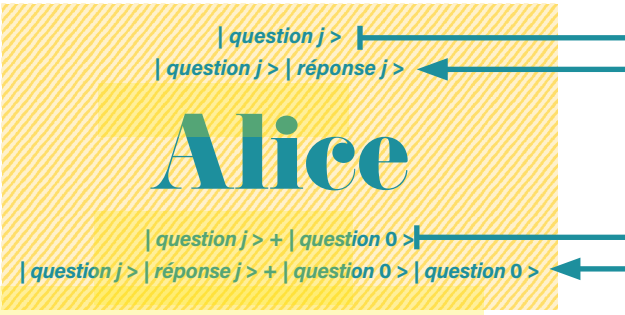


spontanément leur superposition quantique en une fraction de seconde.

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.

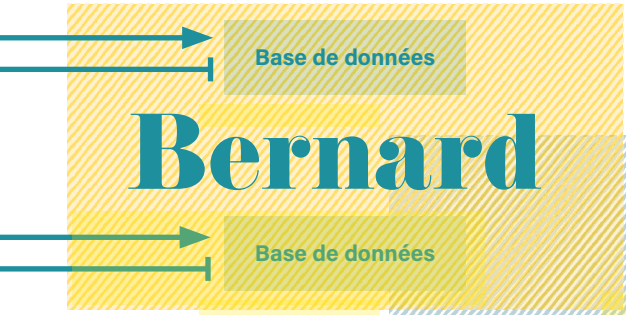
La mémoire vive est juste un dispositif servant à stocker les données, rangées selon une structure arborescente. Chaque élément de donnée est une séquence de huit bits, ou octet, et est affecté d'une adresse qui est elle-même une séquence de bits. Les octets sont comme les feuilles de l'arbre, tandis 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



LE PROTOCOLE QUANTIQUE DE CONFIDENTIALITÉ DES REQUÊTES

Comment garantir la confidentialité des requêtes sur internet ? Décrivons le protocole quantique proposé par Seth Lloyd et ses collègues italiens. On suppose qu'Alice effectue des requêtes dans la base de données de Bernard, et qu'elle ne souhaite pas que Bernard sache de quelle requête il s'agit. Dans ce qui suit, la notation de Dirac $|message\rangle$ signifie qu'un message binaire (une suite de 0 ou 1) a été placé dans un registre de mémoire quantique (formé de bits quantiques). Ainsi, la notation $|question\ j\rangle$ signifie qu'Alice souhaite découvrir le $j^{\text{-ième}}$ enregistrement dans la base de données de Bernard. Alice utilise un registre de mémoire contenant n bits quantiques, ce qui lui permet d'effectuer 2^n requêtes distinctes. On suppose qu'Alice connaît le contenu $|réponse\ 0\rangle$ d'un registre de référence, qui est la réponse à la requête $|question\ 0\rangle$. Afin de vérifier que Bernard ne l'espionne pas, Alice soumet deux requêtes successives dans un ordre arbitraire, non connu de Bernard, et attend la réponse après chacune d'elles. Chaque requête est placée dans un registre quantique à n bits quantiques. Par exemple, elle choisit comme première requête $|question\ j\rangle$, tandis que la seconde requête est la superposition quantique : $|question\ j\rangle + |question\ 0\rangle$, qui lui permettra *a posteriori* de vérifier si, oui ou non, Bernard a tenté de découvrir quelle était sa requête. Une fois reçue la première requête, $|question\ j\rangle$, la base de données de Bernard retourne, grâce à l'utilisation d'une RAM quantique, la réponse $|réponse\ j\rangle$. Cette réponse est véhiculée par un second registre quantique, accolé à la question d'Alice. Autrement dit, Alice reçoit le message : $|\psi_1\rangle = |question\ j\rangle\ |réponse\ j\rangle$. Alice envoie ensuite sa seconde requête $|question\ j\rangle + |question\ 0\rangle$. L'interrogation de la base de données de Bernard a pour résultat de renvoyer à Alice sa seconde requête complétée par les réponses, sous la forme : $|\psi_2\rangle = |question\ j\rangle\ |réponse\ j\rangle + |question\ 0\rangle\ |réponse\ 0\rangle$. Bernard ne sait jamais si le registre qu'il reçoit d'Alice est celui contenant la superposition, ou l'autre registre, ce qui signifie qu'il ne peut pas extraire l'information sur j sans risquer de perturber le registre. À la fin du protocole de communication, Alice mesure le contenu du second registre de $|\psi_1\rangle$ pour déterminer $|réponse\ j\rangle$. Elle peut alors utiliser cette réponse pour vérifier que la superposition du second état $|\psi_2\rangle$ a été préservée. Si ce n'est pas le cas, elle sait en vertu du théorème de non-clonage quantique que Bernard a tenté de connaître sa requête. Le protocole quantique de confidentialité des requêtes est en fait très similaire à un protocole de cryptographie quantique, qui permet l'échange sécurisé de clés secrètes.

Michel Planat
Institut FEMTO-ST, Besançon