ESR 3 – Short article for AppQInfo website

As the world gets increasingly interconnected, free-space quantum key distribution (QKD) holds significant importance in the realm of secure communication. Unlike traditional methods that rely on classical cryptographic algorithms, QKD leverages the principles of quantum mechanics to establish secure communication channels. This technology is crucial for ensuring the confidentiality of sensitive information in the face of evolving threats posed by quantum computers, which could potentially break classical encryption methods. In free-space QKD, quantum keys are transmitted through open air or outer space, offering secure communication over long distances, without the need for physical infrastructure like fiber-optic cables, making it a valuable tool for secure communication in scenarios where traditional methods may be impractical or vulnerable.

Admittedly, free-space QKD distribution will play a crucial role in a potential future quantum internet. The realization of such a network is dependent on having reliable links that can operate in any conditions. In the QuantumFuture group of the university of Padova, one of our focus areas is establishing stable free-space QKD links that can operate under daylight conditions. This is a demanding task due to numerous hindering factors that need to be considered. One of the most significant challenges is atmospheric turbulence, which can distort the quantum signals, leading to errors in the secure key generation process. Additionally, adverse weather conditions such as fog, rain, and snow can further degrade the performance of free-space QKD systems. Another obstacle is the susceptibility of quantum signals to background light, which can be particularly problematic in urban environments with high ambient light levels. Maintaining the alignment of optical components over long distances also poses a technical challenge, requiring sophisticated pointing and tracking (PAT) systems to compensate for movements and vibrations.

To integrate free-space links with already existing fiber infrastructures, we implemented small-scale networks of what we call *intermodal QKD*. The concept involves seamlessly switching between different transmission modes, in our case fiber and free-space, based on the specific conditions or requirements of the communication environment. So far, we have demonstrated intermodal QKD in three experiments in the city of Padova and Vienna at a maximum free-space channel distance of 620 m, relying on compact and versatile telescopes designed by our group and optimized for use in short urban links. Apart from proving that QKD is possible, these trials gave us the opportunity to certify that the theoretical models we use to evaluate the power losses expected in the channel are accurate enough to be used for designing similar systems in the future.

At the same time, we have been working on extending free-space QKD over a 20 km link with a compact transmitter and a commercial 40 cm telescope. Since the impairments caused by the atmosphere are expected to be more severe, it is essential to employ channel sensing methods to estimate the turbulence present in the channel, with the goal of improving the quality of communication through a PAT system. Based on measurements conducted so far, we are designing a high order correction system which will yield possible the performance of QKD.

Before implementing any field trial, it is also useful to have prototypes in the laboratory, which attest that our experimental equipment is operating properly in the conditions expected by the turbulence estimation measurements. For this reason, we have been putting efforts into building a laboratory channel emulator which can reproduce in a systematic manner the conditions present in real atmospheric links.

In conclusion, free-space QKD emerges as a critical technology in ensuring secure communication amid the increasing interconnectivity of our world. The challenges faced in implementing free-space QKD underline the complexity of realizing this technology in real-world scenarios. However, ongoing efforts, such as those undertaken by the QuantumFuture group at the University of Padova, demonstrate promising advancements. As these endeavors progress, they pave the way for the potential establishment of a quantum internet and contribute significantly to the field of secure quantum communication.