PRD – Thèse CIFRE iXblue
Directrice de thèse : Eleni Diamanti
Enbcadrant iXblue : Baptiste Gouraud
Communication quantique cohérente en régime quantique

Objectif de la thèse :

L'objectif de cette thèse est de mettre en œuvre les outils des télécommunications optiques cohérentes à très faible puissance optique pour réaliser des liens cryptographiques dont la sécurité est assurée par les lois fondamentales de la physique quantique. Elle propose d'étudier des systèmes photoniques de distribution quantique de clé basés sur des variables continues (CV-QKD) pour des systèmes de communications sur fibre optique. Les travaux proposés incluent la conception et le développement du système, la démonstration du protocole dans une plateforme compatible avec des liens optiques et des composants existants ainsi que des démonstrations de terrain. Elle s'inscrit dans le cadre du développement de l'infrastructure de communication quantique européenne (EuroQCI) via le projet QKISS qui regroupe deux entreprises, iXblue avec ses compétences en photoniques et Thales avec son expertise en cybersécurité, et des chercheurs pionniers de la CV-QKD (Eleni Diamanti, Philippe Grangier et leurs équipes) pour produire des systèmes industriels complets de cryptographie quantique.

Etat de l'art et hypothèses :

Dans la foulée de la quatrième révolution industrielle où les données sont collectées, transférées et stockées dans des réseaux à l'échelle mondiale, la cybersécurité et la cryptographie sont de la plus haute importance. Par exemple, des technologies telles que l'Internet des Objets (IoT), l'Intelligence Artificielle (IA) ou la Blockchain augmentent le trafic de données. Parallèlement à cette évolution des technologies, le fonctionnement quotidien des entreprises, des administrations et des particuliers (transactions de données personnelles financières et sanitaires, domotique et automobile, cloud computing ...) est de plus en plus confronté à la transmission de données sensibles - voire critiques - qui nécessitent une protection, notamment contre les menaces à sa confidentialité à long terme.

Un modèle de sécurité a émergé ces dernières années comme une alternative aux modèles cryptographiques classiques reposant sur la difficulté de certains calculs mathématiques et qui offrent une sécurité dite algorithmique. Il s'agit de la cryptographie quantique, ou plus précisément de la distribution quantique de clé (QKD, Quantum Key Distribution, en anglais) [1]. Ce modèle exploite les principes fondamentaux de la physique quantique pour offrir une sécurité inconditionnelle, c'est-à-dire une sécurité garantie contre des adversaires sans limite sur leur capacité de calcul. La QKD est en effet robuste face à des attaques par un ordinateur quantique universel, un processeur ultrapuissant. Un tel processeur n'existe pas encore mais de gros investissements sont actuellement déployés pour son développement. Les protocoles cryptographiques actuels sont vulnérables face à de telles attaques, et des données sensibles qui doivent rester secrètes pendant plusieurs années sont donc exposées. En réponse à cette menace, le domaine de la cryptographie post-quantique, qui prône l'étude de nouveaux algorithmes classiques résistants aux attaques quantiques, est en plein développement. Cependant, malgré l'intérêt de tels algorithmes pour les communications à

haute sécurité, ils resteront toujours sujet à des avancées futures rendant obsolètes leurs hypothèses de complexité. Il est donc crucial de développer en parallèle des solutions basées sur la QKD pour sécuriser de façon pérenne la transmission des données à travers les canaux globaux de communication.

Des efforts scientifiques et d'ingénierie importants ont permis ces dernières années le développement des systèmes photoniques de QKD extrêmement performants [2], y compris dans des réseaux de fibre optique déployée [3]. L'équipe académique de Eleni Diamanti à Sorbonne Université (SU), mène les recherches dans ce domaine depuis plusieurs années. Les systèmes de QKD développés par cette équipe sont basés sur des variables dites continues (CV). La cryptographie quantique à variables continues (CV-QKD), présente d'importants avantages par rapport aux autres protocoles QKD dits à variables discrètes (DV-QKD). Dans les protocoles CVQKD, l'information de la clé secrète est codée dans des propriétés du champ électromagnétique des états cohérents comme ceux émis par des lasers. Ils utilisent ainsi des composants standards des télécommunications optiques, bénéficiant de leur faible coût et de leur grande fiabilité, permettant d'obtenir des débits de clé secrète élevés et s'affranchissant en particulier du besoin de détecteurs de photons uniques de la DV-QKD. Développée depuis plus de 20 ans en laboratoire [4-6], avec d'importants succès expérimentaux [7], et plus récemment son adaptation aux techniques de traitement du signal avancées des télécommunications optiques [8, 9], la CV-QKD n'a cependant pas encore atteint un état de maturité industrielle. La présente thèse doit y contribuer. Le protocole sera implémenté en conditions réelles de terrain avec un haut niveau de fiabilité, d'intégration et de performances qui sera poussé à l'état de l'art grâce aux composants de l'industrie télécom et à ses méthodes de traitement de signal. Les résultats de l'équipe incluent la première démonstration expérimentale de la CV-QKD sur des longues distances [7] ainsi que des études de sécurité pratique du dispositif développé [10, 11] travaux ayant suscité un vif intérêt dans la communauté internationale. Dans le cadre d'une collaboration avec l'Institut d'Optique et le laboratoire C2N, l'équipe a aussi développé des puces sur silicium pour la CV-QKD [12].

Les premières expériences ont été basées sur des systèmes optiques à détection cohérente avec modulation binaire de phase et propagation de l'oscillateur local, limitant à la fois le débit maximal de la clé secrète transportée et la portée du système. Les expériences plus récentes [8, 9] implémentent un système photonique à haut débit de QKD, proche du Gbit/s, basé sur des variables continues (CV) en introduisant des avancées significatives en traitement de signal et codage canal à haut débit mises en œuvre depuis une décennie dans les communications sur fibre optique avec l'avènement de la détection cohérente. Une première étape essentielle a été franchie récemment avec l'intégration de ces techniques en conditions de laboratoire, mais utilisant du matériel (générateur de signaux, oscilloscope, détecteur) trop encombrant pour un déploiement sur le terrain et bénéficiant des performances accrues du matériel haut de gamme de laboratoire. Lors de cette thèse, les systèmes seront développés directement avec un niveau d'intégration adapté au terrain et en s'adaptant aux standards de cybersécurité demandés par l'union européenne pour les communications à haut niveau de confidentialité.

Le travail contribuera à la collaboration scientifique étroite entre iXblue et le LIP6-Sorbonne Université. iXblue apportera son savoir-faire et ses ressources pour l'intégration de composants et systèmes photoniques et le LIP6 son expérience de l'optique quantique et en particulier de cryptographie quantique à variables continues. Il s'inscrira dans le cadre de projets

européens en cours et à venir. OpenQKD est un projet H2020 impliquant les deux partenaires depuis 2019 et posant les première bases de l'EuroQCI. QKISS est un autre projet qui débutera en janvier 2023 avec l'ambition de créer de nouveaux systèmes complets de cryptographie quantique répondants aux exigences de robustesses et de qualités de signaux de la QKD et aux standards stricts de la cybersécurité. Dans cette collaboration sont impliqués iXblue, leader du projet et responsable de la couche physique, Thales pour la couche logique impliquant traitement du signal, implémentation du protocole et utilisation des clé sécrètes dans un réseau télécom, ainsi que le LIP6/SU et l'institut d'optique pour leur expertise de l'optique quantique.

Cette thèse se concentre logiquement sur la couche physique du lien QKD. Le premier volant technologique essentiel concerne l'intégration de la couche opto-électronique, avec modulateurs électro-optiques, détecteurs cohérents, lasers à bas bruit de phase, gestion des signaux radiofréquences, qui doit fonctionner sur une bande de fréquence de plusieurs GHz, avec un très faible niveau de bruit et une excellente linéarité. Le second volant est le traitement numérique du signal à haut débit, avec conversion analogique-digitale en continue, mise en forme des symboles, récupération des dérives de phase et de polarisation, génération de vrais nombres aléatoires à haut débit.

[1] V. Scarani et al, "The security of practical quantum key distribution", Rev. Mod. Phys. 81, 1301 (2009).

[2] E. Diamanti, H.-K. Lo, B. Qi, Z. Yuan, "Practical challenges in quantum key distribution, npj Quantum Information 2, 16025 (2016).

[3] M. Peev et al., "The SECOQC Quantum Key Distribution network in Vienna", New J. Phys. 11, 075001 (2009).

[4] F. Grosshans and P. Grangier, "Continuous Variable Quantum Cryptography Using Coherent States," Physical Review Letters, vol. 88, p. 057902, 2002

[5] F. Grosshans et al, Nature 421, 238 (2003).

[6] E. Diamanti and A. Leverrier, "Distributing secret keys with quantum continuous variables: principle, security and implementations", Entropy 17, 6072 (2015).

[7] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution", Nature Photon. 7, 378 (2013).

[8] F. Roumestan, A. Ghazisaeidi, J. Renaudier, P. Brindel, E. Diamanti, and P. Grangier, "Demonstration of Probabilistic Constellation Shaping for Continuous Variable Quantum Key Distribution," Optical Fiber Communications Conference and Exhibition, pp. 1–3, 2021.

[9] F. Roumestan, A. Ghazisaeidi, J. Renaudier, L. Trigo Vidarte, E. Diamanti, P. Grangier, High-Rate Continuous Variable Quantum Key Distribution Based on Probabilistically Shaped 64 and 256-QAM, European Conference on Optical Communications (ECOC) 2021, paper ID 0320 (2021)

[10] P. Jouguet, S. Kunz-Jacques, E. Diamanti, A. Leverrier, "Analysis of imperfections in practical continuous-variable quantum key distribution", Phys. Rev. A 86, 032309 (2012).

[11] P. Jouguet, S. Kunz-Jacques, E. Diamanti, “Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution”, Phys. Rev. A 87, 062313 (2013).

[12] M. Persechino, M. Ziebell, N. Harris, C. Galland, D. Marris-Morini, L. Vivien, E. Diamanti, and P. Grangier, “Towards on-chip continuous-variable quantum key distribution”, in CLEO/Europe - EQEC, Munich, Germany (June 2015).

Encadrement :

La thèse sera administrativement basée dans les locaux de iXblue (contrat doctoral CIFRE). Elle sera enregistrée à l’école doctorale EDITE. L’étudiante, Manon Huguenot, sera amenée à être à 50% de son temps à Besançon (site de iXblue Photonics) et à 50% de son temps à Paris (équipe information quantique du LIP6-Sorbonne Université). La doctorante participera aux travaux commun iXblue-LIP6 déjà en cours dans le cadre de projets européens et aux réunions bimensuelles qui sont organisées dans ce cadre.

Elle sera co-encadrée par 2 chercheurs titulaires de doctorat :

- Eleni Diamanti (LIP6, Directrice de recherche CNRS, HDR), directrice de la thèse à 50%
- Baptiste Gouraud (iXblue, Dr. Ingénieur R&D), co-directeur de la thèse à 50 %

En complément, un lien étroit sera maintenu avec Philippe Grangier et son équipe (Institut d’optique à Palaiseau, CNRS) qui sont au premier plan international sur le thème de la CV-QKD, et collaborent avec le LIP6 et iXblue depuis plusieurs années. Un appui sera apporté également par Jérôme Hauden, responsable recherche et innovation à iXblue Photonics.