Cryptographie quantique : le protocole qui échappe aux espions

En théorie, la physique quantique fournit les moyens de rendre impossible à déchiffrer un message, même s'il est intercepté. En pratique, les dispositifs mobilisés présentent usuellement des failles de sécurité. Sauf à mettre en œuvre un protocole nouveau, s'appuyant sur le « jeu de Bell » : la protection est garantie même si les dispositifs sont contrôlés par un espion.

Depuis des millénaires, les dirigeants et les militaires se sont posé une question difficile. Comment communiquer – envoyer des informations sensibles – et s'assurer que, si les messages tombaient entre des mains ennemies, ils ne livrent pas leurs secrets ? Le problème touche aussi bien les rapports qu'une ambassade transmet par des canaux diplomatiques à son ministère de rattachement que des ordres délivrés sur un champ de bataille. Mais à l'ère de l'information, avec le développement des réseaux de télécommunications, cette question s'applique également à des données plus personnelles, comme les bilans de santé, les transactions bancaires, etc.

LIRE L'ARTICLE