

La Chine lance le premier satellite de communication quantique au monde

written by Françoise Laugée | 6 décembre 2016

À la recherche d'une technique de transmission ultra-sécurisée basée sur les lois de la physique quantique, la Chine prend une longueur d'avance sur les États-Unis et l'Europe dans le domaine de la cryptologie.

Le 16 août 2016, la Chine a lancé depuis la base de Jiuquan, dans le désert de Gobi, un satellite baptisé Mozi, qui permettra de tester la distribution quantique de clés de cryptage uniques (QKD pour Quantum Key Distribution) sur une grande distance.

La mécanique quantique est une théorie développée par Max Planck au début du XX^e siècle qui permet d'expliquer certains phénomènes que la physique classique ne peut pas expliquer. Selon cette théorie, la lumière est à la fois un phénomène vibratoire et corpusculaire : un rayon lumineux est une onde électromagnétique et un flux de photons. La distribution quantique de clés de cryptage unique, inventée il y a 30 ans aux États-Unis, utilise deux propriétés de ces photons, la polarisation et l'intrication quantique. La polarisation permet d'associer à chaque photon transmis une valeur binaire. L'intrication quantique permet, quant à elle, de sécuriser la communication.

La transmission de ces clés utilise les corrélations quantiques au sein d'une paire de photons intriqués en raison de deux caractéristiques essentielles. La première est que l'état quantique (lu comme « 0 » ou « 1 ») des photons est aléatoire : on obtient en conséquence une clé de cryptage de nature elle aussi totalement aléatoire, donc impossible à décrypter même par les plus puissants algorithmes. La seconde caractéristique tient à ce que toute observation, ou mesure, des photons génère des modifications de leur état, créant des défauts, du « bruit » repérable sur l'ensemble de l'émission ; on peut de plus déterminer la quantité d'information espionnée.

Ainsi, l'interception par un tiers est repérée, évaluée, et si l'espionnage est trop important, menaçant la sécurité de la clé, celle-ci ne sera tout simplement pas utilisée pour crypter les messages à transmettre : il suffira d'en générer une nouvelle. Lorsque l'on est sûr que l'émetteur et le récepteur détiennent une clé non espionnée, indécodable puisqu'aléatoire, elle pourra être utilisée tant pour le cryptage que le décryptage (donc par le biais d'un algorithme de chiffrement symétrique) d'informations transmises par n'importe quel canal, tel l'internet.

Au cours d'une mission prévue pour durer deux ans, les scientifiques chinois vont tenter de transmettre des clés de cryptage, par un satellite quantique, sur une distance de 2 500 kilomètres, entre Pékin et Ürümqi, capitale de la région du Xinjiang. Un autre test sera effectué ultérieurement entre Pékin et Vienne, en Autriche. C'est la première fois qu'une technologie de cryptage quantique sera testée dans l'espace. Elle a déjà été utilisée avec succès, aux États-Unis et en Europe, sur une distance maximale de 300 kilomètres, via des réseaux terrestres en fibre optique, pour des applications gouvernementales, militaires, ou encore pour des transmissions entre des établissements bancaires. La première expérimentation remonte à 1992 à l'université de Genève.

Assurer la transmission de messages grâce à des clés de chiffrement inviolables est un enjeu planétaire. Les États-Unis investissent 200 millions de dollars par an dans ce domaine de recherche, indique le Conseil national américain des sciences et technologies. Aujourd'hui à la tête d'une dizaine d'équipes de recherche dans le cadre de la mission chinoise et vice-président de l'université des sciences et technologies, Pan Jianwei, promu docteur en physique quantique de l'université de Vienne à la fin des années 1990, avait sollicité en son temps l'Union européenne pour financer un programme de développement d'un satellite quantique, sans succès. Depuis 2008, des chercheurs européens, notamment à Vienne et à Padoue, travaillent sur le lancement d'un satellite de communication quantique dans le cadre d'un programme baptisé Space-Quest. L'Union européenne a engagé 2,5 milliards d'euros en 2010 pour la recherche dans ce domaine. En mai 2016, Günther Oettinger, commissaire européen à l'économie et à la société numérique, a annoncé un financement d'un milliard d'euros en 2018 consacré aux technologies quantiques.

« Beaucoup de gens pensent que les communications quantiques joueront un rôle, notamment dans le futur d'internet », explique l'Autrichien Anton Zeilinger, chercheur et professeur reconnu en physique quantique qui a dirigé les travaux de doctorat de Pan Jianwei, précisant que cette technique ne serait pas réservée aux communications militaires mais s'appliquerait également aux communications commerciales. Avec le lancement programmé d'autres satellites de communication quantique, la Chine devrait disposer en 2030 d'une constellation assurant la transmission de flux d'informations totalement sûre.

Faire de la Chine *« l'un des pays les plus innovants en 2020 »* et une grande puissance technologique en 2049, année du centième anniversaire de la République populaire : telle est l'ambition exprimée par le président chinois Xi Jinping qui désigne la recherche quantique comme étant l'une des priorités du treizième plan national quinquennal. Une nouvelle révolution informatique est en cours avec l'internet quantique, et la Chine avance à grands pas dans cette voie.

Sources :

- « Satellites : Pékin lance le premier satellite inviolable », Bruno Trévidic, *Les Echos*, 17 août 2016.
- « La Chine prend de l'avance dans le cryptage des communications », Harold Thibault avec David Larousserie, *Le Monde*, 18 août 2016.
- « Cryptage : le saut quantique des Chinois », Yann Verdo, *Les Echos*, 5 septembre 2016.
- « Cryptographie quantique », Wikipédia, dernière modification de cette page le 17 septembre 2016.