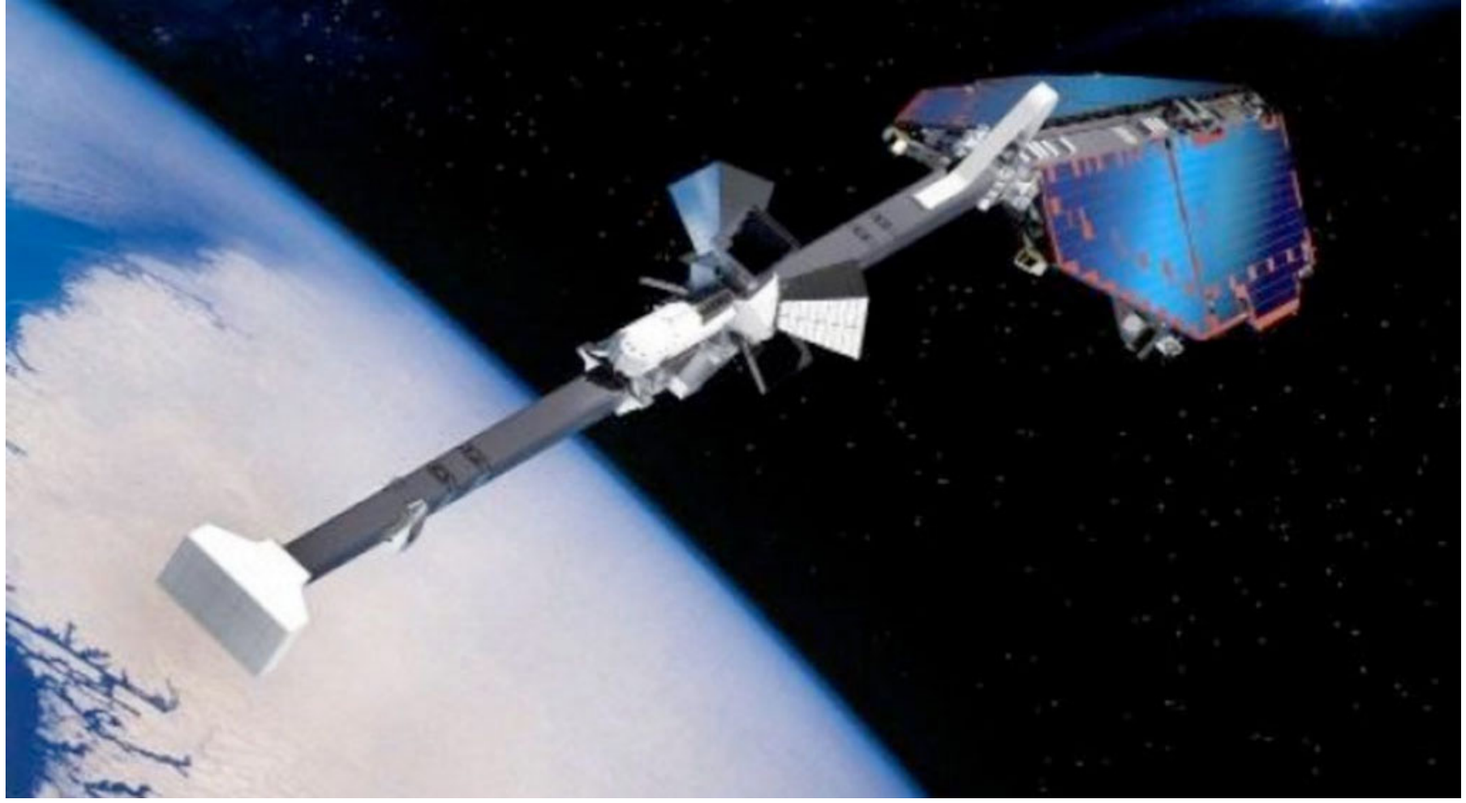
La Chine lance le premier satellite quantique.

L'agence spatiale chinoise a lancé le 16 août le premier satellite de communication quantique de l'histoire.
En phase de test, il prélude l'avènement des communications inviolables à l'horizon 2020-2030.



Dans le monde actuel, l'information est reine - le récent scandale des écoutes mondiales par la NSA, dévoilées par Edward Snowden, nous l'a prouvé.
Et donc, la sécurité des transmissions est devenue un enjeu planétaire de première importance. Dans ce contexte, le lancement et placement en orbite d'un satellite « quantique » expérimental, le premier du genre, par la Chine marque - si son bon fonctionnement se confirme - l'entrée des communications de masse dans une nouvelle ère, bien plus sure.

Du labo de recherche vers l'espace interplanétaire.

Il s'agit de cryptographie quantique, domaine jusque-là réservé aux laboratoires de recherche et à quelques organismes de sécurité nationale, une centaine environ. Un domaine récent qui s'appuie sur les étranges propriétés de la physique quantique, dont les lois organisent le monde des particules élémentaires de matière (électrons, protons, neutrons, atomes) et de lumière (photons).
Mais derrière cette physique complexe, la cryptographie quantique n'a qu'un objet, facile à énoncer : trouver la manière de transmettre entre deux interlocuteurs s'envoyant un message crypté, la clé nécessaire pour le décrypter sans risque qu'une troisième personne puisse l'avoir et donc accéder au message échangé.

Un satellite et deux sites terrestres

Concrètement, les Chinois (en collaboration avec les Australiens) ont satellisé le Quantum Experiments at Space Scale (QUESS) sur une orbite de 1000 km d'altitude, lequel contient un système de cryptage-décryptage quantique de 500 kg. Composé de miroirs semi-réfléchissants, de lasers et autres, ce dispositif est en ligne de mire directe avec deux dispositifs semblables basés sur le sol chinois et australien.
L'idée est de tester pendant 2 ans la possibilité d'émettre efficacement depuis l'un des sites de la Terre vers le satellite des signaux lumineux lasers (groupes de photons) contenant une clé de cryptage-décryptage quantique, puis de transmettre à nouveau depuis le satellite vers le deuxième site terrestre la clé.

La clé de la connaissance

Sachant que sans la connaissance de la clé, un message crypté ne dit rien, il s'agit d'utiliser la technologie quantique seulement pour transmettre la clé, le message (crypté) pouvant transiter entre l'émetteur et le récepteur terrestres par les voies normales (Réseau ou autre), mais en synchronisation avec la transmission quantique.
Une expérience qui n'a jamais encore été tentée, sur de si longues distances et dans l'espace, et qui s'avère essentiel pour en finir une fois pour toutes avec les risques de sécurité des systèmes cryptographiques actuels.

De la physique plutôt que des mathématiques

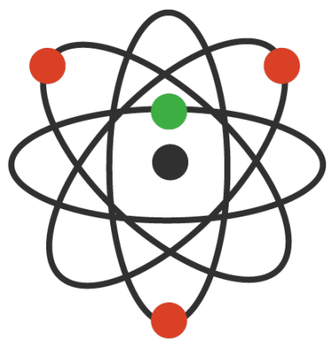
Sans revenir sur ces technologies utilisées actuellement par le Réseau mondial (chiffrement RSA), ce qui en soit mériterait un article, rappelons que la connaissance par un tiers d'une clé cryptant un message dépend de la capacité de ce tiers à résoudre rapidement un certain type de problèmes mathématiques (liés aux nombres premiers) - problèmes que tous les mathématiciens munis d'ordinateurs peuvent résoudre en principe, mais en y mettant tant de temps que cela n'a pas d'intérêt en termes d'espionnage.
Ainsi, la sécurité actuelle des réseaux dépend de la connaissance, des moyens et du génie de personnes. Et il n'est pas dit qu'un groupe de savants géniaux ne trouve un moyen informatique pour résoudre rapidement la classe de problèmes mathématiques liée aux clés de décryptage, mettant à bas toute la sécurité des communications mondiales.

Espion, tu es là !

A l'inverse la cryptographie quantique repose non pas sur un défi à la connaissance mais sur des propriétés physiques - un grand avantage - lesquelles reposent sur des lois qui rendent impossible l'interception des signaux lumineux et leur lecture (pour extraire la clé) sans que l'émetteur et le récepteur n'en soient informés - via des perturbations sur ces signaux.
Bref, la cryptographie quantique possède une qualité essentielle : aucun espion ne peut « aspirer » la clé sans être repéré. Peu importe, diriez-vous, car l'espion aura déjà la possibilité de décrypter le message ! Non, car les chiffres de la clé sont envoyés par des impulsions lasers successives, si bien que le hackage (piratage) par un tiers d'une impulsion alertera de sa présence sans pour autant lui permettre de connaître toute la clé.

Einstein et les fantômes

Pour les passionnés qui éprouveraient quelque frustration à ne pas trouver ici le détail du processus de transmission quantique d'une clé, disons de manière très succincte que le secret de cette inviolabilité repose sur le fait que les impulsions de photons contenant la clé (chaque impulsion donnant un chiffre de la clé) gardent entre l'émetteur et le récepteur (Terre-Satellite ou Satellite-Terre) une « cohérence quantique ».
En un mot, l'émetteur qui envoie la clé possède un groupe de photons « intriqué » avec le groupe émis, un lien étrange au coeur de la physique quantique, qui fait que toute perturbation du groupe émis se répercute instantanément - quelle que soit la distance, même d'un bout à l'autre de l'Univers - en une perturbation du groupe resté sur Terre (et vice-versa).



Un lien qu'Einstein lui-même avait qualifié de « spooky » (fantomatique) tant cela l'avait choqué.
Un fantôme donc qui nous aidera à nous protéger...