ONERA
THE FRENCH AEROSPACE LAB

www.onera.fr

PROPOSITION DE SUJET DE THESE

Intitulé : Free space & fibered QKD with untrusted nodes: strategies to overcome channel impairments

Référence : **PHY-DOTA-2023-15**
(à rappeler dans toute correspondance)

Début de la thèse : Octobre 2023	**Date limite de candidature :** Mars 2023

Mots clés :

Quantum key distribution, free-space, optical fiber

Profil et compétences recherchées :

Master 2 or Engineering schools with majors in Physics, Optics, Quantum Physics.

Skills : Optics, quantum physics, modeling tools, notions in cryptography.

Présentation du projet doctoral, contexte et objectif :

Context:

During the last 30 years, intense efforts were made in France and around the worlds towards a future implementation of a global-scale quantum information network. In particular, quantum key distribution (QKD) is a communication method enabling two parties to share a secret key used to encrypt and decrypt the exchanged messages with information-theoretic (unconditional) security. Two major challenges are addressed to realize a large-scale deployment of QKD: enabling long-distance links and ensuring unconditional security.

As opposed to classical signal, quantum signal cannot be amplified, so that directly transmitting quantum information through optical fiber over arbitrary long distances is not possible. Satellite-based QKD is thus seen as a very promising solution to enable transcontinental communications, with remarkable developments including of course the series of experimental demonstrations based on the Micius satellite [Liao-2017] and theoretical studies addressing the impact of atmospheric turbulence [Marulanda-2021].

Security weaknesses can come from several sources. If many schemes rely on a trusted node to emit or detect the quantum signal, alternative protocols with only untrusted nodes are considered, among which the entanglement-based QKD [Zeilinger-2017]. Furthermore, in QKD systems, measurement devices can be attacked by an eavesdropper. For this reason, measurement-device independent (MDI) QKD protocols have been developed as an alternative solution, where secret keys are generated based on the time-reversed entanglement protocol, and the single photon detection is performed by a public untrusted measurement platform. Such protocols have been experimentally demonstrated first widely on fibered links, and more recently in free-space channels.

Whatever the channel, free-space or fibered, fluctuations of the environmental conditions ultimately result in transmission losses, which dramatically impact the QKD performance.

In free-space, the effect of atmospheric turbulence on the propagating quantum signal is detrimental to long distance MDI QKD link feasibility and has to be compensated, which is the topic of a few recent studies. In 2020, Cao et al [Cao-2020] experimentally demonstrated on a horizontal 19.2 km atmospheric channel how adaptive optics combined with remote synchronization and frequency locking can provide the necessary real-time compensation of these effect for MDI QKD. Following this work, Wang et al. proposed last year a feasibility study for an actual ground-satellite link [Wang-2021], especially accounting for orbital parameters, but where atmospheric turbulence impact was reduced mostly to beam wandering and beam spreading. In practice, ground-space links modeling is complex [Marulanda-2021], and promising MDI protocols imply establishing uplinks (from ground to a space relay) that are known to be challenging in terms of adaptive optics pre-compensation due to point-ahead anisoplanatism [Lognoné-2022]. Further developments are thus needed so as to establish a complete strategy of channel impairments compensation.

In terrestrial links, record lengths of fibered links have been demonstrated using a specific MDI protocol, the twin-field (TF) QKD protocol [Wang-2022], enabled in particular by active phase stabilization. In deployed fibers however, attenuation and phase fluctuations are much higher than in spools and strongly depend on

the environmental conditions. Strategies inspired from frequency metrology have been proposed, relying on phase stabilization for high precision frequency transfer, and should be explored further for large scale deployment [Clivati-2022].

Research project:

The project is to explore untrusted node QKD schemes, for free-space but also fibered terrestrial links, and propose strategies to overcome the propagation channel impairments.

In the case of free-space, the atmospheric turbulence conditions related to the two propagation channels and the resulting trade-offs on the adaptive optics design, the finite-size effects induced by the limited time during which both ground stations are within the satellite view, but also the need in high precision synchronization (~ps) for the MDI protocol have to be addressed. Besides, since MDI protocols involve pre-compensated LEO uplinks, it is planned to work on dedicated innovative adaptive optics pre-compensation schemes, in the continuity of [Lognoné-2022], so as to further limit the impact of point-ahead anisoplanatism and hence reduce uplink losses.

In the case of fibered links, exploiting the progress in the field of frequency transfer should enable to improve the phase stabilization and ultimately the QKD performance.

Environment:

The PhD student will benefit from the expertise of LIP6 in quantum information and cryptography, of ONERA in turbulence modeling, wavefront sensing and correction, and of LNE-SYRTE in time and frequency metrology. The PhD student will be able to rely on previous outputs and results of this collaboration [Marulanda-2021], including analytical and numerical tools dedicated to turbulence modeling, key extraction as well as key generation rate computation. In the case of uplink configurations, the PhD student will also benefit of our recent advances on the improvement of adaptive optics pre-compensation efficiency [Lognoné-2022].

Cao et al., "Long-distance free-space measurement-device-independent quantum key distribution", Physical Review Letters 125(26), 260503 (2020).

Clivati et al., "Coherent phase transfer for real-world twin-field quantum key distribution", Nature Communications 13, 157 (2022).

Liao et al., "Satellite-to-ground quantum key distribution", Nature 549, 43-47 (2017).

Lognoné et al., "Phase estimation at point-ahead angle for AO pre-compensated ground to GEO satellite telecoms", submitted to Optics Express (2022).

Marulanda et al., "Analysis of satellite-to-ground quantum key distribution with adaptive optics", arXiv:2111.06747 (2021).

Wang et al., "Feasibility of space-based measurement-device-independent quantum key distribution", New Journal of Physics 23, 045001 (2021).

Wang et al., "Twin-field quantum key distribution over 830-km fibre", Nature Photonics 16, 154-161 (2022).

Anton Zeilinger, Light for the quantum. Entangled photons and their applications: a very personal perspective. Physica Scripta, 92(7), 072501 (2017).

Collaborations envisagées

Eleni Diamanti (LIP6 – CNRS, Sorbonne University), Caroline Lim (LNE-SYRTE, Observatoire de Paris), Daniele Dequal (Agence Spatiale Italienne).

Laboratoire d'accueil à l'ONERA

Département : Optique et Techniques Associées

Lieu (centre ONERA) : Châtillon

Contact : Jean-Marc Conan

Tél. : 01 46 73 47 48 Email : jean-marc.conan@onera.fr

Directrice de thèse

Nom : Eleni Diamanti

Laboratoire : Laboratoire d'informatique de Paris 6 – CNRS, Sorbonne Université

Tél. : 01 44 27 83 12

Email : eleni.diamanti@lip6.fr

Pour plus d'informations : https://www.onera.fr/rejoindre-onera/la-formation-par-la-recherche