Offre de stage de recherche
Cryptographie quantique avec des variables continues

En utilisant la physique quantique, la cryptographie quantique cherche à implémenter des primitives cryptographiques dépassant les limites de la cryptographie classique. L'exemple le plus éminent est la distribution quantique de clefs (QKD, pour Quantum Key Distribution), initiée en 1984 par Bennett et Brassard, qui arrive aujourd'hui à maturité avec des systèmes commerciaux déjà disponibles.

Le principe de la QKD est qu'un espion ne peut pas acquérir de l'information sur les signaux quantiques envoyés sans introduire un surplus détectable de bruit. À la fin du protocole, Alice et Bob possèdent deux clefs identiques et secrètes, qui, utilisées comme un masque jetable (one-time pad), permettent de communiquer de façon sécurisée. Contrairement à la cryptographie classique, la QKD ne fait pas d'hypothèse sur la puissance de calcul (même quantique) de l'attaquant et offre donc une sécurité inconditionnelle.

L'information peut être encodée dans des variables discrètes (DV QKD, avec la polarisation des photons) ou continues (CV QKD, avec les quadratures du champ électromagnétique, proposée par Grosshans et Grangier en 2001 [1, 2]). La CV QKD peut notamment être implémentée avec des équipements télécoms standard et être multiplexée en longueur d'onde avec des signaux classiques.

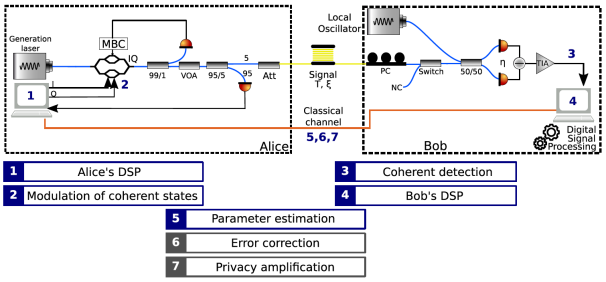

Figure 1: Le système CV QKD implémenté dans notre laboratoire. [3]

Durant ce stage, nous allons nous intéresser aux aspects théoriques de la cryptographie quantique avec des variables continues. Selon les préférences du candidat ou de la candidate, le stage pourra se concentrer sur les preuves de sécurité (plutôt mathématiques, basées sur la théorie quantique de l'information), la sécurité de l'implémentaton et les attaques par canaux cachés (plutôt physique), ou la réconciliation de l'information et les codes correcteurs d'erreurs (plutôt informatique).

Outre la CV QKD, nous pourrons aussi aborder la DI QKD (Device Independent QKD), qui, en utilisant la violation d'inégalités de Bell, permet de considérer que les dispositifs d'Alice et Bob sont contrôlés par l'adversaire et qui est donc insensible aux attaques par canaux cachés. Enfin, nous pourrons aussi travailler sur d'autres primitives cryptographiques comme l'argent quantique.

Un niveau M2 en physique, mathématiques, informatique ou ingénierie (stage de césure ou de fin d'études) est attendu. Ce stage ne pourra pas être directement suivi d'une thèse de doctorat, sauf éventuellement un an après.

Le stage aura lieu dans l'équipe Quantum Information du LIP6, et se fera en collaboration avec Philippe Grangier de l'IOGS.

Références

[1] Frédéric Grosshans et Philippe Grangier. "Continuous variable quantum cryptography using coherent states". In : (2001). Publisher: arXiv Version Number: 2. DOI : 10.48550/ARXIV.QUANT-PH/0109084. URL : https://arxiv.org/abs/quant-ph/0109084 (visité le 30/09/2024).

[2] Fabian Laudenbach et al. "Continuous-Variable Quantum Key Distribution with Gaussian Modulation – The Theory of Practical Implementations". en. In : *Advanced Quantum Technologies* 1.1 (août 2018). arXiv:1703.09278 [quant-ph], p. 1800011. ISSN : 25119044. DOI : 10.1002/qute.201800011. URL : http://arxiv.org/abs/1703.09278 (visité le 06/09/2023).

[3] Yoann Piétri et al. *QOSST: A Highly-Modular Open Source Platform for Experimental Continuous-Variable Quantum Key Distribution*. en. arXiv:2404.18637 [quant-ph]. Mai 2024. URL : http://arxiv.org/abs/2404.18637 (visité le 30/09/2024).

Professeure référente	Eleni Diamanti
Laboratoire	LIP6 (Sorbonne Université - CNRS)
Lieu	4 place Jussieu 75252 Paris Cedex 05
Date	Second semestre, année académique 2024-2025
Contacts	Eleni.Diamanti@lip6.fr, Alexis.Rosio@lip6.fr