Tremendous progress in experimental quantum optics in the past decades, enabling efficient control and engineering of quantum states of light and matter, has triggered the so-called second quantum revolution. The variety of quantum technologies are now being intensively developed to enable their full-scale implementations in the near future. All of them are based on the phenomenon of quantum entanglement that can bring perfect correlations between intrinsically probabilistic quantum systems. Therefore, distribution of entanglement among remote parties becomes a highly relevant task, both from the perspective of quantum technologies and fundamental tests of physical reality. On the other hand, development of quantum computers poses a potential threat to the security of the whole confidential communication that is being done using classical cryptography. Indeed, the presumably complex computational problems, laying at the core of commonly utilized classical encryption methods, can be efficiently solved with quantum algorithms. Meanwhile, quantum key distribution (QKD) protocols for exchange of secure cryptographic keys are based on the detection of quantum entanglement, directly or effectively shared between the trusted parties. Because of this, security of quantum communication relies not on the presumed complexity of mathematical calculations, but on the fundamental laws of nature and can be verified using information-theoretical proofs.

Although QKD protocols have been tested many times, both in the laboratory environment as well as in the field, these experiments typically used dedicated optical links. However, full-scale implementation of secure quantum communication requires deployment of the entanglement distribution and QKD protocols in the existing networking environment, where optical links are simultaneously utilized for the data transmission using multiplexed classical signals. The overall secure quantum communication rate will also have to be increased. This can be achieved through quantum signal multiplexing. Unfortunately, simultaneous transmission of classical and quantum signals through the same waveguide causes mutual crosstalk. Since the power of quantum signals is many orders of magnitude lower than that of classical signals, this noise is largely destructive for quantum communication. Despite this, only sporadic efforts have been made towards multiplexed quantum communication and co-existence with classical data signals, focusing only on specific protocols.

Therefore, in the proposed project, we will comprehensively study and develop secure quantum communication towards robust and efficient implementation in the multiplexed optical networks. Collaborative nature of the project will enable research in two very different approaches to quantum communication, based on the so-called discrete and continuous quantum variables, which rely respectively on particle- and wave-type properties of quantum light. By revealing the advantages and weaknesses of each of the approaches, taking into account practical setup imperfections, we will set benchmarks and solutions for entanglement distribution and QKD in the studied environment. Additionally, scaling of setup imperfections by the increase of the number of trusted network nodes will be researched. We will propose feasible solutions aimed at compensating the negative effects of crosstalk and network scaling by either adapting the entanglement verification and security analysis methods, modifying the sources of entanglement and set-up schemes or by employing data processing methods. The outcomes of the proposed research will be communicated to the affiliated experimental groups for subsequent tests and verification. The results of the project will therefore both contribute to theoretical study of fundamental properties of entanglement of quantum states in multimode environments and pave the way to full-scale deployment of practical quantum communication in the highly relevant multiplexed networks environment.