Titre (en français) : Distribution de clé quantique à variables continues à travers la turbulence atmosphérique

Titre (en anglais)**:** Continuous-variable quantum key distribution through atmospheric turbulence

Thesis director: Eleni Diamanti, LIP6, CNRS, Sorbonne Université

Thesis subject:
In the context of the future space-ground optical links and telecommunication networks, the issue of securing the transmission channel using quantum resources is currently under intense investigation around the world because of the promise it holds for security levels impossible to reach solely by classical means. Quantum key distribution (QKD) enables two parties to share a secret key used to encrypt and decrypt the exchanged messages with information-theoretic (unconditional) security. Among prevalent QKD technologies, continuous-variable quantum key distribution (CV-QKD) systems offer the major advantage of being compatible with standard telecommunication technologies, which could greatly facilitate and limit the cost of their deployment. Since the demonstration by the LIP6 team that such systems could be suitable for long-distance fibered communication on the ground, this technology has been the subject of intense developments worldwide.

As a baseline, we consider the case of space-to-ground CV-QKD, where a low Earth orbit (LEO) satellite crossing the sky aims at establishing a secret key with an optical station on the ground. The key information is encoded on the amplitude and phase of laser-generated low intensity coherent states. After propagation through a turbulent atmospheric channel, the transmitted signal is coupled into a single-mode optical fibre on the ground, and is then coherently detected and post-processed to extract a secret key. The secret key generation rate quantifies the performance of the system.

In classical optical communication, the atmospheric turbulence degrades the phase and amplitude of the propagating signal. This hampers the coherent detection of the coupled flux, and ultimately limits de CV-QKD performance. As a result, it appears necessary to minimize the amplitude of such fluctuations, while also ensuring an operational satellite-to-ground link during a maximum amount of time, whose upper limit is naturally set by the duration of the satellite visibility above horizon.

To fulfil the first requirement, it is possible to use adaptive optics (AO) to measure and correct in real-time the turbulence-induced phase aberrations, and hence to optimize the coupling of the resulting corrected signal into a single mode fibre. AO has been used in astronomy for over 30 years to bring the resolution of optical systems towards the diffraction limit. In particular, the ONERA team has been at the heart of AO developments on international giant telescopes. Designing and implementing an AO system requires a fine knowledge and modelling of the atmospheric turbulence, which is the reason why the ONERA team developed dedicated analytical and numerical tools for applications in astronomy and specific cases of classical free-space optical telecommunication. The combination of AO and CV-QKD for ground-space optical links is a new research topic demanding knowledge in each of these fields. To date, some preliminary studies have used

simplified models and described AO as a promising technology for CV-QKD, however none of them shows a fine enough knowledge on turbulence modelling to conclude on the impact of turbulence and AO correction on the flux fluctuations.

The difficulty to fulfil the second requirement lies in the fact that the LEO satellite moves across the sky during a very limited amount of time (usually less than 10 minutes). As a result, the propagating signal encounters rapidly varying turbulence conditions and undergoes a Doppler frequency shift. Both these effects have to be considered for the estimation of the CV-QKD performance.

In this PhD thesis, our main goal is to demonstrate the feasibility of CV-QKD between a LEO satellite and the ground, considering the particularities of the turbulent transmission channel. Estimating the impact of the coupled flux fluctuations on the key generation rate is essential and constitutes a major goal of the thesis. A first part of this work consists in a theoretical and modelling study. The aim is to develop a numerical tool enabling to relate directly the coupled flux statistics to the key generation rate. The PhD student will benefit both from the expertise of LIP6 in quantum information and cryptography and from the expertise of ONERA in wave front sensing and correction. At ONERA, the student will be able to rely on the analytical and end-to-end simulation tools to model the propagation channel and the statistical properties of the coupled flux. At LIP6, the student will exploit numerical tools dedicated to key extraction as well as key generation rate computation. Besides the LEO-to-ground scenario, different configurations of optical links may be considered: geostationary satellite-to-ground transmission, and free-space urban CV-QKD, for example between a building and a drone. Comparisons with discrete-variable (DV) QKD protocols will also be performed. The second part of the thesis will then be dedicated to the design and implementation of a first in-lab experimental demonstration. This would constitute a world first proof of concept and pave the way towards the development of efficient space-based CV-QKD systems.

Additional remarks:
The PhD student will be at the heart of a collaboration between two top-level research teams with an expertise recognized internationally. The student will especially benefit from major experimental instruments being developed at ONERA for classical free-space optical telecommunication (to be adapted to the CV-QKD requirements), and from state-of-the-art QKD and more generally quantum communication experiments performed at LIP6 in the context of large-scale collaborative projects with the European Commission and with the French national space agency (CNES).