Quantum information science studies the application of quantum mechanics to processing, storing and transmitting information. The most spectacular application of quantum technologies in computer science is quantum cryptography. It is important to notice, that there exist commercial quantum cryptographic systems. Quantum Cryptography presents a new form of security, which is based on on physical security, with the only assumption that quantum mechanics offers a correct physical description of the devices, No assumption is required on the eavesdropper's power, provided she does not contradict any quantum law. Using this assumption, the security of the schemes can be proven.

Unfortunately if one considers a concrete physical realization of a cryptographic protocol, one has to deal with noise, which deforms the action of the protocol. The key issue is to estimate how these imperfections affect the safety of the whole protocol. The aforementioned imperfections are modelled with the use of quantum channels, and, in the most general scenario, we do not impose any assumptions on the noise type. We model the quantum communication line as a mixture of ideal line – which does not change the input state, and the noise modelled as random quantum channel.

In order to recognise the properties of this mixture, we need to understand the properties of typical quantum channels. During the course of the project we will study information quantities for typical quantum channels, and next we will derive the security bounds for a typical quantum communication line.