PROGRÈS ET DÉFIS POUR la cryptographie quantique

Eleni DIAMANTI
Laboratoire d'Informatique de Paris 6, CNRS, Sorbonne Université, F-75005 Paris
eleni.diamanti@lip6.fr

La cryptographie quantique, et plus particulièrement la distribution quantique de clés, promet la communication des données avec une sécurité absolue, indépendante des capacités d'un espion éventuel. Malgré des progrès significatifs, pour son utilisation dans une large gamme d'applications, des défis liés à la performance, le coût et la sécurité pratique des systèmes devront être abordés les prochaines années.

À l'heure de la quatrième révolution industrielle, où les données sont collectées, transférées et stockées dans des réseaux à l'échelle globale, la cybersécurité et la cryptographie deviennent des sujets de grande importance. Le développement des technologies telles que l'Internet des Objets, l'Intelligence Artificielle ou le Blockchain, augmente le trafic des données dans des réseaux, tandis que le fonctionnement quotidien des industries, des administrations et des individus, impliquant des transactions des données personnelles de santé ou financières, et des secrets commerciaux ou nationaux, est de plus en plus confronté à la transmission des données sensibles ou même critiques, qui nécessitent de la protection, notamment face à des menaces contre leur confidentialité à long terme. Il existe en effet des données qui doivent être gardées secrètes pendant des décennies !

La cryptographie moderne fournit des outils fondamentaux, basés sur les mathématiques et la théorie de complexité algorithmique, qui permettent la sécurisation numérique de nos données. En particulier, la cryptographie à clé publique (ou cryptographie asymétrique) permet actuellement des communications sécurisées sur Internet. Elle se base cependant sur des hypothèses calculatoires, comme la difficulté de factorisation des grands nombres pour le protocole RSA ; elle est donc de façon inhérente vulnérable aux futures avancées matérielles et algorithmiques, y compris la construction d'un ordinateur quantique de grande taille. Cette menace devenant plausible dans un horizon moyen-terme grâce à des récents progrès fulgurants, il devient crucial de faire évoluer nos pratiques cryptographiques.

Cette évolution amènera très probablement vers une combinaison des techniques classiques et quantiques [1]. La recherche pour des nouveaux algorithmes classiques résistant à l'ordinateur quantique (regroupés sous le nom de cryptographie post-quantique) est en cours, avec des résultats prometteurs. Cependant, la sécurité de tels algorithmes restera dans tous les cas calculatoire et elle devra donc être

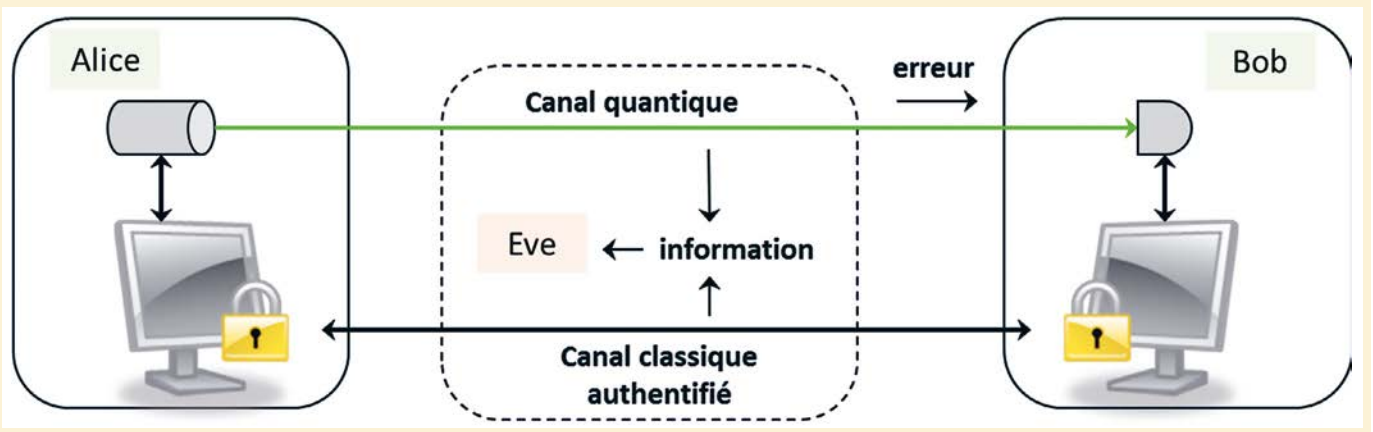

Figure 1. La distribution quantique de clés permet à un transmetteur, Alice, et un récepteur, Bob, d'échanger une clé secrète, en utilisant deux canaux de communication : un canal utilisé pour la transmission des signaux quantiques et un canal public mais authentifié utilisé pour l'échange d'informations entre les deux interlocuteurs. Si un espion potentiel, Eve, tente d'obtenir de l'information sur l'état des objets quantiques ceci induira inévitablement, grâce aux lois de la mécanique quantique, des erreurs dans la corrélation des données partagées par Alice et Bob. Celles-ci seront relevées pendant la phase de communication.

renforcée par la cryptographie quantique. L'algorithme-phare du domaine est la distribution quantique de clés (en anglais, *quantum key distribution* – QKD), qui promet, en principe, la sécurité inconditionnelle des communications reposant uniquement sur les lois de la physique (*figure 1*). En effet, la QKD est la seule méthode de génération de clé offrant une sécurité absolue dans le sens de la théorie de l'information et elle a l'avantage d'être sûre face à des attaques futures : il n'est pas possible pour un espion de conserver une copie des signaux quantiques envoyés dans un processus de QKD, en raison du théorème de non-clonage quantique.

Les applications potentielles de la cryptographie quantique incluent la garantie de sécurité dans des infrastructures critiques, les institutions financières et la défense nationale. Avec son potentiel stratégique, ce domaine joue un rôle central dans le contexte plus large des technologies quantiques et a été le sujet d'un très grand effort scientifique et d'ingénierie ces dernières années.

Les protocoles et la technologie

Comme pour tout le domaine des communications quantiques, les systèmes QKD exploitent le codage de l'information quantique dans certaines propriétés des signaux photoniques. Les deux parties qui communiquent, Alice et Bob, échangent un grand nombre de signaux par un canal physique (fibre optique ou espace libre), et des informations supplémentaires envoyées sur un canal classique public mais authentifié. Ils suivent ainsi un protocole qui aboutit à la génération d'une chaîne de bits – la clé – secrète avec un niveau de sécurité voulu au prix d'une réduction de la taille de chaîne initiale [2].

Les protocoles QKD peuvent être distingués essentiellement par la technique de détection utilisée pour extraire les informations sur la clé encodées dans les propriétés de la lumière. Des techniques de détection de photons uniques sont nécessaires pour des protocoles à variables discrètes (DV), comme le célèbre protocole BB84 et sa version à état leurre, où l'information est codée typiquement dans la polarisation ou la phase d'impulsions cohérentes atténuées simulant des vrais états à photon unique, ainsi que pour les protocoles dits à référence de phase, comme le *coherent-one-way* (COW) et le protocole à décalage de phase différentiel (DPS), où l'information est codée respectivement dans le temps d'arrivée des photons et dans la phase entre les impulsions adjacentes [2]. En outre, dans des protocoles QKD à variables continues (CV), l'information de la clé est codée dans les quadratures du champ électromagnétique quantifié, comme ceux des états cohérents, et des techniques de détection cohérente (homodyne ou hétérodyne) sont utilisées dans ce cas [3]. De tels détecteurs sont habituellement déployés dans des communications optiques classiques, ainsi l'approche CV offre la possibilité d'une mise en œuvre compatible avec les systèmes des télécommunications standards. À tous ces protocoles de type préparation-et-mesure, où Alice envoie des impulsions codées à Bob qui décode en suivant un protocole spécifique, s'ajoutent les protocoles à base d'intrication où les deux parties reçoivent les photons d'un état intriqué et exécutent des mesures appropriées [2].

En ce qui concerne les démonstrations pratiques, la performance des liaisons point-à-point est évaluée par la distance à laquelle les clés secrètes peuvent être distribuées et par le débit de génération de la clé secrète pour un niveau de sécurité donné. Le but ultime est de fournir un niveau maximal, correspondant à la sécurité contre les attaques les plus générales, avec un débit et une distance de communication qui sont compatibles avec des applications pratiques. Quelques expériences récentes ont fourni des bonnes performances et définissent l'état de l'art dans le domaine pour les liaisons fibrées [4] (*figure 2*).

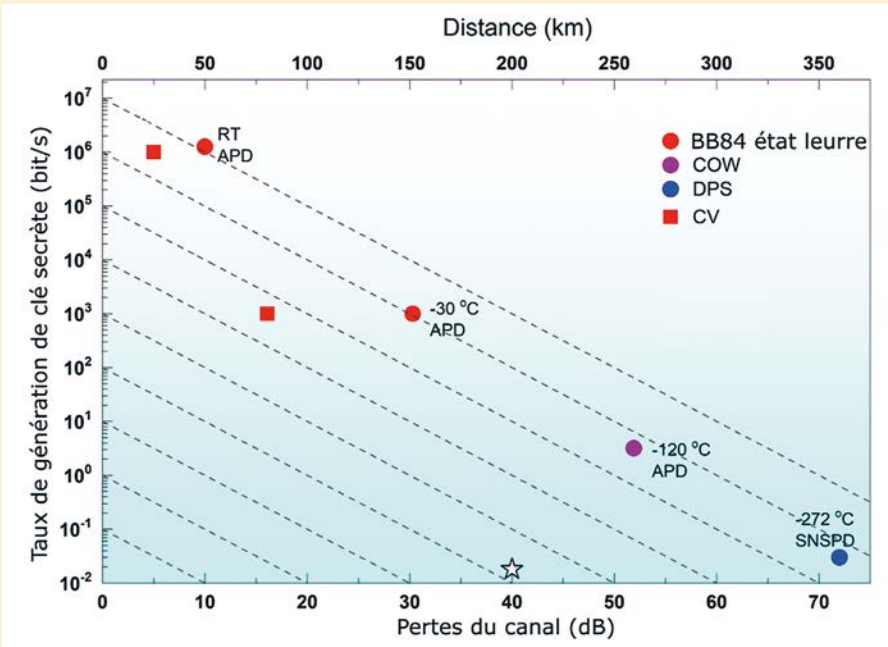

Figure 2. Quelques résultats représentatifs d'expériences de QKD en utilisant les protocoles à l'état leurre avec des détecteurs à photodiode d'avalanche (APD) à température ambiante (RT) ou refroidies ; le protocole COW ; le protocole DPS avec des détecteurs de photons uniques supraconducteurs (SNSPD) ; et le protocole CV-QKD. Les performances ne peuvent pas être comparées directement parce-que le niveau de sécurité garantie peut être différent pour chaque implémentation. Un coefficient de pertes de fibre optique de 0,2 dB/km est considéré dans cette figure. (Figure reprise partiellement par la *figure 1*d de la référence [4].)

https://doi.org/10.1051/photon/20189133

Les défis de performance et de sécurité pratique

Les résultats illustrés à la *figure 2* permettent d'apprécier les progrès importants des dernières années mais aussi d'identifier certaines barrières inhérentes des mises en œuvre de la cryptographie quantique.

Une première barrière concerne la distance maximale de communication qui peut être atteinte sur des canaux de fibre optique. L'atténuation de la lumière à la longueur d'onde des télécommunications (1550 nm) étant de l'ordre de 0,2 dB/km, les pertes engendrées par la propagation dans le canal limitent la portée des liens QKD point-à-point à quelques centaines de kilomètres : au-delà, générer un seul bit de clé secrète nécessiterait plusieurs années, même en utilisant des sources et des détecteurs de lumière parfaits, ce qui présente peu d'intérêt pratique. L'extension de la portée des systèmes QKD est un défi majeur pour les applications du domaine. Pour les systèmes basés sur la détection de photon unique, le facteur-clé est le bruit de ces détecteurs. Les détecteurs basés sur des nanofils supraconducteurs (SNSPD – en anglais, *superconducting nanowire single photon detectors*) sont des dispositifs extrêmement prometteurs pour les communications quantiques grâce à leur efficacité élevée, et leurs faibles temps morts, taux de coups d'obscurité et incertitude temporelle, et sont commercialement disponibles. Leur utilisation a permis d'atteindre 72 dB de pertes de canal, ce qui est équivalent à 360 km de fibre standard. Pour les systèmes à variables continues, qui sont généralement plus sensibles aux pertes, le facteur crucial est l'excès de bruit – le bruit excédant le bruit de photon fondamental des états cohérents – qui doit être le plus bas possible, mais aussi la capacité d'évaluer précisément la valeur de ce bruit, ce qui devient de plus en plus difficile avec la distance [3].

Afin de franchir les distances à l'échelle mondiale, il est nécessaire de recourir à deux approches : des structures réseaux et des liens satellitaires (*figure 3*). Des réseaux avec des nœuds fidèles, qui correspondent essentiellement à des liaisons point-à-point connectées, ont été mis en œuvre, y compris en Europe. Cependant, pour une sécurité globale d'un bout à l'autre de la chaîne de communication, il est nécessaire d'utiliser des répéteurs quantiques, qui sont encore à un stade précoce de développement. L'utilisation des satellites comme des relais quantiques permettrait de s'affranchir des pertes inhérentes aux canaux terrestres. En effet, les effets des pertes et des fluctuations dues à l'atmosphère sont limités à son épaisseur d'environ 10 kilomètres, et la lumière peut ensuite se propager de façon quasiment imperturbable vers des satellites à orbite basse ou éventuellement géostationnaires. Plusieurs défis liés par exemple à la diffraction ou à la précision du pointage se présentent pour des telles expériences et ont été abordés dans des études de faisabilité importantes [5]. Un pas majeur a été franchi en 2017 avec les expériences du premier satellite équipé avec des systèmes quantiques, développé par la Chine. Son utilisation a notamment permis la distribution de clés quantiques sur une distance de 600 km, impossible à atteindre avec une liaison terrestre.

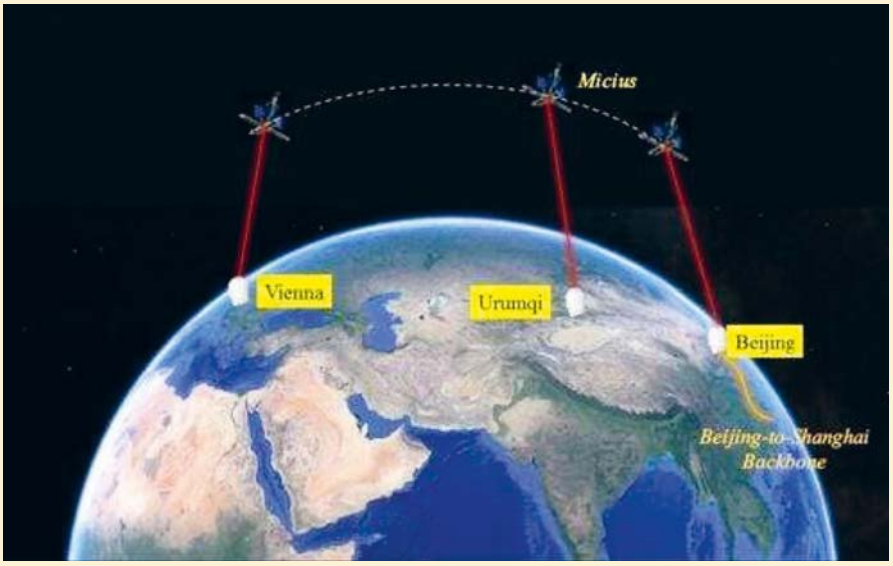

Figure 3. Dans les futurs réseaux quantiques, des liaisons terrestres et satellitaires seront nécessaires pour une utilisation des communications quantiques sur une échelle globale. Les nœuds de ces réseaux peuvent être considérés fiables, comme dans le cas des réseaux mis en œuvre jusqu'à présent, ou non fiables, ce qui nécessitera le déploiement des répéteurs quantiques. Dans la première catégorie, le satellite chinois Micius a été utilisé récemment pour une communication sécurisée entre deux interlocuteurs en Chine et en Autriche en distribuant une clé secrète sur une distance inédite.

La deuxième barrière pour des systèmes QKD concerne le taux maximal de génération de clé secrète possible en utilisant des canaux de communication pratiques, et donc bruités, ce qui est sujet à des limitations théoriques récemment déterminées. En pratique, les clés de chiffrement produites par la QKD peuvent être utilisées dans un schéma de chiffrement symétrique comme le protocole AES (en anglais, *Advanced Encryption Standard*), qui est résistant à une attaque par ordinateur quantique, ou encore être combinées avec la méthode de masque jetable afin d'obtenir une sécurité absolue. Dans les deux cas, le taux de clé obtenu par la couche QKD sous-jacente pour un scénario d'application typique est crucial. Des taux plus élevés permettent une mise à jour plus fréquente de clés de chiffrement dans le cas du chiffrement symétrique, et une augmentation proportionnelle de la bande

https://doi.org/10.1051/photon/20189133

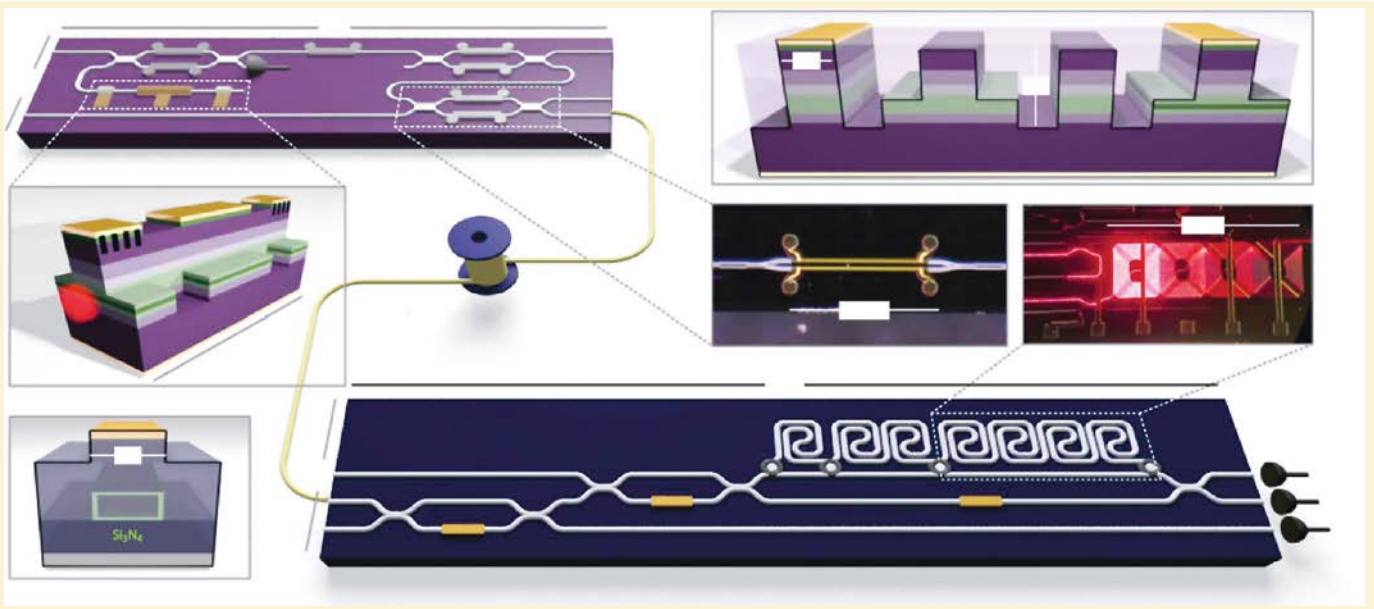

Figure 4. Une architecture de photonique intégrée pour l'implémentation de QKD à variables discrètes. L'architecture combine des techniques sur InP (transmetteur) et sur *silicon oxinitride* (récepteur). (D'après [7])

passante de communication dans le cas du chiffrement à masque jetable. Actuellement, il existe encore une forte disparité entre les débits de communications optiques classiques et la QKD. Des taux de plusieurs centaines de Gigabits par seconde et par canal de longueur d'onde sont atteints aujourd'hui par des méthodes classiques, tandis que des taux de l'ordre du Mégabit par seconde sont réalisés par des systèmes QKD. Ces derniers sont suffisants par exemple pour la transmission vidéo ; cependant pour chiffrer des grands volumes de trafic de réseau classique en utilisant la cryptographie à masque jetable, il sera nécessaire d'augmenter de façon significative le taux de clés secrètes produites par la QKD.

Comme pour le défi de la portée, les performances des détecteurs de photon unique, et plus particulièrement leur efficacité quantique et leur temps-mort, déterminent le débit de génération de clé dans des systèmes basés sur leur utilisation. Les performances récentes des détecteurs de type SNSPD ouvrent la voie à des taux quadruples par rapport à l'état de l'art. Pour les systèmes à variables continues, augmenter la bande passante des détecteurs cohérents, tout en gardant un bruit électronique faible, ainsi que la mise au point des systèmes avancés avec génération de la référence de phase en niveau du récepteur, seront des étapes nécessaires. Pour augmenter encore plus le taux, il est aussi possible d'utiliser le multiplexage en longueur d'onde ou en mode spatial, qui sont des technologies utilisées couramment en communications optiques.

En plus de barrières de performance analysées ci-dessus, un défi important pour les prochaines années sera le développement des systèmes permettant de réduire la complexité, les coûts, et la consommation de puissance. L'intégration photonique offre un niveau de miniaturisation élevé, ouvrant la voie à des modules compacts qui peuvent être produits en masse à bas coût [6]. Des premiers efforts dans cette direction ont été entrepris récemment, en utilisant principalement les plateformes d'intégration sur silicium (Si) et sur le phosphate d'indium (InP), pour des modules de transmission et de réception, et pour tous les principaux protocoles QKD (*figure 4*). Le déploiement des systèmes répondant aux exigences des applications pratiques sera aussi grandement facilité par la coexistence dans la même fibre des signaux quantiques avec le trafic des données usuelles, éliminant le besoin pour des fibres dédiées. Plus généralement, la conception des nouvelles architectures réseau pour l'acheminement de l'information, en intégrant les contraintes des systèmes de cryptographie quantique, garantira des performances optimales et flexibles pour ces réseaux hybrides émergents.

On remarque aussi finalement que, bien que la sécurité d'un protocole QKD puisse être prouvée rigoureusement, sa mise en œuvre réelle contient souvent des imperfections qui peuvent ne pas être prises en compte dans la preuve de sécurité correspondante. En exploitant des telles imperfections, des attaques diverses ont été proposées, ciblant la source ou les détecteurs. Certaines d'entre elles ont même démontré leur efficacité contre des systèmes commerciaux. En réponse à cette menace de « hacking » quantique, il a été nécessaire de développer des contre-mesures correspondantes [8]. Une approche plus fondamentale afin de regagner la sécurité dans la mise en œuvre pratique de la QKD est la conception de nouveaux protocoles, notamment les protocoles DI (en anglais, *device independent*) et MDI (*measurement*

https://doi.org/10.1051/photon/20189133

device independent). Ces protocoles proposent des solutions exploitant des principes de base de la mécanique quantique, en particulier la non-localité des états quantiques intriqués et sa confirmation en utilisant les inégalités de Bell ; même si la mise en œuvre de tels protocoles reste encore difficile, elle permettra d'établir la sécurité sans connaitre les détails de l'implémentation.

Perspectives

Adresser les défis présentés dans cet article permettra d'avancer vers des systèmes de cryptographie quantique pratiques intégrés et flexibles, offrant des garanties de sécurité maximale et faisant partie de réseaux de communication à l'échelle globale. Avec des avancées attendues sur la certification et la standardisation de la QKD, ceci permettra leur utilisation pour la sécurisation des transactions dans la vie courante. La QKD est l'application-phare du domaine, mais tous ces progrès s'étendront sur une riche gamme d'applications au-delà de la distribution de clés, permettant d'utiliser l'avantage obtenu en exploitant des ressources quantiques pour des tâches complexes et variées [9]. Des travaux de recherche partout dans le monde s'appliquent à déterminer la puissance et les limitations des communications quantiques ; les développements des prochaines années seront certainement des étapes cruciales vers l'internet quantique du futur.

POUR EN SAVOIR PLUS

[1] E. Diamanti, E. Kashefi, Best of both worlds, *Nature Phys.* 13, 3 (2017)

[2] V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dusek, N. Lütkenhaus, M. Peev, The security of practical quantum key distribution, *Rev. Mod. Phys.* **81**, 1301 (2009)

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

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

[5] R. Bedington, J.-M. Arrazola, A. Ling, Progress in satellite quantum key distribution, *npj Quantum Information* **3**, 30 (2017)

[6] A. Orieux, E. Diamanti, Recent advances on integrated quantum communications, *J. Opt.* **18**, 083002 (2016)

[7] P. Sibson *et al.*, Chip-based quantum key distribution, *Nature Communications* **8**, 13984 (2017)

[8] H.-K. Lo, M. Curty, K. Tamaki, Secure quantum key distribution, *Nature Photonics* **8**, 595 (2014)

[9] A. Broadbent, C. Schaffner, Quantum cryptography beyond quantum key distribution, *Des. Codes Cryptogr.* **78**, 351 (2016)