



Des capteurs ultraperformants pour contrer les espions

Une équipe de l'UNIGE et d'ID Quantique a développé des détecteurs de photons uniques aux performances inédites, ouvrant de nouvelles perspectives pour la cryptographie quantique.

Comment combattre le vol de données, véritable enjeu de société? La physique quantique a la solution. Ses théories permettent en effet d'encoder de l'information (un qubit) dans des particules de lumière (un photon) et de faire circuler ces dernières dans une fibre optique de manière ultrasécurisée. Mais l'utilisation de cette technologie de télécommunication à grande échelle se heurte notamment aux performances des capteurs de photons uniques utilisés. Une équipe de l'Université de Genève (UNIGE), avec l'entreprise [ID Quantique](#), est parvenue à multiplier par vingt leur vitesse. Cette innovation, à découvrir dans la revue *Nature Photonics*, permet d'atteindre des performances jamais obtenues auparavant dans la distribution quantique des clés.

Acheter un billet de train, réserver un taxi, se faire livrer un repas: autant de transactions effectuées quotidiennement via des applications mobiles. Celles-ci se basent sur des systèmes de paiement impliquant un échange d'informations secrètes entre l'utilisateur/trice et sa banque. Pour ce faire, la banque génère une clé publique, qu'elle transmet à son/sa client-e, et une clé privée, qu'elle garde secrète. Avec la clé publique, l'utilisateur/trice peut modifier l'information, la rendre illisible et l'envoyer à la banque. Grâce à sa clé privée, la banque peut la décrypter.

Ce système est désormais menacé par la puissance de calcul des ordinateurs quantiques. Pour y remédier, la cryptographie quantique – ou «distribution quantique de clés» (QKD, pour *quantum key distribution* en anglais) – est la meilleure option. Elle permet à deux parties de produire des clés secrètes partagées et de les transmettre grâce à des photons, via fibre optique, de manière ultrasécurisée. En effet, les lois de la mécanique quantique stipulent qu'une mesure affecte l'état du système mesuré. Ainsi, si un-e espion-ne tente de mesurer les photons pour voler la clé, l'information sera instantanément altérée et l'interception révélée.

Limites actuelles

L'application de ce système est notamment limitée par la vitesse des détecteurs de photons uniques, utilisés pour réceptionner l'information. Après chaque détection, ils doivent en effet récupérer durant une trentaine de nanosecondes, ce qui limite le débit des clés secrètes à environ 10 mégabits par seconde. Une équipe de l'UNIGE dirigée par Hugo Zbinden, professeur associé au Département de physique appliquée de la Faculté des sciences de l'UNIGE, est parvenue à repousser cette limite en développant un détecteur avec des meilleures performances. Ces travaux ont été menés en collaboration avec l'équipe de Félix Bussièrès de la société [ID Quantique](#), *spin-off* de l'université.



Grâce à ces capteurs, les scientifiques sont parvenu-es à générer une clé secrète à un débit de 64 mégabits par seconde sur 10km de fibres optiques.

Illustrations haute définition

contact

Hugo Zbinden

Professeur associé
Département de physique
appliquée
Faculté des sciences
UNIGE

+41 22 379 05 04
Hugo.Zbinden@unige.ch

Fadri Grünenfelder

Doctorant
Département de physique
appliquée
Faculté des sciences
UNIGE

fagrue@com.uvigo.es

DOI: [10.1038/s41566-023-01168-2](https://doi.org/10.1038/s41566-023-01168-2)

«Actuellement, les détecteurs les plus rapides pour cette application sont les détecteurs de photons uniques à nanofils supraconducteurs», explique Fadri Grünenfelder, ex-doctorant au Département de physique appliquée de la Faculté des sciences de l'UNIGE et premier auteur de l'étude. «Ces dispositifs comportent un minuscule fil supraconducteur refroidi à -272°C . Si un photon unique le frappe, il se réchauffe, cesse d'être supraconducteur pendant un court instant, ce qui génère un signal électrique détectable. Lorsque le fil redevient froid, un autre photon peut être détecté.»

Performances record

En intégrant non pas un mais quatorze nanofils dans leurs capteurs, les chercheurs/euses sont parvenu-es à obtenir des taux de détection record. «Nos détecteurs peuvent compter vingt fois plus vite qu'un dispositif à un seul fil», explique Hugo Zbinden. «Si deux photons arrivent dans un court laps de temps au sein de ces nouveaux détecteurs, ils peuvent toucher des fils différents et être détectés tous les deux, alors qu'avec un seul fil, c'est impossible.» Les nanofils utilisés sont également plus courts, ce qui participe à réduire leur temps de récupération.

Grâce à ces capteurs, les scientifiques sont parvenu-es à générer une clé secrète à un débit de 64 mégabits par seconde sur 10km de fibres optiques. Ce débit est suffisamment élevé pour sécuriser, par exemple, une visioconférence avec plusieurs participant-es. C'est cinq fois plus que les performances de la technologie actuelle, sur cette distance. En prime, ces nouveaux détecteurs ne sont pas plus complexes à produire que les dispositifs actuels, disponibles sur le marché.

Ces résultats ouvrent de nouvelles perspectives pour le transfert ultrasécurisé de données, crucial pour les banques, les systèmes de santé mais aussi les gouvernements et l'armée. Ils pourront par ailleurs être appliqués dans de nombreux autres domaines où la détection de la lumière est un élément clé, comme l'astronomie et l'imagerie médicale.

UNIVERSITÉ DE GENÈVE
Service de communication

24 rue du Général-Dufour
CH-1211 Genève 4

Tél. +41 22 379 77 17

media@unige.ch

www.unige.ch