Je me sentais un peu en décalage ce jour où je me suis retrouvé à la table de milliardaires. Mon rôle était sans doute de divertir ceux qui s'intéressaient au monde quantique. Parmi les invités se trouvaient Sergey Brin et Larry Page, les fondateurs de Google. À ma surprise, ils en savaient long sur l'information quantique. Après quelques échanges sur la façon dont la physique quantique changera l'usage d'internet, je suggérai alors de travailler sur des « requêtes quantiques sur internet » qui mettraient en péril le modèle économique de la firme, car les internautes deviendraient invisibles. Rêve ou utopie ?

La confidentialité est de fait rare à notre époque, en particulier sur internet où, à chaque fois que nous cherchons quelque chose sur Google, nos requêtes sont enregistrées pour la postérité – ou du moins pour les annonceurs. Les fournisseurs d'accès affirment protéger la vie privée de leurs clients en cryptant les informations personnelles. Mais les méthodes employées ne sont pas toujours efficaces.

Les lois de la physique arrivent à la rescousse. Les communications sur des « canaux quantiques » permettent déjà aux banques et à d'autres institutions d'envoyer des données avec un cryptage pratiquement inviolable. Ainsi, il existe déjà des techniques cachant nos requêtes à des indiscrets qui risqueraient de les intercepter. Mais à l'avenir, grâce à l'internet dit « quantique », tout un chacun enverra des requêtes et recevra des réponses avec l'assurance que personne, pas même Google, ne sache quelles questions ont été posées. De plus, les mêmes techniques qui garantiront la confidentialité des requêtes fonctionneront pendant toute la durée de la connexion.

Bien sûr, les moteurs de recherche sauvegardent et analysent les données des utilisateurs afin d'afficher des publicités ciblées. C'est ainsi qu'ils rentrent dans leurs frais et font des bénéfices. S'ils décident de garder secrètes les données des utilisateurs, les moteurs de recherche auront besoin d'un nouveau modèle commercial. Et les utilisateurs décideront eux-mêmes s'ils sont prêts à payer leurs recherches ou s'ils préfèrent la gratuité… au prix de leur anonymat.

En bref

> Quand un internaute navigue sur la Toile, même de façon anonyme, des informations personnelles peuvent être extraites par d'autres acteurs.

> Grâce à une version quantique d'internet, les moteurs de recherche fourniront les réponses aux requêtes avec l'assurance que personne n'a sauvegardé ou copié les données.

> De telles requêtes quantiques nécessiteront pour les bases de données un nouveau type de stockage de mémoire qui fait déjà ses preuves en laboratoire.

LE THÉORÈME DE NON-CLONAGE

La capacité de la physique quantique à procurer une confidentialité totale découle d'un fait très simple : les systèmes quantiques peuvent exister dans des états multiples, superposés. À tout instant, un atome peut se trouver en différents endroits, un photon polarisé à la fois horizontalement et verticalement, le moment magnétique d'un électron pointer vers le haut et vers le bas, et ainsi de suite.

Par conséquent, alors qu'un bit de donnée classique enregistre soit la valeur 0, soit la valeur 1, un bit quantique (ou qubit) peut représenter les deux valeurs 0 et 1 en même temps. Qui plus est, dans ce cas, on ne peut pas réaliser une copie exacte de ce qubit, et toute tentative en ce sens changera l'état du qubit. Cette règle, connue sous le nom de « théorème de non-clonage » (défini en 1982 par William Wootters, Wojciech Zurek et Dennis

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 !