Architecture FPGA pour distribution quantique de clés à variables continues

Coordinateurs : Eleni Diamanti (QI) - Bertrand Granado (SYEL)

Axes transverses référencés:

- Axe “Architecture, systèmes et réseaux” (ASN)
- Axe “Sécurité, sûreté et fiabilité” (SSR)

Équipes participantes: QI, SYEL

1 Noms des personnes impliquées par équipe

- Eleni DIAMANTI (QI, Directrice de Recherche, CNRS)
- Bertrand GRANADO (SYEL, Professeur, Sorbonne Université)
- Amine RHOUNI (SYEL et QI, Ingénieur de Recherche, CNRS)
- Julien DENOULET (SYEL, Maître de Conférences, Sorbonne Université)
- Matteo SCHIAVON (QI, Post-Doctorant, Sorbonne Université)
- Yoann PIÉTRI (QI, Doctorant, Sorbonne Université)

2 Descriptif du projet

Les données sont un aspect fondamental du monde contemporain. Elles sont très souvent porteuses d'informations sécrètes, confidentielles ou simplement privées. Leur transmission doit être sécurisée et il apparaît crucial d'avoir des systèmes à la fois pratiques et efficaces pour effectuer cette tâche. La distribution quantique des clés (en anglais *Quantum Key Distribution, QKD*) représente un tel système : elle permet d'échanger des clés cryptographiques avec une sécurité dite inconditionnelle – indépendante de la puissance de calcul d'un acteur malveillant qui attaque le système – basée sur les lois de la physique quantique. Parmi les différents protocoles qui ont étés proposés pour effectuer cette tâche, les protocoles à variables continues (en anglais, *continuous variables, CV*) présentent l'avantage de pouvoir s'appuyer sur l'utilisation des composants et des techniques développés pour les communications optiques classiques, permettant d'atteindre de très hauts débits avec un coût maîtrisé. De récents résultats obtenus par l'équipe QI du LIP6 [1] ont démontré que cette technologie est aussi efficace dans des conditions à très hautes pertes, comme dans le cas d'un canal en espace libre pour des communications spatiales ; pour ce type de canal, toutes les implémentations expérimentales jusqu'à aujourd'hui ont été effectuées avec des technologies QKD basées sur des variables discrètes. Ces résultats ont justifié l'inclusion d'un transmetteur QKD à variables continues dans le projet européen QUDICE (https://qudice.eu/), qui vise la réalisation de différentes charges utiles quantiques pour micro-satellites. L'équipe QI du LIP6 est responsable de la conception, la construction et la validation de cette charge utile.

Un défi fondamental pour la construction d'un transmetteur CV-QKD est la mise en place d'un système de contrôle qui gère les différentes composants et réalise le traitement du signal requis pour passer des symboles bruts, issus d'un générateur quantique de nombres aléatoires, aux signaux électriques à envoyer à un modulateur optique.

Un système de ce type a été l'objet d'un premier prototype, implémenté sur ordinateur [2], qui permet d'effectuer toutes les étapes requises pour l'estimation des performances du protocole. Cependant, ce prototype effectue lentement les opérations de traitement du signal ; pour un système opérationnel, qu'il soit terrestre ou satellitaire, il est nécessaire de concevoir une architecture spécialisée à l'aide d'un système micro-électronique intégrée au sein d'un FPGA.

L'objectif du présent projet est la conception de cette architecture, intégrant le contrôle et le traitement du signal nécessaire pour un transmetteur de distribution quantique de clés à variables continues, en utilisant des FPGA. L'intégration en temps réel d'algorithmes de traitements du signal est une des spécialité de l'équipe SYEL dont les membres apportent au projets leur compétences et expertises pour définir et concevoir l'architecture pour la mise en oeuvre du système à l'aide de FPGA qui sera utilisé dans le cadre du projet QUDICE. Ce système sera testé avec le système CV-QKD présent dans le laboratoire de l'équipe QI. Les résultats obtenus pourront donner lieu à une publication scientifique.

3 Importance du projet pour le LIP6

Ce projet s'inscrit dans l'effort pour le développement des nouvelles technologies quantiques, qui a été la cible d'importants investissements au niveau national et européen.

L'équipe d'information quantique (QI) du LIP6 est à l'avant-garde dans ces nouvelles technologies, avec une longue expérience dans le développement de systèmes CV-QKD, dans le cadre de nombreux projets nationaux et européens. Un de ces projets, QUDICE, est centré sur le développement d'un transmetteur de cryptographie quantique à variables continues pour satellite. La mise en place d'un tel système nécessite la réalisation d'un système de contrôle et traitement des données sur FPGA, qui représente un des domaines d'expertise de l'équipe SYEL du LIP6.

L'équipe SYEL est une équipe travaillant sur la définition et la conception d'architectures de systèmes électronique pour le traitement du signal et des images, en utilisant notamment des FPGA. Ses travaux pour la physique des hautes énergies avec des contraintes de traitements de l'ordre de 25 nano-secondes [3], les systèmes basés sur des FPGA tolérants aux radiations [4] ou pour des applications bio-médicales avec de fortes contraintes d'intégration (temporelle, énergétique ou de volume) [5] lui ont permis d'être reconnue au niveau national et international.

L'objectif du présent projet est d'exploiter cette complémentarité d'expertises au sein du LIP6 pour démarrer un nouvel axe de recherche dans le domaine de l'électronique spatiale pour le quantique. Cet axe de recherche a le potentiel de doter le LIP6 des compétences dans les domaines du quantique et du spatial, deux secteurs stratégiques qui sont déjà au centre de l'intérêt des plusieurs acteurs institutionnels et dont l'importance semble destinée à croître dans les années qui viennent. Ceci sera la base pour la recherche des financements pour une thèse visant à étudier la mise en oeuvre de systèmes FPGA résistants aux erreurs introduites par l'exposition aux radiations et les techniques pour tester leur efficacité, toujours dans le cadre des applications pour la cryptographie quantique.

4 Sujet de stage

Titre du stage: Conception d'un système basé sur FPGA pour la distribution quantique de clés à variables continues à travers un lien satellite-terre

Sujet: Entre les différents technologies quantiques, la distribution quantique des clés représente celle qui présente le plus haut niveau de maturité. L'utilisation de protocoles à variables continues permet

d'atteindre des très hautes performances avec les composants utilisés dans les télécommunications classiques. L'équipe QI du LIP6 a déjà développé dans ses laboratoires un système complet de distribution quantique de clés à variables continues (CV-QKD), contrôlé par une paire d'ordinateurs en charge du traitement du signal et de la communication avec la partie optique en utilisant des convertisseurs analogique-numérique. Une étape fondamentale pour le déploiement d'un tel système dans le monde réel et pour des liaisons satellites est la réalisation d'un système de contrôle embarqué. L'objectif de ce stage est la définition et la conception d'une architecture électronique pour la mise en place du contrôle et du traitement de données pour la partie transmetteur d'un système de distribution quantique de clés à variables continues. Cette architecture sera intégrée au sein d'un FPGA. L'étudiant ou étudiante travaillera en collaboration étroite avec l'équipe QI, qui fournira les compétences nécessaires sur la distribution quantique des clés et sur les besoins de traitement de données et de contrôle pour le transmetteur, et avec l'équipe SYEL, qui donnera les compétences nécessaires à la définition et la conception d'architectures électronique sous contraintes et leur mise en oeuvre sur FPGA. Il ou elle mettra en oeuvre le système de contrôle et de traitement des données sur une carte FPGA et le testera en utilisant le transmetteur CV-QKD présent au sein du laboratoire LIP6. Ce stage représente le premier pas vers la réalisation d'un système de communication quantique embarqué utilisant un FPGA pour satellite.

Une suite à ce stage est envisagée dans le cadre d'une thèse, qui aura entre autre pour objet d'étudier les techniques pour rendre l'architecture définie résistantes aux erreurs dûs aux radiations.

Lieu: LIP6, Campus Pierre et Marie Curie, Sorbonne Université

Encadrants: Eleni DIAMANTI (QI), Bertrand GRANADO (SYEL), Amine RHOUNI (SYEL/QI), Julien DENOULET (SYEL)

References

[1] Valentina Marulanda Acosta, Daniele Dequal, Matteo Schiavon, Aurélie Montmerle-Bonnefois, Caroline B. Lim, Jean-Marc Conan, and Eleni Diamanti. Analysis of satellite-to-ground quantum key distribution with adaptive optics. *arXiv:2111.06747 [quant-ph]*, 2021.

[2] Yoann Piétri, Luis Trigo Vidarte, Matteo Schiavon, Philippe Grangier, Amine Rhouni, and Eleni Diamanti. Cv-qkd receiver platform based on a silicon photonic integrated circuit. In *Optical Fiber Communication Conference (OFC) 2023*, page M1I.2. Optica Publishing Group, 2023.

[3] Jean-Christophe Prévotet, Bruce Denby, Patrick Garda, Bertrand Granado, and Christian Kiesling. Hardware solutions for implementation of neural networks in high energy physics triggers. In *ESANN*, pages 349–356, 2002.

[4] Fakhreddine Ghaffari, Olivier Romain, and Bertrand Granado. Mitigation transient faults by backward error recovery in sram-fpga. *Radiation Effects on Integrated Circuits and Systems for Space Applications*, pages 249–276, 2019.

[5] Orlando Chuquimia, Bertrand Granado, Xavier Dray, and Andrea Pinna. *Hand Crafted Method: ROI Selection and Texture Description*, pages 49–58. Springer International Publishing, Cham, 2021.