Réputée inviolable, la sécurité « quantique » a été hackée

- Informatique - Sécurité Informatique -

Date de mise en ligne : mardi 31 août 2010

Spyworld Actu

Une équipe de chercheurs a réussi à intercepter un message sur un réseau quantique, alors que cette technologie est censée être la plus sûre du monde.

La cryptographie est la science du secret. La cryptographie « quantique », une discipline mettant en pratique les propriétés de la mécanique quantique dans le but de protéger certaines transmissions de données très sensibles. Pour le moment, rien ne permet d'égaler le niveau de sécurité atteint par ces systèmes (cette technologie arrive tout juste à maturité et n'a donc pas été encore largement mise en oeuvre). On les a même longtemps pensé inattaquables. C'était sans compter sur l'acharnement de chercheurs norvégiens, allemands et espagnols qui viennent de mettre en défaut les deux principaux systèmes quantiques commercialisés. Leurs travaux sont publiés dimanche dans la revue Nature Photonics.

Lorsque deux personnes veulent communiquer secrètement (on appelle généralement l'émettrice « Alice » et le récepteur « Bob » l'espionne est appelée « Eve »), elles s'envoient des messages codés. Pour les décrypter, il faut que les deux personnes disposent de la « clé » qui permettra de les déchiffrer. Au départ seule Alice la détient. Et il ne faut surtout pas qu'elle soit interceptée quand elle est envoyée à Bob. C'est là que la cryptographie quantique intervient. Alice envoie la clé sous forme de photons émis un par un dans une fibre optique (une prouesse technologique particulièrement difficile). Bob réceptionne ces photons et mesure leurs propriétés. Ce sont elles qui vont lui permettre de reconstituer la clé. Pour s'en emparer, Eve doit elle aussi observer ces photons sans laisser de trace suspecte. Or la physique quantique explique qu'il est impossible d'observer un photon sans en modifier les propriétés. C'est le célèbre principe d'incertitude d'Heisenberg. En d'autres termes, Alice et Bob peuvent, en s'échangeant des informations par un canal standard, détecter immédiatement toute tentative d'espionnage : la cryptologie quantique est théoriquement inviolable.

Les deux principaux systèmes commercialisés mis en défaut

Si personne ne peut mettre en défaut la théorie, la mise en oeuvre pratique n'est manifestement pas exempte de failles. Les mêmes chercheurs norvégiens avaient en effet montré en 2009 que l'utilisation d'une lumière laser pouvait perturber le détecteur censé donner l'alerte. En émettant un flash très bref, les Norvégiens avaient démontré qu'ils pouvaient « aveugler » ce compteur de photons. En implémentant cette méthode, ils ont réussi à récupérer l'intégralité de la clé sans déclencher la moindre alerte. Il aura tout de même fallu aux chercheurs plus de deux mois pour mettre en place leur « mouchard » sur les deux systèmes de cryptographie quantique les plus commercialisés au monde. Mais l'essentiel est là : la cryptographie quantique est vulnérable.

« Au final, nos travaux vont permettre de renforcer ces systèmes », appuie Vadim Makarov un des auteurs norvégiens de l'étude. Les chercheurs ont en effet travaillé en étroite collaboration avec la société leader du secteur afin qu'ils puissent apporter des modifications à leur produit avant la publication des résultats de l'étude. « La cryptographie quantique reste le nec plus ultra de la sécurité », conclut le chercheur.

Post-scriptum :

http://www.lefigaro.fr/sciences-tec...