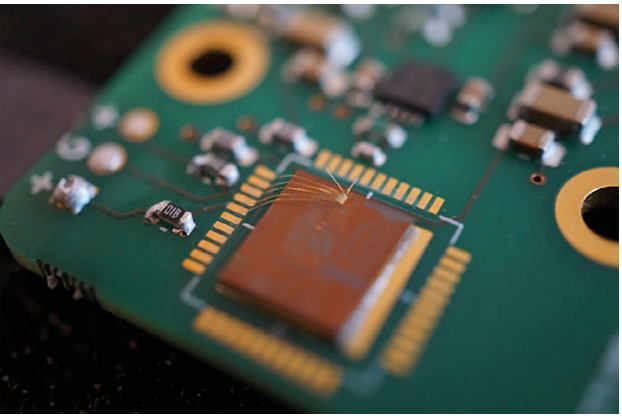
COMMUNICATIONS SÉCURISÉES AVEC DES VARIABLES QUANTIQUES CONTINUES

Yoann PIÉTRI*, Eleni DIAMANTI
LIP6 – Sorbonne Université – CNRS, 4 place Jussieu, 75005 Paris
*yoann.pietri@lip6.fr



La distribution quantique de clés est une application majeure des technologies quantiques permettant la sécurisation des communications pour des données de haute confidentialité. Son déploiement pratique dans des infrastructures de réseaux nécessite des systèmes de haute performance, compacts et robustes. Dans cet article, sont présentés les concepts de base, les performances et les défis actuels de tels systèmes basés sur le codage de l'information dans des propriétés des quadratures du champ électromagnétique.

https://doi.org/10.1051/photon/202513049

Au cœur des technologies quantiques se trouve l'utilisation de propriétés intrinsèquement quantiques telles que la superposition, l'intrication ou le principe d'incertitude pour réaliser des tâches avec un avantage par rapport à leur équivalent classique, en termes de puissance de calcul, de sécurité, de précision de mesure... Une application phare de ce domaine est la distribution quantique de clé (QKD, de l'anglais *Quantum Key Distribution*). En effet, cette famille de protocoles permet à deux utilisateurs de confiance, habituellement nommés Alice et Bob, munis d'un canal de communication quantique public, et d'un canal de communication classique, public mais authentifié, de procéder à l'échange d'une clé (*i.e.* une chaîne de bits) avec une sécurité basée non pas sur des problèmes mathématiques (et donc une sécurité calculatoire) mais sur les lois de la Physique Quantique, en particulier en utilisant le théorème de non-clonage et les relations d'incertitudes [1].

Il existe deux grandes familles de protocoles de QKD : dans la première, dite à Variables Discrètes (*Discrete Variable Quantum Key Distribution*, DV-QKD), l'information est codée sur des propriétés discrètes de photons uniques telle que la polarisation, alors que dans la deuxième, dite à Variables Continues (*Continuous Variable Quantum Key Distribution*, CV-QKD), l'information est codée sur des propriétés continues, en pratique les valeurs moyennes de quadratures du champ électromagnétique [2]. L'avantage de cette deuxième famille est double : d'une part, le protocole peut utiliser des états cohérents, qui sont relativement simples à ●●●

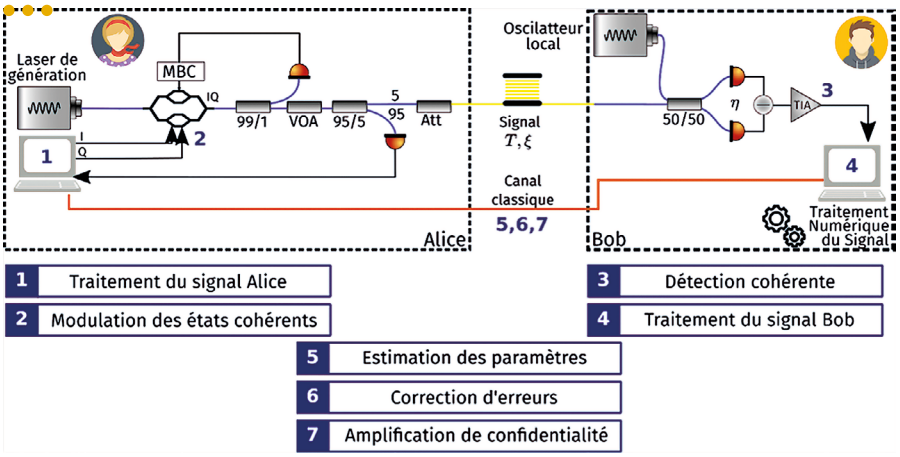


Figure 1. Schéma expérimental et étapes d'un protocole implémenté dans un système CV-QKD moderne [4]. Le traitement numérique du signal joue un rôle primordial pour la stabilité et performance du système. Les étapes de 5 à 7 suivent l'échange des états quantiques et visent l'extraction de la clé secrète finale. Le dispositif expérimental est constitué des composants des télécommunications standards. Le MBC (Contrôleur de Bias du Modulateur) permet d'asservir le modulateur sur son point de fonctionnement. Pour simplifier, le détecteur omet les équipements de calibration et de compensation de la polarisation.

créer avec un laser et à moduler en quadrature avec des dispositifs disponibles commercialement ; de l'autre, la détection de quadratures peut s'effectuer de manière efficace et à température ambiante avec des détecteurs balancés, eux aussi commercialement disponibles. De manière globale, le schéma de communication pour la CV-QKD est comparable à celui des communications cohérentes classiques, ce qui permet d'utiliser un certain nombre de composants et d'outils d'une grande maturité technologique.

LA DISTRIBUTION QUANTIQUE DE CLÉ À VARIABLES CONTINUES

La CV-QKD a été proposée pour la première fois en 1999, avec l'encodage de l'information sur l'amplitude et la phase d'états comprimés. En 2002, Grosshans et Grangier proposent un protocole dont l'encodage est basé cette fois sur les quadratures d'états cohérents, bien plus simples à générer [3]. Ces deux protocoles se basent alors sur la mesure d'une unique quadrature, et en 2004, Weedbrook et co-auteurs proposent de mesurer les deux quadratures pour augmenter l'information partagée. Bien que d'autres propositions aient été faites par la suite, comme par exemple de mesurer les deux quadratures d'états comprimés, d'utiliser des états thermiques ou une communication à deux sens, ou encore des versions indépendantes des systèmes de mesure, nous allons nous concentrer par la suite sur le protocole basé sur les états cohérents et la détection double-quadrature qui est conceptuellement simple et est utilisé largement dans des systèmes actuels. Un exemple d'un montage expérimental d'un tel système est montré dans la figure 1.

Une intuition du protocole peut être donnée en observant la figure 2.

Alice, sur la gauche, envoie un des quatre états cohérents, représentés par la croix et le bruit quantique intrinsèque sur les quadratures en rouge. L'amplitude A est reliée au nombre de photons moyens dans les états. Lorsque l'état est transmis à Bob, il y a, d'une part, une perte de photons (les valeurs moyennes se compressent alors vers l'origine, effet non représenté sur la figure) et un bruit en excès se rajoute au bruit quantique (interaction avec l'environnement, attaque par un adversaire, bruit de préparation ou de mesure...). En réalisant un grand nombre de mesures et en comparant ses résultats avec une partie des valeurs d'Alice, Bob peut estimer le facteur de perte du canal et le bruit en excès. Ces derniers peuvent alors être utilisés pour borner l'information récupérée par un espion, en faisant l'hypothèse pessimiste que toutes les pertes et tout le bruit sont dus à cet espion. Il est intuitif de voir que l'amplitude va avoir un effet sur les performances du protocole : si elle est trop élevée,

Table 1. Caractéristiques principales de protocoles de distribution quantique de clés à variables discrètes et continues.

	DV-QKD	CV-QKD
Encodage	Qubits (ou qudits) Dimension 2 (ou $n \in \mathbb{N}^*$)	Quadratures Dimension ∞
Détection	Détecteurs de photons uniques Bande passante : 100 MHz - 1GHz Efficacité modérée ou nécessite du refroidissement cryogénique Équipement spécialisé Haut coût énergétique	Détecteurs balancés (photodiodes standards) Bande passante : 1 GHz – 100 GHz Bonne efficacité à température ambiante Équipement télécom standard Faible coût énergétique
Source	Photons uniques ou Impulsion cohérente faible (états leurres)	États cohérents (ou états comprimés)
Résilience aux pertes	Résilience plus importante Record : 421 km	Résilience moins importante Record : 202.81 km
Post-traitement	Post-traitement simple	Post-traitement avancé
Intégrabilité sur puces	Transmetteur : démontré Récepteur : partiellement démontré	Transmetteur : démontré Récepteur : démontré

il est facile pour l'espion de distinguer entre les quatre états de base et de passer inaperçu ; et si elle est trop faible, il n'y aura pas assez d'information partagée entre Alice et Bob.

En pratique Alice peut moduler les valeurs moyennes des quadratures selon plusieurs manières, généralement appelés les modulations. Historiquement, la modulation de choix est la modulation Gaussienne où les valeurs moyennes des deux quadratures sont choisies selon une distribution Gaussienne. Néanmoins, inspirées des communications classiques, des modulations discrètes sont aussi considérées telles que les *Phase Shift Keying* (PSK, modulation par changement de phase), les *Quadrature Amplitude Modulation* (QAM, modulation d'amplitude en quadrature) ou encore des QAM avec mise en forme probabiliste (*Probabilistic Constellation Shaping*, PCS). D'une part, ces modulations sont les seules qui peuvent être effectivement réalisées avec des systèmes digitaux, mais, considérant que des PCS-QAM à haute densité sont très proches d'une modulation Gaussienne, des bons débits avec des modulations à faible densité permettrait aussi d'utiliser des équipements moins exigeants en termes de performances et de simplifier la correction d'erreurs. Le défi de ces modulations réside néanmoins dans les preuves de sécurité, qui sont encore un sujet actif de recherche. Le taux de génération de clé secrète dépend de plusieurs paramètres du système, en particulier de la variance de modulation d'Alice (reliée au nombre moyen de photons par symbole), de la transmittance du canal quantique, du bruit en excès, et de l'efficacité quantique et du bruit électronique du détecteur. Il dépend également de la modulation utilisée et du fait de considérer un nombre infini de symboles (dit cas asymptotique) ou, dans un cas plus réaliste, un nombre fini de symboles, ce qui nécessite l'application des termes correctifs [5].

TRAITEMENT NUMÉRIQUE DU SIGNAL POUR LA CV-QKD À HAUT DÉBIT

Depuis 2015, de nombreux efforts en CV-QKD ont eu pour objectif de transférer la complexité des systèmes de la partie optique vers des algorithmes de post-traitement. Le post-traitement, inspiré des méthodes des télécommunications classiques, permet d'augmenter le taux de répétition, réduire les interférences inter-symboles, et corriger une partie des erreurs physiques.

Une des techniques standard est maintenant d'utiliser un laser à onde continue (*Continuous Wave*, CW) et d'appliquer une mise en forme d'impulsions basée sur des filtres respectant le critère de Nyquist, et permet, en théorie, d'éliminer les interférences entre symboles. Un filtre de choix est le filtre cosinus surélevé (*Raised Cosine*, RC) ; en pratique, la plupart des systèmes implémentent ce filtre en utilisant un filtre racine de cosinus surélevé (*Root Raised Cosine*, RRC) en émission et un filtre adapté (le même) en réception.

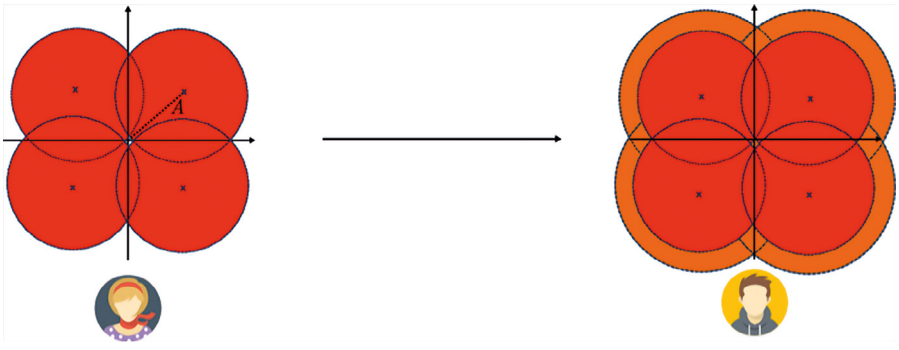
Du fait de la séparation des lasers de génération du signal et pour l'oscillateur local, comme montré dans la figure 1, des différences de fréquence et de phase existeront, et devront être corrigées. Des erreurs d'horloge peuvent aussi exister. Ces différentes notions sont regroupées sous le terme de synchronisation (en temps, en fréquence et en phase) et représentent un défi pour augmenter les taux de répétition et distances atteignables en CV-QKD. La méthode principalement adoptée aujourd'hui est d'utiliser des références classiques, appelées pilotes, multiplexées en fréquence ou en temps. Le défi majeur émerge alors d'un compromis : un bon rapport signal-à-bruit sur ces pilotes en réception permettra une bonne synchronisation mais requiert une bonne isolation de ces références par rapport au signal quantique, au risque sinon d'augmenter le bruit en excès. Des optimisations doivent alors être réalisées pour obtenir le meilleur débit de clé secrète. Les étapes du traitement numérique du signal nécessaires sont résumées dans la figure 3.

DÉFIS DE LA DISTRIBUTION QUANTIQUE DE CLÉS À VARIABLES CONTINUES

Malgré de larges avancées ces dernières années, le domaine de la QKD ne reste pas sans défis. Ces défis industriels, technologiques et scientifiques sont des sujets de recherche éminents à l'heure actuelle et nous soulignons les plus importants ci-dessous.

Augmentation du débit de clé secrète et temps réel : pour atteindre un échange de message avec une sécurité inconditionnelle, il est nécessaire que la taille de la clé soit au moins supérieure à celle de la taille du message, impliquant ainsi que le débit de la génération de clé soit supérieur à celui du débit de ● ● ●

Figure 2. Idée conceptuelle d'un protocole de QKD à variables continues où Alice et Bob utilisent une constellation de quatre états cohérents.



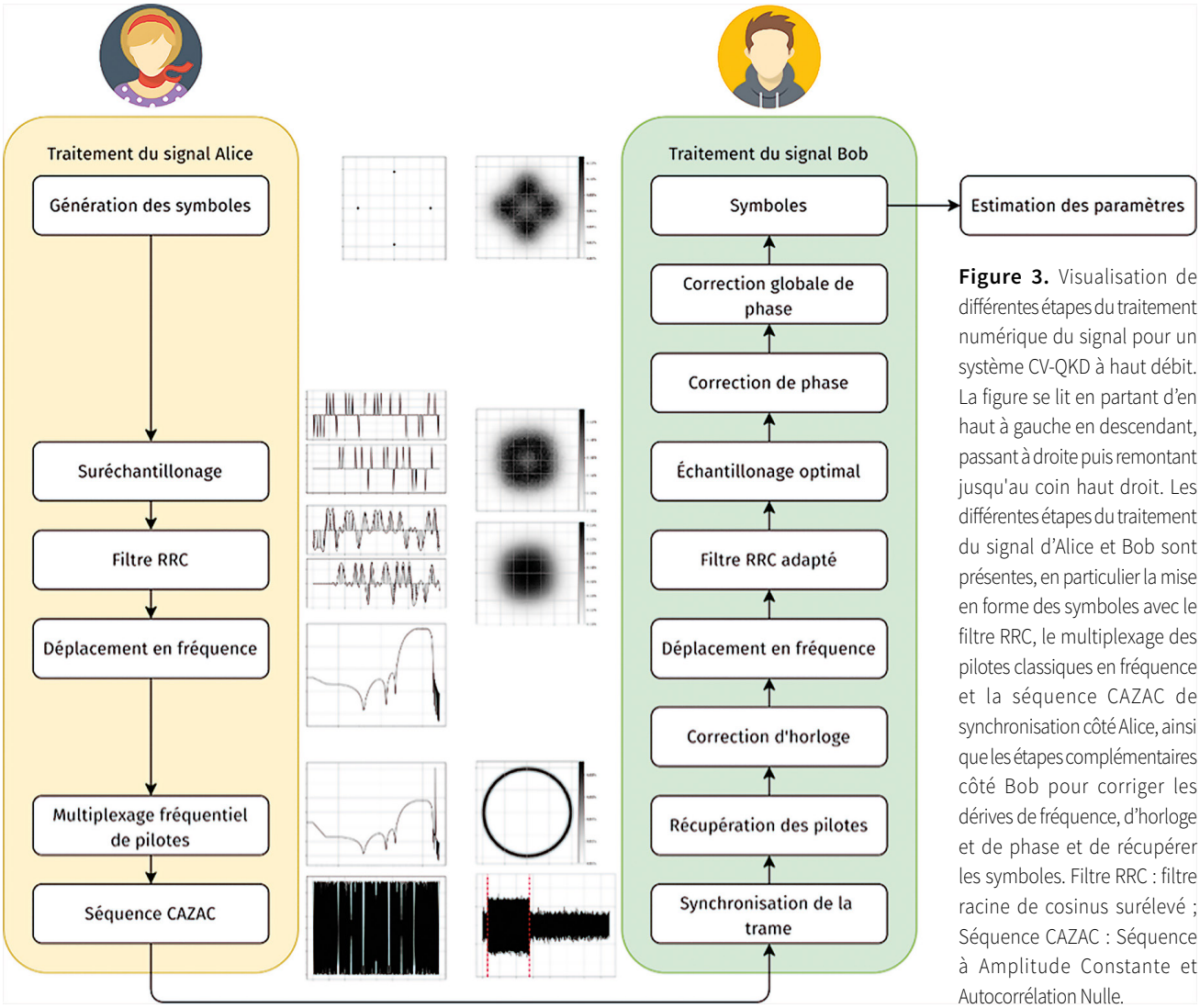


Figure 3. Visualisation de différentes étapes du traitement numérique du signal pour un système CV-QKD à haut débit. La figure se lit en partant d'en haut à gauche en descendant, passant à droite puis remontant jusqu'au coin haut droit. Les différentes étapes du traitement du signal d'Alice et Bob sont présentes, en particulier la mise en forme des symboles avec le filtre RRC, le multiplexage des pilotes classiques en fréquence et la séquence CAZAC de synchronisation côté Alice, ainsi que les étapes complémentaires côté Bob pour corriger les dérives de fréquence, d'horloge et de phase et de récupérer les symboles. Filtre RRC : filtre racine de cosinus surélevé ; Séquence CAZAC : Séquence à Amplitude Constante et Autocorrélation Nulle.

communication. L'augmentation de ce débit peut passer par plusieurs efforts (réduction des pertes et/ou du bruit, amélioration des preuves de sécurité, ...) mais passe aussi par l'utilisation même des protocoles à variables continues, qui permettent d'augmenter le taux de répétition de la source et de la détection au-dessus du Gigahertz voire des dizaines de Gigahertz. De plus, les systèmes doivent atteindre des fonctionnements en temps réel, et éliminer les goulots d'étranglement dans le post-traitement.

Augmentation de la distance : l'information quantique ne pouvant pas être copiée, les communications quantiques sont limitées, en pratiques, par les pertes induites par les canaux de communication, qui sont exponentielles avec la distance dans les fibres optiques. Dans le cas de la CV-QKD, un facteur limitant la distance est le bruit de phase entre les deux lasers utilisés dans le système. En effet, malgré l'envoi de pilotes pour corriger cette différence, il existe toujours une erreur résiduelle, qui croit lorsque le rapport signal-à-bruit de pilotes décroît. À grande distance, il devrait être possible de corriger cet effet en augmentant la puissance des pilotes émis, mais cela résulte en une augmentation du bruit induit par le pilote sur les données quantiques. Ainsi, un des axes de recherche actuels réside en l'amélioration de l'isolation entre les données quantiques et les pilotes, et l'amélioration des algorithmes de récupération de la phase. Un autre domaine très actif est celui des communications satellitaires. En effet, les pertes y sont moins importantes (à distances égales), ce qui permet d'atteindre des distances plus importantes. Néanmoins, ces communications apportent de nouveau défis, en particulier à cause des turbulences qui modifient le mode spatial (et peuvent donc limiter les efficacités de couplage) mais aussi à cause des paramètres du canal (transmittance et bruit en excès) qui sont variables et qui nécessitent donc des techniques spécialisées [6].

Réduction de la taille et coût des systèmes : une étape importante pour une adoption potentiellement plus large est la miniaturisation des systèmes avec des processus fiables. L'utilisation de composants de photonique intégrée a aujourd'hui ● ● ●

L'horizon de la QKD s'étend

Plus vite et plus loin : valorisez votre QKD avec la performance des SNSPDs.

Clavis XGR QKD

ID281 Pro SNSPD

info@idquantique.com | www.idquantique.com

un grand potentiel pour les technologies de communication quantique. La CV-QKD est, de plus, un bon candidat pour l'intégration photonique, dans la mesure où les composants nécessaires sont les mêmes que pour les communications classiques et bénéficie donc des années de recherche dans le domaine. A contrario, les systèmes DV-QKD se révèlent plus difficiles à intégrer, notamment à cause des détecteurs de photons uniques, qui doivent de surcroît être refroidis pour opérer à de bonnes efficacités à des longueurs d'ondes telecoms. Récemment, plusieurs démonstrations de systèmes intégrés pour la CV-QKD ont été démontrés à des distances de l'ordre de la dizaine à la centaine de kilomètres, principalement en utilisant des technologies compatibles avec le process CMOS (Photonique sur Silicium) [7], voir figure en début de l'article. Un défi important réside néanmoins dans l'intégration des sources lasers, qui ne sont pas possibles sur Silicium à des longueurs d'ondes telecoms et requièrent donc d'autres plateformes ou de l'hybridation.

Déploiement des systèmes compatibles avec les communications classiques : pour pouvoir être viable, les systèmes de communication quantique doivent être déployés sur des réseaux de télécommunications et l'opération de ces systèmes doit être démontrée en parallèle d'infrastructures classiques. En effet le déploiement d'une nouvelle infrastructure parallèle spécifique pour la communication quantique ne permet pas le passage à l'échelle et semble peu probable sur le long terme. Dans l'Union Européenne, cet effort prend la forme du projet EuroQCI qui a pour vocation l'établissement et l'utilisation d'un réseau de communication quantique européen. En France, des réseaux sont déployés en région Parisienne et dans la région Niçoise. Le réseau de la région Parisienne est composé de 8 nœuds reliés par 14 fibres dédiées aux applications quantiques (mais issues du réseau telecom classique). Deux systèmes CV-QKD ont été déployés sur le réseau, dont un reliant deux laboratoires académiques sur un lien de 14.64 km et avec un débit de clé secrète asymptotique de 0.85 Megabit/s. Des efforts similaires sont aussi présents dans de nombreux autres pays de l'Union Européenne et dans le monde.

Certification et standardisation des systèmes : la certification et la standardisation de systèmes est un effort indispensable pour une adoption en dehors du monde académique. En ce qui concerne la standardisation, plusieurs organismes de normalisation ont commencé à publier des normes, et un exemple particulier est l'institut européen des normes de télécommunications (ETSI) qui a un comité dédié à la QKD. La certification est, en Europe, adressée par un projet ambitieux, qui a pour vocation la création d'une autorité de certification de systèmes QKD européenne. Le défi est alors d'identifier les différentes attaques par canaux cachés, valider les potentielles contre-mesures et de prévoir des tests pour savoir si un système QKD est sujet à une attaque particulière.

Preuves de sécurité : pour atteindre une sécurité inconditionnelle, les systèmes de QKD doivent reposer sur des preuves robustes et correspondant aux implémentations pratiques. Ces preuves doivent aussi être valides en considérant un nombre fini d'états échangés et pas seulement dans la limite asymptotique (effets de taille finie). En ce qui concerne la CV-QKD, les preuves sont complètes dans le cas où la modulation est Gaussienne (que ce soit dans le cas asymptotique ou avec effets de taille finie). Lorsque des modulations discrètes sont utilisées, il existe une preuve générale dans le cas asymptotique, mais le cas fini est encore source de nombreuses recherches. Il faut s'assurer de plus que ces preuves soient composables, c'est dire que le protocole de QKD peut être composé avec un autre protocole sans compromettre la sécurité. Enfin, l'hybridation avec des protocoles de cryptographie post-quantique sera nécessaire pour l'intégration dans des systèmes modernes permettant une sécurité en profondeur.

CONCLUSION

La cryptographie quantique, et en particulier la distribution quantique de clés, est rentrée ces dernières années dans une phase de maturation technologique qui fait avancer l'ingénierie des systèmes et leurs performances de façon significative, ouvrant la voie à leur utilisation pour des cas d'usage réels à court terme. Les protocoles à variables continues sont particulièrement bien adaptés à des réseaux métropolitains et à des configurations qui requièrent des débits élevés et des conditions d'utilisation contraignantes. Adresser les défis du domaine permettra l'adoption de cette technologie pour des communications sécurisées dans des infrastructures de grande envergure.

RÉFÉRENCES

[1] V. Scarani *et al.*, Rev. Mod. Phys. **81**, 1301 (2009).

[2] E. Diamanti, A. Leverrier, Entropy **17**, 6072 (2015).

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

[4] Y. Piétri *et al.*, Quantum **8**, 1575 (2024).

[5] F. Roumestan *et al.*, Journal of Lightwave Technology **42**, 5182 (2024).

[6] V. Marulanda-Acosta *et al.*, New J. Phys. **26**, 023039 (2024).

[7] Y. Piétri *et al.*, Optica Quantum **2**, 428 (2024).