La cryptographie quantique est là, l'ordinateur du futur se prépare

Technologie

Posté par: Visiteur

Publié le : 26-09-2010 12:01:06

Après les lasers, transistors, ordinateurs, premières applications de la physique quantique, une nouvelle révolution est en cours, de la cryptographie à l'informatique, grâce à la domestication d'atomes et autres particules aux propriétés surprenantes

Dans notre monde quotidien, une porte est soit ouverte, soit fermée. Dans l'infiniment petit, un atome ou un électron peut se trouver comme suspendu entre deux états possibles. Plus bizarre encore: des particules "jumelles" peuvent être si étroitement associées - les physiciens disent "intriquées" - qu'à des dizaines kilomètres de distance, toute action sur l'une est trahie par sa jumelle. Les physiciens exploitent ces propriétés pour garantir des communications inviolables ou permettre au rêve d'un ordinateur quantique de se concrétiser un jour...peut-être d'ici 10 ou 25 ans. "La cryptographie quantique, ça marche bien", déclare Philippe Grangier, de l'Institut d'optique de Palaiseau (Essonne), dont les travaux ont permis d'établir un lien ultra-sécurisé sur 18 km entre Thalès Palaiseau et Thalès Massy. "Nous avons une technique maison brevetée" qui permet de distribuer des clefs secrètes de chiffrage entre ici et Massy", précise-t-il.

L'information est codée sur une impulsion lumineuse contenant quelques photons (grains de lumière). Toute tentative d'intrusion "va la changer et ce changement sera détecté", explique ce chercheur. En 2008, le premier réseau de télécommunication sécurisé grâce à la cryptographie quantique a été réalisé à Vienne, entre six centres espacés jusqu'à 85 km, dans le cadre d'un projet européen. De la Suisse à l'Australie, des start up (Id Quantique, MagiQ Technologies, Sequrenet, Quintessence Labs) se sont lancées dans la distribution de clefs de cryptage garantissant l'inviolabilité de messages...même si un ordinateur quantique, doté d'une puissance de calcul permettant de casser les codes actuels, voit le jour. Avec la miniaturisation croissante de l'électronique, "en 2020, il n'y aura plus qu'un seul atome dans les éléments logiques d'un ordinateur", souligne M. Grangier. De grands progrès ont été faits pour manipuler individuellement atomes et autres particules. "On peut attraper un seul atome au bout d'un faisceau laser et coder de l'information à l'intérieur", ajoute-t-il. Ainsi piégés, deux atomes ultrafroids distants de 5 microns ont été "intriqués" au sein de son laboratoire. "On ne peut plus dire quel est l'état de chacun des atomes, si c'est 1 ou 0", précise le chercheur. Dans un ordinateur classique, la valeur d'un bit est soit 1, soit 0. Un bit quantique, c'est les deux à la fois. Cette faculté pour une particule d'être comme "suspendue" entre deux états laisse espérer des vitesses de calcul phénoménales. "Cela a été une vraie révolution de comprendre que si on ne manipulait plus des bits classiques mais des bits quantiques, un problème réputé difficile devenait facile", explique M. Grangier. Avec seulement 10 particules, mille composantes évolueraient en même temps lors des calculs, avec 30 particules on aurait 1 milliard de composantes, ce qui permet de "traiter en parallèle une quantité faramineuse d'informations", souligne son collègue Alain Aspect. Depuis quinze ans, différentes équipes testent l'utilisation d'atomes ultrafroids, d'ions, de supraconducteurs comme supports de bits quantiques. Guère plus de huit atomes participent aux calculs. "A petite échelle, ça marche de mieux en mieux", résume Philippe Grangier sans vouloir prédire quand l'ordinateur quantique pourrait exister.

afp.com