Sur la communication quantique (et les exagérations)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 19 juin 2017

https://www.bortzmeyer.org/communication-quantique.html

Dans un article publié dans Science <http://science.sciencemag.org/content/356/6343/1140>, un groupe de chercheurs annonce avoir réussi à transporter des photons intriqués sur plus de mille kilomètres. Mais ce n'est pas cette avancée scientifique intéressante que je veux commenter, mais les grossières exagérations avec lesquelles elle a été annoncée, notamment la promesse ridicule que la communication quantique allait donner un Internet plus sûr, voire un « Internet inviolable » (comme dit dans l'article sensationaliste de l'Express <http://www.lexpress.fr/actualite/sciences/teleportation-quantique-tout-comprendre-a-la-prouesse-realisee-par-la-chine_1918657.html>).

L'article en question promet en effet, outre l'Internet inviolable, de la téléportation, des « ordinateurs dotés d'une puissance de calcul sans commune mesure avec les plus puissantes machines actuelles » et même « un Internet basé à l'avenir sur les principes de la physique quantique ». Revenons au monde réel. L'article originel <http://science.sciencemag.org/content/356/6343/1140> est bien plus modeste. (Au passage, il n'est pas disponible en ligne, car où irait-on si tout le monde pouvait accéder facilement aux résultats scientifiques ? Heureusement, on le trouve <http://sci-hub.bz/10.1126/science.aan3211> sur Sci-Hub, qu'on ne remerciera jamais assez.) Les auteurs ont réussi à transmettre des photons intriqués sur une distance plus grande que ce qui avait été fait avant. Beau résultat (l'opération est très complexe, et est bien décrite dans leur article) mais en quoi est-ce que ça nous donne un Internet inviolable ? L'idée est que la communication quantique est à l'abri de l'écoute par un tiers, car toute lecture, même purement passive, casserait l'intrication et serait facilement détectée. Sa sécurité est donc physique et non plus algorithmique. La NSA serait donc réduite au chômage ? C'est en tout cas ce que promet l'Express…

Il y a plusieurs raisons pour lesquelles cette promesse est absurde. La plupart de ces raisons découlent d'un fait simple que le journaliste oublie complètement dans son article : la communication de point à point n'est qu'une partie du système technique complexe qui permet à Alice et Bob de s'envoyer des messages de manière sécurisée. Si on ne considère pas la totalité de ce système, on va se planter. D'abord, citons « l'argument de Schneier », écrit il y a plus de huit ans <https://www.schneier.com/blog/archives/2008/10/quantum_cryptog.html> et toujours ignoré par les vendeurs de solutions quantiques : la communication quantique ne sert à rien, pas parce qu'elle ne marche pas (au contraire, les progrès sont importants) mais parce qu'elle sécurise ce qui était déjà le maillon le plus fort

du système. Quant on veut surveiller les gens, la plupart du temps, on ne va pas casser la cryptographie qui les protège. On va faire plus simple : exploiter une faille du protocole de communication, ou une bogue du logiciel qui le met en œuvre, ou tout simplement récupérer l'information à une des deux extrêmités (il ne sert à rien de faire de la communication quantique avec Google si Google fournit toutes vos données à la NSA). Avant de remplacer la cryptographie classique, il faudrait déjà sécuriser tous ces points. Autrement, le surveillant et l'espion, qui sont des gens rationnels, continueront à attaquer là où la défense est faible. Déployer de la communication quantique, c'est comme utiliser un camion blindé pour transmettre de l'argent entre deux entrepôts dont les portes ne ferment pas à clé. (C'est d'autant plus important que la communication quantique n'est pas de bout en bout : elle n'arrive pas jusqu'aux PC d'Alice et Bob.)

Et ce n'est pas la seule faiblesse de la communication quantique. La plus importante, à mon avis, est qu'elle n'authentifie **pas**. Vos messages ne peuvent pas être interceptés mais vous ne pouvez pas être sûr de savoir à qui vous parlez. Vous avez une communication sécurisée avec…quelqu'un, c'est tout. Cela rend la communication quantique très vulnérable à l'attaque de l'Homme du Milieu. Il existe bien sûr des remèdes contre cette attaque, mais tous dépendent de la cryptographie classique, avec ses faiblesses.

En parlant de cryptographie classique, notons aussi que la communication quantique est limitée à la distribution de clés. Vous avez toujours besoin d'un algorithme classique (comme AES) pour chiffrer.

Autre limite de la communication quantique : elle protège le **canal**, pas les **données**. Une fois les données « au repos » (sur les disques durs des ordinateurs d'Alice et Bob), elles sont aussi vulnérables qu'avant. Un piratage avec fuite de données (comme Ashley Madison, Yahoo, Sony…) se ferait aussi bien avec communication quantique que sans.

Qu'y avait-il encore comme promesses dénuées de sens dans l'article de l'Express ? Ah, oui, « des ordinateurs dotés d'une puissance de calcul sans commune mesure avec les plus puissantes machines actuelles ». Ici, il semble que l'auteur ait confondu la communication quantique avec le calcul quantique, qui n'a rien à voir. Et quant à la téléportation, elle relève plus de la science-fiction : l'expérience décrite dans Science n'a rien à voir avec de la téléportation, même limitée.

Voilà, comme d'habitude, on a une avancée scientifique réelle, décrite dans un article sérieux mais que personne ne lira, sur-vendue dans un dossier de presse aguicheur, lui-même repris sans critique et sans vérification dans de nombreux médias. Vu l'information reçue par les citoyens ordinaires, il n'est pas étonnant que la sécurité informatique soit actuellement si mauvaise.

Depuis la parution de cet article, l'ANSSI a publié une bonne synthèse sur le sujet <https://www.ssi.gouv.fr/agence/publication/lavenir-des-communications-securisees-passe-t-il-par-la>.