Sujet de stage M2 – Étude de la consommation énergétique et optimisation d'une chaîne de traitement pour la Distribution Quantique de Clés à Variables Continues

Encadrants : Yoann Piétri et Adrien Cassagne

Laboratoire LIP6, équipes QI et ALSOC, Paris

Contexte

Les technologies quantiques, c'est-à-dire l'application des lois de la mécanique quantique à des fins technologiques, est un domaine en plein essor [1]. Parmi les technologies les plus matures, on retrouve **la Distribution Quantique de Clé (*Quantum Key Distribution*, QKD), qui permet d'échanger des clés cryptographiques entre deux utilisateurs de confiance.** Ces clés peuvent être ensuite combinées avec des algorithmes de chiffrement avec sécurité parfaite pour atteindre des communications invulnérables.

Néanmoins, dans le domaine des technologies quantiques, **des initiatives s'élèvent pour l'estimation et l'optimisation des aspects énergétiques de ces technologies** [1]. Bien que certains travaux existent dans le domaine du calcul quantique, les aspects énergétiques des communications quantiques restent peu étudiés, alors que la question est centrale à l'heure où les premiers systèmes commerciaux commencent à être déployés. Ainsi, **une analyse énergétique est cruciale pour le passage à l'échelle de réseaux de communication quantique**.

Une première étude a permis de mettre en lumière certains compromis et de proposer une comparaison entre les deux grandes familles de QKD [2] : à savoir, les protocoles à variables discrètes (DV), qui encodent l'information sur des propriétés des photons uniques et **les protocoles à variables continues (CV)**, qui encodent l'information sur les quadratures du champ électromagnétique, et utilisent des détecteurs cohérents. Ces derniers sont hautement efficaces à température ambiante et ont un coût énergétique largement réduit par rapport aux détecteurs de photons uniques.

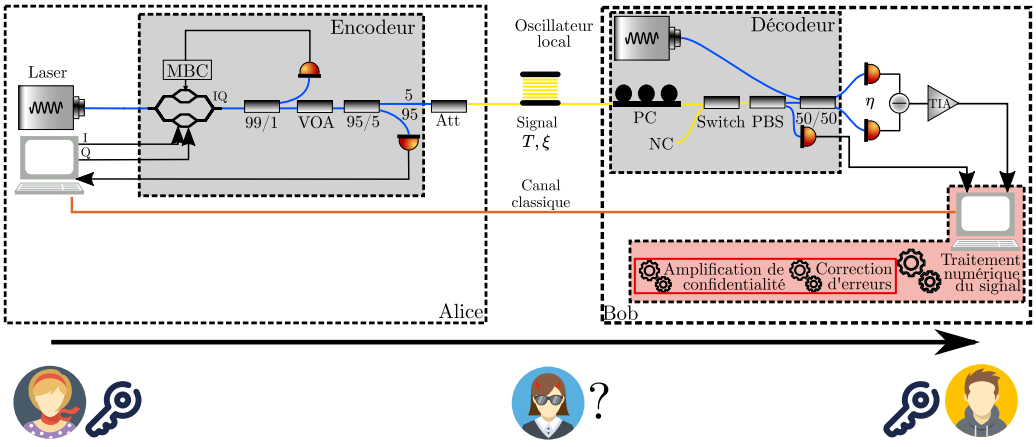

Figure 1 – Schéma d'implémentation d'un système CV-QKD. La couche physique est composée d'une source, d'un encodeur, d'un décodeur et d'un détecteur. La couche logicielle est composée d'une chaîne de traitement numérique du signal, et des algorithmes de correction d'erreurs et d'amplification de confidentialité.

Cette première étude se base seulement sur la partie *hardware* quantique. Or, les protocoles de QKD ont aussi **une partie algorithmique "classique", comprenant tout particulièrement la correction d'erreurs et l'amplification de confidentialité** (voir Fig. 1). Ainsi, l'analyse énergétique de la partie "classique" de la QKD est une étape nécessaire pour pouvoir comparer les différents systèmes.

Objectifs

L'objectif principal de ce stage et de **mettre en œuvre des techniques permettant de quantifier la consommation énergétique d'un système complet de CV-QKD**. La partie *hardware* quantique a déjà

1. "À la découverte des technologies quantiques" par Eleni Diamanti (équipe QI, LIP6) et Olivier Ezratty (2021) : `https://youtu.be/Hn6Gs-bqdOY?si=cg8O7eZq-36xnXpx`

fait l'objet d'une précédente étude et le ou la stagiaire viendra la compléter avec une analyse sur les algorithmes dits "classiques". En ce sens, **des compétences sur les technologies quantiques ne sont pas obligatoires**.

Le ou la stagiaire aura accès à des plateformes expérimentales à l'état de l'art pour la Distribution Quantique de Clé, la correction d'erreurs et les mesures énergétiques, qui lui permettront d'effectuer ces mesures dans diverses configurations et avec divers paramètres. Typiquement, le ou la stagiaire travaillera sur **des nœuds de calcul équipés de CPU multi-cœurs et de GPU**. Pour la partie énergétique, le ou la stagiaire sera amené à utiliser une plateforme de mesure novatrice à haute résolution, spécialement conçue en interne.

Le stage se décompose en trois grandes étapes :

1. Avec l'aide de ses encadrants, **le ou la stagiaire mettra en place une chaîne de communication complète pour la CV-QKD**. Pour cela, il s'appuiera sur des logiciels à code source ouvert comme AFF3CT [3], Cryptomite ou QOSST [4]. Dans cette tâche, le ou la stagiaire montera en compétence sur le système de communication étudié.
2. **Le ou la stagiaire comparera la chaîne de traitement sur différentes plateformes matérielles en terme de débit et de consommation énergétique**. Il ou elle pourra par exemple évaluer la consommation de différents composants (comme des CPU ou des GPU). Des compromis entre vitesse de calcul et consommation énergétique sont attendus.
3. Fort des résultats précédents, **le ou la stagiaire proposera des optimisations sur la chaîne de traitement**. Pour cela, il ou elle pourra s'appuyer sur des techniques de programmation parallèle comme les instructions SIMD ou la programmation multi-thread.

Enfin, le ou la stagiaire participera à la conception d'un poster et d'un article scientifique pour présenter ses résultats.

Environnement de travail

Le ou la stagiaire sera à l'intersection de deux équipes de recherche. QI, d'une part, est une équipe spécialisée dans l'information quantique et, entre autres, les systèmes de communications quantiques expérimentaux. Et ALSOC, d'autre part, est une équipe portée sur les aspects matériels et logiciels des systèmes embarqués au sens large. Le ou la candidate profitera donc de cette double expertise. Le stage propose une problématique majeure qui pourrait avoir des répercutions dans le monde de la recherche d'abord, puis dans celui de l'industrie ensuite. En ce sens, le ou la candidate retenu(e) intégrera un environnement de recherche au sein du laboratoire LIP6. **Le ou la stagiaire pourra interagir avec les doctorant(e)s des équipes de recherche**. En particulier, deux doctorants travaillent actuellement sur l'implémentation de systèmes CV-QKD mais pas du point de vue de la consommation énergétique.

Compétences attendues

— Curiosité scientifique
— Langages C/C++ et Python
— Environnement Unix
— Notions en programmation parallèle (threads POSIX, OpenMP, StreamPU, ...)
— Notions en programmation SIMD (AVX, NEON, MIPP, ...)
— Gestionnaire de version (Git)

Candidater : Merci d'envoyer un e-mail aux deux encadrants, à savoir yoann.petri@lip6.fr et adrien.cassagne@lip6.fr, contenant un CV avec au minimum les notes de M1 et de M2.

Références

[1] Alexia Auffèves : Quantum technologies need a quantum energy initiative. *PRX Quantum*, 3:020101, Jun 2022.

[2] Raja Yehia, Yoann Piétri, Carlos Pascual-García, Pascal Lefebvre et Federico Centrone : Energetic analysis of emerging quantum communication protocols, 2025.

[3] Adrien Cassagne, Olivier Hartmann, Mathieu Léonardon, Kun He, Camille Leroux, Romain Tajan, Olivier Aumage, Denis Barthou, Thibaud Tonnellier, Vincent Pignoly, Bertrand Le Gal et Christophe Jégo : Aff3ct : A fast forward error correction toolbox ! *SoftwareX*, 10:100345, 2019.

[4] Yoann Piétri, Matteo Schiavon, Valentina Marulanda Acosta, Baptiste Gouraud, Luis Trigo Vidarte, Philippe Grangier, Amine Rhouni et Eleni Diamanti : Qosst : A highly-modular open source platform for experimental continuous-variable quantum key distribution. *Quantum*, 8:1575, décembre 2024.