the limit of classical information needed to activate quantum resources as a function of the dimension d is determined. At the end, the fidelity of the teleportation with classical communication is measured for channels with different characteristics.

In the fifth chapter, we are dealing with the problem of generating states that are useful in cryptographic protocols. We use the parametric PDC (parametric down conversion) as a source of entangled pairs. It is known that with the high pump power, the creation of many pairs of photons becomes more likely and it has a negative impact on the fidelity of the resulted state. We show a way to circumvent this negative limitation which allows for relatively high pumping laser power. In a consequence it leads to a greater efficiency (speed) in cryptographic key generation.

The last chapter is (devoted) to the method for constructing efficient quadratic quantum detection criteria in quantum states. They are ideal in situations of limited number of measurements that we can perform on quantum state. We present many examples that illustrate how the new entanglement indicator works.

In the final chapter we give a summary, in which the main results of the dissertation are collected.