Contenu archivé le 2023-03-09

Des chercheurs démontrent la fiabilité de la cryptologie quantique

Des scientifiques belges et espagnols ont démontré pour la première fois que les nouveaux systèmes de cryptologie quantiques sont plus sûrs que les systèmes de sécurité actuels. Le soutien de l'UE provient du projet Q-ESSENCE («Quantum interfaces, sensors and communication bas...

Des scientifiques belges et espagnols ont démontré pour la première fois que les nouveaux systèmes de cryptologie quantiques sont plus sûrs que les systèmes de sécurité actuels. Le soutien de l'UE provient du projet Q-ESSENCE («Quantum interfaces, sensors and communication based on entanglement»), qui a reçu près de 5 millions d'euros au titre du thème Technologies de l'information et de la communication (TIC) du septième programme-cadre (7e PC), et du projet PERCENT («Percolating entanglement and quantum information resources through quantum networks»), soutenu à hauteur de 700 000 euros dans le cadre d'une subvention de démarrage du CER (Conseil européen de la recherche) au titre du 7e PC également. L'étude a été récemment publiée dans la revue scientifique Nature Communications.

En utilisant des clés générées par des particules quantiques, la transmission de données est garantie par les lois de la physique, selon les chercheurs de l'Université libre de Bruxelles (ULB) en Belgique et l'Institut de sciences photoniques de Barcelona, en Espagne. Les lois de mécanique quantique établissent que l'observation d'une particule dans son état quantique modifie cet état, ce qui signifie que dans les cas où les particules quantiques sont utilisées en tant que clés de transmission de données, toute forme d'espionnage peut être facilement et immédiatement détectée.

Comme les chercheurs l'ont fait remarquer dans leur article, un «problème central en cryptographie est la distribution entre utilisateurs distants de clés secrètes pouvant

être utilisées, par exemple, pour le cryptage de messages». Ils expliquent que «cette tâche est impossible en cryptographie classique à moins d'émettre des hypothèses sur la puissance informatique des espions. La distribution quantique de clés (ou cryptographie quantique), offre une sécurité contre les adversaires disposant d'une puissance informatique illimitée».

C'est le principe à l'origine de tous les systèmes de cryptographie quantique sur le marché, mais les failles dans la mise en oeuvre de ces systèmes constatées dans le passé les laissent vulnérables aux attaques des pirates quantiques, forçant les chercheurs à découvrir de meilleurs moyens de sécuriser les données. Selon les travaux menés par le post-doctorant Jonathan Barrett, des chercheurs de l'ULB ont développé une méthodologie qui n'était pas basée sur l'identification des changements de l'état quantique des particules.

Au contraire, les appareils quantiques étaient utilisés comme des boîtes noires pour recevoir et transmettre des données; si l'émetteur et le récepteur pouvaient détecter certaines corrélations entre les données produites par leurs boîtes respectives, la sécurité des clés quantiques était garantie. Ainsi, toute tentative d'espionnage de données devient complètement inutile et la sécurité de la transmission de données se place aux limites de notre compréhension actuelle des lois de physique.

Ce qui restait à prouver, néanmoins, était la fiabilité de cette nouvelle approche étant donné que les tests s'étaient concentrés sur quelques attaques limitées. Stefano Pironio de la faculté de sciences de l'ULB et Lluis Masanes et Antonio Acín de l'Institut de sciences photoniques à Barcelone ont démontré que cette nouvelle approche permettait de générer des clés à une vitesse raisonnable, comparable à celles utilisées dans les systèmes actuels, assurant ainsi la sécurité complète du système.

Les chercheurs ont écrit dans Nature Communications que leurs travaux offrent «un formalisme général de confirmation de sécurité» des protocoles de cryptographie quantique. «Cela est possible en termes de forte notion de sécurité, de sécurité universelle de composabilité, selon laquelle la clé secrète générée par le protocole est impossible à distinguer de la clé secrète idéale», expliquent-ils.

Bien que leurs preuves se basent sur une supposition mineure sur le fonctionnement des appareils quantiques, les résultats de cette recherche montre clairement que cette nouvelle approche est possible en principe, ouvrant ainsi la voie à des formes plus sûres de cryptographie quantique. Les auteurs concluent: «Nos travaux contribuent à combler l'écart entre les preuves de sécurité théoriques et les réalisations pratique de cryptographie quantique».Pour de plus amples informations, consulter: ULB: http://www.ulb.ac.be Nature Communications: http://www.nature.com/ncomms Q-ESSENCE: http://qurope.eu/projects/qessence

Pays

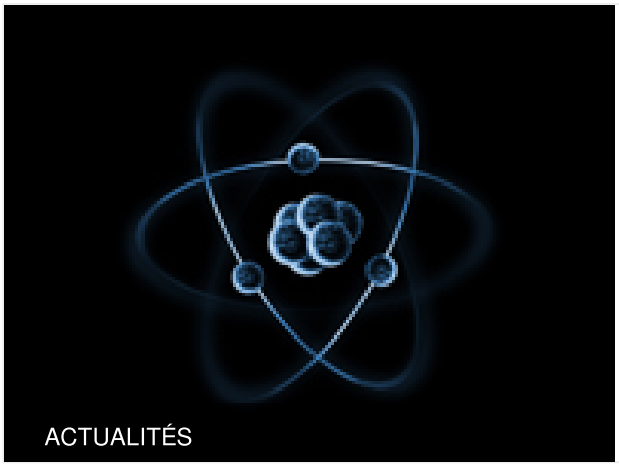
Belgique, Espagne

Cet article apparaît dans...

MAGAZINE RESEARCH*EU

Des modes de transports innovants: où serions-nous sans nos voitures?

Articles connexes



Des scientifiques dépassent la sensibilité des mesures quantiques

4 Avril 2011

Le feu des projecteurs sur les projets de l'UE en matière de confiance et de sécurité

18 Février 2010

Dernière mise à jour: 31 Mars 2011

Permalink: https://cordis.europa.eu/article/id/33258-researchers-prove-safety-of-quantum-cryptology/fr

European Union, 2025