Dieks), s'applique également aux chaînes de qubits, représentant par exemple des mots ou des phrases. En conséquence, quelqu'un qui espionnerait un canal quantique (typiquement une fibre optique transportant des photons dans des états de polarisation multiple) ne pourrait intercepter la communication sans la perturber et ainsi révéler l'intrusion.

Il existe plusieurs techniques de cryptage quantique pour échanger des données en toute confidentialité, grâce à la propriété de non-clonage. Mais elles supposent que les destinataires soient autorisés à lire les données que vous envoyez : le simple fait d'envoyer une requête à Google à travers un canal quantique ne résoudra pas le problème.

DES REQUÊTES CONFIDENTIELLES

Cependant, en 2008, avec Lorenzo Maccone, de l'université de Pavie, et Vittorio Giovannetti, de l'École normale supérieure de Pise, nous avons découvert que le théorème de non-clonage autorise aussi des requêtes confidentielles. Dans le protocole que nous avons conçu, un utilisateur doit être capable d'envoyer au moteur de recherche une « question quantique » : une chaîne de qubits qui contient simultanément la bonne question et une autre, peu importe laquelle.

Le moteur de recherche trouve les réponses à vos questions multiples et y répond sous forme d'un paquet quantique qu'il vous renvoie. Si le moteur de recherche fait une copie de vos questions pour ses archives, vous saurez que la confidentialité a été violée parce que l'état quantique de vos questions d'origine aura subi une perturbation détectable par votre ordinateur. Point essentiel, le moteur de recherche peut apporter des réponses sans détecter physiquement (et à plus forte raison sans cloner) la chaîne de qubits qui encode les questions, et donc sans savoir quelles étaient les questions.

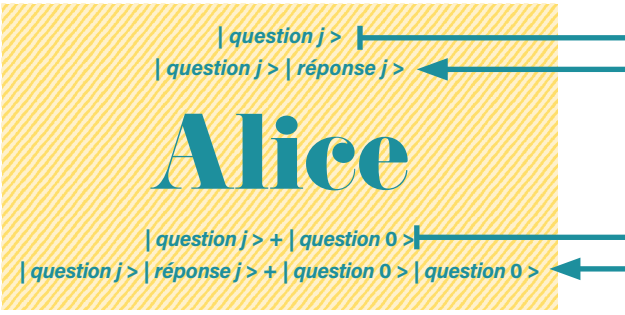
Même si un tel tour de force est impossible avec les ordinateurs, les bases de données et les matériels de mise en réseau dont nous disposons actuellement, nous nous sommes aperçus qu'il n'est pas, techniquement, hors de portée.

La première exigence pour formuler des requêtes privées quantiques est un internet quantique rudimentaire. La technologie pour échanger des messages quantiques sur une ligne dédiée existe déjà et est utilisée pour sécuriser les communications. Cependant, un internet quantique à part entière ne sera pas une simple ligne entre deux points, mais devra constituer un réseau dont les nœuds aiguillent les paquets de données de sorte que chaque utilisateur puisse atteindre tout autre utilisateur ou tout serveur web. Il s'avère qu'aiguiller des données sans en faire de copies temporaires (et donc sans souffrir des conséquences du théorème de non-clonage) est une tâche non triviale, et nécessite une technologie complexe qui n'en est qu'au stade expérimental : le routeur quantique.

C'est ce qu'ont réussi à fabriquer en 2021 Matteo Pompili, de l'université de technologie de Delft, aux Pays-Bas, et ses collègues. Ils ont conçu un réseau quantique doté de… trois nœuds (les routeurs) reliant des qubits constitués de centres NV (pour *Nitrogen vacancy*), c'est-à-dire des impuretés (un atome d'azote et une lacune, dans le réseau cristallin d'un diamant).

La deuxième exigence pour effectuer avec confidentialité des recherches sur internet est que les utilisateurs et les serveurs de données soient dotés d'ordinateurs quantiques rudimentaires, capables de stocker et de manipuler des qubits. Malheureusement, les qubits sont instables et ont tendance à perdre

Si le moteur de recherche fait une copie de vos questions, vous le saurez tout de suite. Confidentialité garantie !



spontanément leur superposition quantique en une fraction de seconde.

Les ordinateurs quantiques expérimentaux qui stockent des qubits sous la forme d'états magnétiques d'ions simples suspendus dans le vide, par exemple, ne peuvent pour l'instant stocker qu'environ 20 qubits à la fois. Un ordinateur quantique abouti nécessiterait des centaines, voire des milliers, de qubits, et cela ne se fera probablement pas avant plusieurs décennies, même en version expérimentale. Par chance, dans l'optique de requêtes quantiques à caractère personnel, une trentaine de qubits devraient suffire : bien codée, une requête de 30 qubits peut extraire une réponse dans une base de données contenant plus d'un milliard d'entrées. Or les dernières avancées parviennent à intriquer 53 qubits lorsqu'il s'agit de supraconducteurs et 51 avec des atomes neutres.

ON RAME POUR LA RAM

Pour l'instant, tout a l'air de bien rouler : les requêtes confidentielles quantiques semblent n'exiger que de très simples ordinateurs et systèmes de communication quantiques. Mais c'est maintenant que cela se complique. Pour répondre à une requête quantique à plusieurs volets, la base de données du moteur de recherche doit être capable de fournir simultanément la réponse à chaque composante de la question. Pour cela, il faudra un nouveau type de stockage de données nommé « mémoire vive quantique », ou RAM (*Random Access Memory*, soit mémoire à accès aléatoire) quantique.

La mémoire vive est juste un dispositif servant à stocker les données, rangées selon une structure arborescente. Chaque élément de donnée est une séquence de huit bits, ou octet, et est affecté d'une adresse qui est elle-même une séquence de bits. Les octets sont comme les feuilles de l'arbre, tandis que l'adresse contrôle le chemin qui va du tronc à une feuille donnée. Le premier bit de l'adresse spécifie laquelle des deux branches suivre au niveau le plus bas de l'arbre, le deuxième bit contrôle l'embranchement du deuxième niveau, et ainsi de suite. Les branches se dédoublent à chaque niveau et, dans une mémoire vive traditionnelle avec des adresses à 30 bits, il faut actionner 2^{30} (plus de 1 milliard) commutateurs pour récupérer les données.

On peut imaginer une version quantique de la mémoire vive traditionnelle. La seule différence est que les interrupteurs qui aiguillent l'information dans l'arbre binaire doivent maintenant être capables d'acheminer l'information le long de deux branches différentes simultanément, puisque chaque bit d'une question quantique peut spécifier deux chemins différents. On peut construire de tels commutateurs quantiques avec les techniques existantes, comme les miroirs semi-transparents qui « scindent » les photons en leur faisant suivre deux trajectoires à la fois. Le problème est que les circuits quantiques sont excessivement sensibles au bruit et aux erreurs : il suffit qu'un des commutateurs soit défaillant pour que la confidentialité du qubit correspondant soit perdue. Un bit d'adresse contrôlant un nombre énorme de commutateurs, les risques de perdre la confidentialité sont très élevés.

Avec Lorenzo Maccone et Vittorio Giovannetti, nous avons proposé un concept différent pour l'adressage d'une mémoire vive (classique comme quantique), où beaucoup moins de commutateurs sont mis en jeu pour chaque appel à la mémoire. L'idée est d'aiguiller les bits d'adresse le long des mêmes branches d'arbre que vont devoir suivre les données, plutôt qu'à travers des lignes d'adressage séparées. Comme les bits d'adresse passent séquentiellement à travers le réseau, nous appelons cela une mémoire vive en « brigade de seaux » (de l'anglais *bucket brigade*).

UNE BRIGADE DE SEAUX

L'architecture en brigade de seaux n'impose d'actionner qu'un seul commutateur à chaque niveau du réseau, alors que la mémoire vive ordinaire actionne tous les commutateurs à tous les niveaux *(voir l'encadré page 118)*. Le gain est remarquable : une mémoire vive à brigade de seaux ayant un milliard d'emplacements de mémoire actionne 30 commutateurs pour