An important discovery in the field of encryption is a public-key cryptography. In these schemes each of the parties posses its own pair of keys: a private and public. This public can be publicly announced and can be used by anyone to encrypt a message that is intended for the holder of the accompanying private key. Rivest, Adleman and Shamir in 1977 invented a public-key encryption scheme that became known as RSA. RSA is based on an assumption that integer factorization is computationally difficult task. ElGamal is another widely known public-key encryption method, invented in 1984. This encryption system is based on an assumption that computing discrete logarithms is a hard problem. Public-key cryptographic schemes utilizes also elliptic curves over large finite fields.

Summarizing, standard classical cryptography schemes are based on the following assumptions,
Assumption 1: computational power of eavesdropper is limited,
Assumption 2: factoring integers, solving the discrete logarithm on elliptic curves etc. is a hard problem.

Quantum computers shed doubts on the long-term applicability of these schemes, e.g. Shor’s algorithm is able to perform efficient factorization and solving the discrete logarithm on elliptic curves.

Quantum Cryptography presents a new form of security, which is based on on physical security, the only assumption is quantum mechanics offers a correct physical description of the devices, No assumption is required on the eavesdropper’s power, provided it does not contradict any quantum law. Using this assumption, the security of the schemes can be proven.

During the project we will derive a security proof for cryptographic protocols with the most general attacks, i.e. assuming that the eavesdropper has access to quantum memory and is able to entangle his system with the transmitted qubit. For this purpose we will derive a universal conditional entropic uncertainty relation and make a formal description of security of quantum key distribution protocols based on generalised probabilistic theories.