

Communication quantique : plus fort que le chiffrement de bout en bout ?

Utiliser les lois de la physique quantique pour protéger les communications ? C'est la perspective que dessine une équipe de recherche chinoise, emmenée par le professeur Jian-Wei Pan, de l'université de Hefei. Moins d'un an après être parvenus à mettre sur orbite le premier satellite de communication quantique au monde, Micius, les chercheurs chinois ont réussi à transmettre des photons dits intriqués à deux stations situées au sol et distantes de 1203 kilomètres.

L'intrication est un des phénomènes les plus étranges de la physique quantique, il permet de lier deux particules dans un état quantique similaire. Si l'état de l'une d'entre elles est modifié, par exemple via une interception, l'état de l'autre s'en trouve immédiatement affecté, quelle que soit la distance séparant ces deux particules jumelles. C'est cette propriété que démontre l'équipe chinoise, dont les résultats ont été salués par la communauté scientifique.

Photons intriqués, interception écartée

L'expérience apparaît d'abord comme une piste de recherche intéressante pour la sécurisation des échanges, avec la création de clefs cryptographique quantique que l'équipe de Jian-Wei Pan présente comme la prochaine étape. Pour créer une telle clé, les deux parties utiliseraient les résultats d'une série de mesures sur des paires de photons intriqués. La clé en question peut ensuite être utilisée pour chiffrer les messages envoyés sur un canal régulier. Et le duo détecterait toute présence d'un intrus essayant d'intercepter et de retransmettre les photons, car cela détruirait l'intrication informant l'émetteur et le récepteur de la tentative d'espionnage et détruisant le message.

Ce premier *proof-of-concept* pour le chiffrement quantique arrive à l'heure où les premiers ordinateurs quantiques menacent à moyen terme la totalité des algorithmes de chiffrement classiques. « *C'est la première étape vers des communications quantiques sécurisées dans le monde entier, et peut-être même une Internet quantique* », explique Anton Zeilinger, un expert en physique quantique de l'université de Vienne en Autriche. Car, au-delà de la sécurisation des échanges, les Chinois lorgnent aussi vers la téléportation quantique, une technique qui utiliserait également l'intrication mais pour communiquer instantanément entre deux points.

Vers une course à l'espace quantique ?

La publication des résultats de cette expérience, dans le journal [Science](#), apparaît donc comme un pas significatif pour la communication quantique. « *Il nous a fallu 14 années pour parvenir à ce résultat* », résume Jian Wei-Pan, dans les colonnes du [New Scientist](#). Même si on est encore très loin de toute application pratique. Seulement un photon sur 6 millions a été capté avec succès par les stations de base, l'un des défis de l'expérience consistant à capturer les flux lumineux émis depuis un satellite survolant la Terre à 500 km d'altitude. Mais l'expérience chinoise pourrait bien donner des idées aux autres puissances, qui seront soucieuses de ne pas laisser la Chine prendre trop

d'avance sur une technologie aussi stratégique. De quoi lancer une « *course mondiale aux communications quantiques depuis l'espace* », comme le pense Jian-Wei Pan ?

Jusqu'à présent, les communications quantiques ont été testées sur de la fibre optique, entraînant une déperdition de signal et limitant les distances. Le précédent record de communication quantique était déjà détenu par la Chine, avec une distance de 404 km établi en 2016 sur une fibre optique de haute qualité. D'ores et déjà, avec son satellite Micius, Pékin envisage de pousser son avantage en augmentant les distances. Prochaine étape : une communication sécurisée entre Pékin et Urumqi, ville de l'ouest de la Chine, soit 2 400 kilomètres. En juillet 2018, un test entre la capitale chinoise et Vienne (en Autriche) est également attendu.

A lire aussi :

[Quantique : IBM aligne désormais 17 qubits et défie Google](#)

[L'informatique quantique, une épée de Damoclès pour le chiffrement](#)

[Google Chrome s'essaie au chiffrement post-quantique](#)

crédit photo © Pavel Ignatov / Shutterstock