**COMMUNIQUÉ DE PRESSE**

Paris, le 5 mai 2021

# La cryptographie quantique expérimentale en ordre de bataille : déjouons d'abord les attaques les plus simples !

**La distribution quantique de clés (quantum key distribution – QKD) représentera à court terme un atout majeur dans la sécurisation des communications privées et sensibles. Pour être efficaces, cette technologie doit être capable de résister à des attaques externes. Une expérience réalisée par des chercheurs de Télécom Paris, Institut Polytechnique de Paris et publiée dans *Nature Scientific Reports*, a démontré que pour une vulnérabilité donnée, plusieurs parcours d'attaques sont possibles, avec des niveaux de complexité expérimentale variés. L'équipe a développé une méthodologie complète pour mesurer l'ampleur des attaques. Cette approche permet de privilégier le développement des contremesures dans le cas des attaques les plus simples et d'améliorer la conception des équipements en matière de cryptographie quantique, ouvrant ainsi la voie à la certification de leur sécurité.**

Notre capacité à envoyer des messages secrets à l'insu de forces potentiellement hostiles a toujours occupé une place importante dans notre société. Qu'il s'agisse de Jules César, qui employait une forme de chiffrage dans ses communications à ses généraux, ou de la télémédecine, qui représente une des applications les plus marquantes des réseaux de télécommunications, la garantie d'un niveau de sécurité élevé a toujours été primordiale. Dans ce contexte, la distribution quantique de clés constitue une démarche selon laquelle des clés secrètes sont distribuées à distance entre deux interlocuteurs.

Romain Alléaume, Maître de conférences à Télécom Paris, Institut Polytechnique de Paris, explique : « *Les techniques cryptographiques employées actuellement reposent sur la difficulté présumée de certains problèmes mathématiques. La sécurité QKD, en revanche, se fonde entièrement sur les lois de la physique quantique. Elle permet ainsi d'établir des clés dont la sécurité peut être garantie dans le futur, même face à un adversaire qui disposerait d'une puissance de calcul illimitée, y compris un ordinateur quantique.* »

## Cryptographies classique et quantique : deux outils complémentaires

Malgré le fait qu'elle offre un niveau de sécurité supérieur, la QKD et de façon plus générale la cryptographie quantique, a peu de chance de se voir supplantée par la cryptographie classique. En effet, cette technologie ne propose pas tous les services de sécurité et elle se limite pour l'instant essentiellement aux distances métropolitaines. La QKD permet néanmoins d'obtenir des niveaux de sécurité sans précédent pour certaines applications ciblées, lorsqu'elle est conjuguée à la cryptographie classique. Comparons la sécurité automobile à la sécurité des réseaux : alors que nous conduisons toujours plus vite, les ceintures de sécurité (la cryptographie classique) ne sont peut-être pas assez efficaces. Ici, la QKD joue un rôle analogue à celui de l'airbag : une couche de sécurité supplémentaire permettant de protéger la confidentialité des données sur le long terme. Ces perspectives très prometteuses ont favorisé le déploiement récent de réseaux QKD, notamment au Royaume-Uni, au Japon, en Corée et à grande échelle, en Chine.

## Une exigence, la certification de sécurité

En 2019, l'Europe a lancé l'initiative EuroQCI dont l'objectif est de déployer dans les dix prochaines années une infrastructure de communication quantique au niveau paneuropéen, visant à connecter les sites publics stratégiques et à contribuer à la souveraineté numérique de l'Europe. Parmi les particularités d'EuroQCI figure le fait que cette infrastructure sera intégrée dans la cryptographie classique et reposera sur des systèmes de certification de sécurité qui n'existent pas encore. La promesse de sécurité inconditionnelle qu'offre la QKD sur le plan théorique ne suffit pourtant pas à garantir un niveau de sécurité élevé pour des applications concrètes. Pour l'heure, il nous faut développer une approche standardisée afin d'évaluer et certifier la sécurité des produits QKD. La certification de sécurité est une étape incontournable dans l'élargissement du marché des technologies de cryptologie quantiques telles que la QKD et le générateur quantique de nombres aléatoires (Quantum Random Numbers Generator - QRGN). Il s'agit d'une tâche complexe, qui nécessite la collaboration d'experts issus de différents domaines dont la sécurité informatique et l'ingénierie et la théorie quantiques.

Plusieurs organismes internationaux de normalisation, tels que l'ISO et le QKD Industry Specification Group de l'ETSI[1] œuvrent activement dans ce sens, dans le cadre de la méthodologie dite des «Critères Communs »[2].

**Une protection quantique contre les piratages et les attaques**

Francesco Mazzoncini, doctorant à l'Institut Polytechnique de Paris et co-auteur de l'article, détaille : « *En nous inspirant de la méthodologie mise en œuvre dans les appareils de cryptographie classique, nous avons réalisé une évaluation de la vulnérabilité expérimentale d'un système QKD à variables continues pour contrer les attaques de saturation ciblant ses détecteurs. Nous avons testé deux stratégies d'attaque à cette fin. La mise en œuvre de la première stratégie a été particulièrement difficile : il s'agissait d'effectuer un déplacement cohérent important, une tâche dont la complexité est bien connue. En revanche, la deuxième stratégie qui consistait à projeter un laser externe précisément sur le récepteur QKD a été beaucoup plus facile à réaliser.* »

Cet article co-publié avec ses collègues Rupesh Kumar and Hao Qin, tous deux anciens membres du groupe Information Quantique et Applications de Telecom Paris, offre un nouveau point de vue sur la conception des équipements de cryptographie quantique : si la quête d'une sécurité parfaite a surtout incité les cryptographes quantiques à étudier, sous l'aspect théorique, les attaques complexes et mettre en œuvre des contremesures, cette expérience montre que, en pratique, les attaques simples mais efficaces peuvent être les plus dangereuses– elles doivent donc être traitées en premier ! *« Heureusement, nous avons également développé une contremesure à nos deux attaques, qui peut être intégrée dans un logiciel et présente donc un coût modique. Il s'agit simplement d'effectuer un test statistique pour vérifier que le détecteur calibré fonctionne bien dans son champ de linéarité »*, ajoute Romain Alléaume. Avec cette approche, les chercheurs initient également une réflexion sur le compromis entre la performance du système de communication quantique, son niveau de sécurité et son coût. Prioriser les attaques permet d'investir dans les contremesures qui assurent la sécurité du système sans altérer sa performance ni augmenter son coût de façon disproportionnée.

« *Notre travail présente donc une méthodologie complète, qui repose sur la mesure de l'ampleur des attaques et permet d'évaluer la sécurité des équipements de cryptographie quantique, constituant ainsi une avancée concrète vers la certification de sécurité QKD.* »

Pour en savoir davantage sur la QKD et la résistance aux attaques :

*Experimental vulnerability analysis of QKD based on attack ratings*

Rupesh Kumar (University of York), Francesco Mazzoncini (Télécom Paris), Hao Qin (CAS Quantum Network Co.) et Romain Alléaume (Télécom Paris)

www.nature.com/articles/s41598-021-87574-4

**À propos de Télécom Paris – www.telecom-paris.fr**

Télécom Paris est une grande école du top 4 des écoles d'ingénieurs généralistes françaises. Reconnue pour sa proximité avec les entreprises, cette école publique garantit une excellente employabilité dans tous les secteurs et apparait comme la 1re grande école d'ingénieurs du numérique. Avec des enseignements d'excellence et une pédagogie innovante, Télécom Paris est au cœur d'un écosystème d'innovation unique, fondé sur l'interaction et la transversalité de sa formation, de sa recherche interdisciplinaire, de ses deux incubateurs d'entreprises et de ses campus (Paris et Sophia Antipolis – Eurécom). Son laboratoire LTCI est présenté par l'HCERES comme une unité phare dans le domaine des sciences du numérique avec à la fois un rayonnement remarquable à l'international, un volume exceptionnel d'activités vers le monde socio-économique et les entreprises, et un engagement fort dans la formation. Membre fondateur de l'Institut Polytechnique de Paris, école de l'IMT (Institut Mines-Télécom), Télécom Paris se positionne comme le collège de l'innovation par le numérique du plateau de Saclay.


**CONTACTS PRESSE TÉLÉCOM PARIS**

**Isabelle Mauriac**
Attachée de presse
01 43 38 75 35 • 06 27 70 71 60
imauriac@imedia-conseil.fr

**Stéphane Menegaldo**
Responsable de la communication scientifique
01 75 31 98 53 • 06 16 60 06 76
stephane.menegaldo@telecom-paris.fr


[1] European Telecommunications Standards Institute
[2] www.commoncriteriaportal.org