ONERA
THE FRENCH AEROSPACE LAB

www.onera.fr

PROPOSITION DE SUJET DE THESE

Intitulé : Untrusted node QKD : strategies to overcome free-space channel impairments

Référence : **PHY-DOTA-2024-19**
(à rappeler dans toute correspondance)

Début de la thèse : A partir d'octobre 2024	**Date limite de candidature :** Mars 2024

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, as for example entanglement-based QKD [Zeilinger-2017] and measurement-device-independent QKD (MDI) [Cao-2020], both involving a satellite relay and two ground stations, hence two free space channels.

However, in each free space channel, the amplitude and phase fluctuations induced by atmospheric turbulence hamper the preservation of indistinguishability during propagation of the emitted photons, in terms of spatial, timing and spectral modes. This is for instance detrimental to long distance MDI QKD free space 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 frequency locking and synchronization of the ground stations at the level of few tens of ps can provide real-time compensation of these effect for MDI QKD. Results were promising but limited to very low key rates, which could be enhanced by improving the accuracy and stability of time and frequency synchronization. Especially, a dedicated all-optical synchronization approach has been demonstrated in [D'Auria-2020] over 100 km. Also, Wang et al. proposed 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], especially when two channels are involved. Besides, 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-2023]. Further developments are thus needed so as to establish a complete strategy of channel impairments compensation for future QKD networks.

Research project:

The project is to explore free-space untrusted node QKD schemes (entangled-based and MDI) so as to propose strategies to overcome the propagation channel impairments.

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 uplinks, it is planned to work on dedicated innovative adaptive optics pre-compensation schemes, in the continuity of [Lognoné-2023], so as to further limit the impact of point-ahead anisoplanatism and hence reduce uplink losses.

In-lab experimental demonstrations are also planned either with a simple channel emulation with Variable Optical Attenuators or with our more realistic in lab turbulence emulator PICOLO coupled to an adaptive optics system. Comparison of in-lab and theoretical performance is considered as an essential step towards the ground-space demonstrations planned in the next decade (see for instance ESA project SAGA).

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 synchronisation. 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].

*Y. **Cao** et al., "Long-distance free-space measurement-device-independent quantum key distribution", Physical Review Letters 125(26), 260503 https://doi.org/10.1103/PhysRevLett.125.260503 (2020).*

*V. **D'Auria** et al., "A universal, plug-and-play synchronisation scheme for practical quantum networks", npj Quantum Information 6, 21 https://doi.org/10.1038/s41534-020-0245-9 (2020).*

*S.-K. **Liao** et al., "Satellite-to-ground quantum key distribution", Nature 549, 43-47 https://doi.org/10.1038/nature23655 (2017).*

*P. **Lognoné**, J.-M. Conan, G. Rekaya Ben Othman, and N. Védrenne, "Phase estimation at the point ahead angle for AO pre compensated ground to GEO satellite telecoms", Optics Express https://doi.org/10.1364/OE.476328 (2023a).*

*V. **Marulanda** Acosta, D. Dequal, M. Schiavon, A. Montmerle-Bonnefois, C. B. Lim, J.-M. Conan, E. Diamanti, "Analysis of satellite-to-ground quantum key distribution with adaptive optics", https://arxiv.org/abs/2111.06747 (2021).*

*X. **Wang** et al., "Feasibility of space-based measurement-device-independent quantum key distribution", New Journal of Physics 23, 045001 https://doi.org/10.1088/1367-2630/abf534 (2021).*

*A. **Zeilinger**, Light for the quantum. Entangled photons and their applications: a very personal perspective. Physica Scripta, 92(7), 072501 https://doi.org/10.1088/1402-4896/aa736d (2017).*

Collaborations envisagées :

Co-encadrement par Caroline Lim (LNE-SYRTE, Observatoire de Paris), collaborations envisagées avec Daniele Dequal (ESA), Sébastien Tanzilli et Olivier Alibart (INPHYNI).

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 : 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