Titre : Analyse de sécurité de la distribution quantique de clés à variables continues dans des scénarios réalistes

Title: Security analysis of continuous-variable quantum key distribution in realistic scenarios

Directeur de thèse/Thesis director: Eleni Diamanti, LIP6, CNRS, Sorbonne Université
Co-directeur de thèse/ Thesis co-director: Philippe Grangier, Laboratoire Charles Fabry, CNRS, Institut d'Optique Graduate School, Université Paris Saclay

Thesis subject:
The thesis is situated in the field of quantum information and in particular quantum cryptography. A central application in this field is quantum key distribution (QKD), which allows two parties to share a secret key that can be subsequently used for message exchange, even in the presence of eavesdroppers with unlimited power. This is impossible by classical means. Continuous-variable (CV) QKD, where the key information is encoded on the quadratures of the electromagnetic field, is particularly appealing from a practical point of view in that it only requires technology compatible with coherent optical communications. Advanced systems leveraging such technology, and in particular the modulation of quantum states according to large discrete constellations as well as digital signal processing techniques, have been developed by our group, with excellent performance.

Such experimental advances also bring new theoretical questions that need to be addressed regarding the security of the corresponding implementations. In particular, an important open question, which will be tackled in this thesis, is the proof of security for CV-QKD with discrete modulation, when finite-size effects are taken into account. Indeed, current security proof techniques apply to asymptotic limits or to very small constellations that do not give a compelling performance in terms of secret key rate and range. Extending such proofs is crucial for guaranteeing the security of current implementations and will require the use of a range of mathematical, both analytical and numerical, tools.

Advancing towards a comprehensive theoretical framework for modern CV-QKD systems will also allow us to tackle the issue of practical security, which refers to side channels that may be inadvertently available to the eavesdropper hence opening the way to security breaches. Such attacks may require physical access to the QKD hardware or simply to third-party software operated by the QKD systems. Their goal is to allow the eavesdropper to change the physical behavior or central parameters of the system to allow for an attack. The analysis of such attacks can be extremely subtle and requires an in-depth understanding and modeling of the fundamentals of the implemented protocol. Identifying such vulnerabilities can guide suitable countermeasures and is an important step towards certification of QKD technology, which is presently a major objective in the field.

Additional remarks:
The thesis project is situated in the context of the industry-academic collaborative project QKISS, which is part of the ambitious EuroQCI project, aiming at the deployment of a quantum secured communication infrastructure on the European continent in the next years. The thesis director and co-director are partners in QKISS. The thesis is also situated in

the context of a joint collaboration between the hosting academic lab at LIP6 and the French Ministry of Defense (Ministère des Armées), regarding in particular the analysis of side-channel attacks. The PhD student will directly benefit from these collaborations, and also from the multiple associated interactions and activities.

The thesis project is primarily of theoretical nature. The subject requires knowledge in classical and quantum information theory, cryptography, while notions in optics, signal processing and hardware security are also useful.