

Base de données

Bernard

Base de données

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 $|\text{message}\rangle$ 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 $|\text{question } j\rangle$ signifie qu'Alice souhaite découvrir le j -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 $|\text{réponse } 0\rangle$ d'un registre de référence, qui est la réponse à la requête $|\text{question } 0\rangle$. 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 $|\text{question } j\rangle$, tandis que la seconde requête est la superposition quantique : $|\text{question } j\rangle + |\text{question } 0\rangle$, 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, $|\text{question } j\rangle$, la base de données de Bernard retourne, grâce à l'utilisation d'une RAM quantique, la réponse $|\text{réponse } j\rangle$. Cette réponse est véhiculée par un second registre quantique, accolé à la question d'Alice. Autrement dit, Alice reçoit le message : $|\psi_1\rangle = |\text{question } j\rangle |\text{réponse } j\rangle$. Alice envoie ensuite sa seconde requête $|\text{question } j\rangle + |\text{question } 0\rangle$. 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 : $|\psi_2\rangle = |\text{question } j\rangle |\text{réponse } j\rangle$

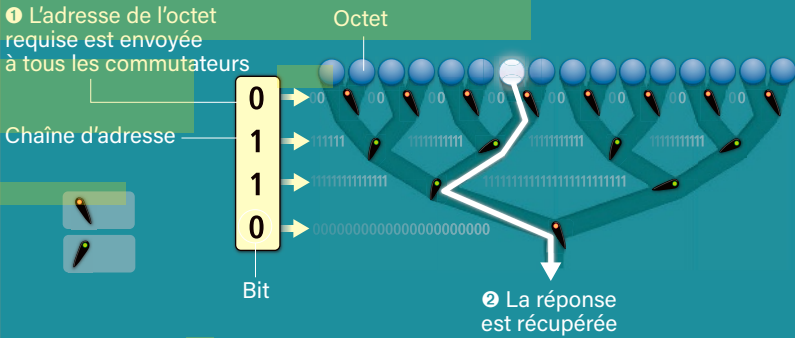
+ $|\text{question } 0\rangle |\text{réponse } 0\rangle$. Bernard ne sait jamais si le registre qu'il reçoit d'Alice est celui contenant la superposition, ou l'autre registre, ce qui signifie qu'il ne peut pas extraire l'information sur j sans risquer de perturber le registre. À la fin du protocole de communication, Alice mesure le contenu du second registre de $|\psi_2\rangle$ pour déterminer $|\text{réponse } j\rangle$. 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

Une mémoire vive quantique

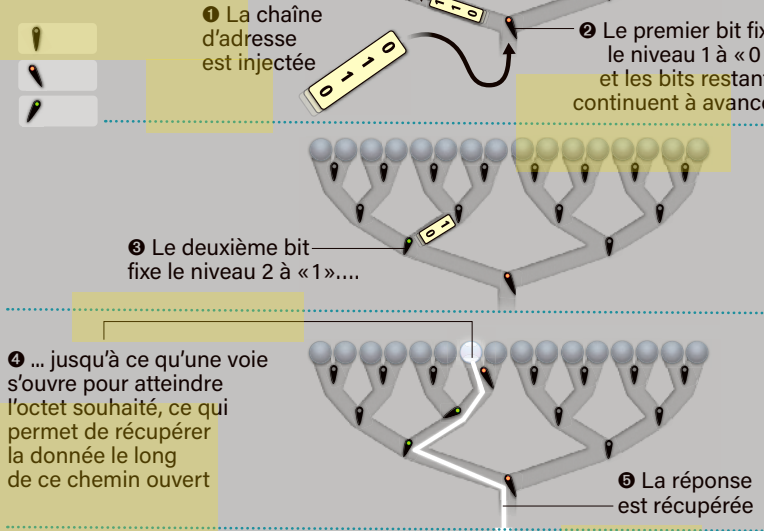
Afin d'offrir une confidentialité absolue, les moteurs de recherche stockeront l'information concernant le contenu de la Toile dans une mémoire vive (ou RAM) quantique. Les utilisateurs enverront des requêtes multiples sous forme d'un unique « paquet quantique ». La RAM quantique ajoutera les réponses au paquet et le renverra. Toute perturbation dans l'état quantique du paquet alertera l'utilisateur, qui saura ainsi s'il y a eu violation de la confidentialité. La RAM quantique nécessitera de remplacer l'architecture RAM ordinaire par une architecture dite « en brigade de seaux ».

Dans une RAM ordinaire, les octets de données sont disposés en arbre. La récupération d'un octet de données impose d'actionner tous les commutateurs du réseau. Pour une RAM quantique, il ne serait pas réaliste d'actionner un grand nombre de commutateurs : en raison de la fragilité des états quantiques, le taux d'erreurs serait trop élevé.



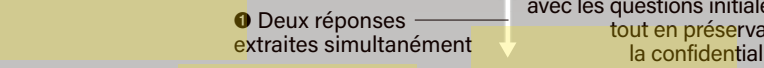
RAM À BRIGADE DE SEAUX

Dans cette architecture, l'extraction d'un octet ne mobilise que les commutateurs d'un seul chemin.



VERSION QUANTIQUE

Dans une RAM quantique à brigade de seaux, deux chemins peuvent être ouverts afin de récupérer deux données, qui seront renvoyées avec les questions initiales.



du problème de la connexion de la mémoire vive quantique à des canaux de communication quantique. Mais aucune de ces difficultés ne paraît insurmontable.

D'ailleurs, Francesco De Martini et son équipe de l'université de Rome-La Sapienza ont construit une RAM quantique très simple au moyen de lasers, de polariseurs et de détecteurs de photons. Le groupe a fait la démonstration de notre protocole de requêtes sur une petite base de données. Les requêtes confidentielles quantiques sont donc une possibilité réelle.

À leur suite, en 2021, avec des collègues de l'institut de technologie du Massachusetts, à Cambridge, nous avons également proposé une architecture de circuit intégré photonique pour bâtir une RAM quantique. Ici, les qubits sont fondés sur des impuretés (un atome cette fois de silicium et une lacune) dans un réseau cristallin de diamant.

Par ailleurs, nous avons récemment remarqué que les techniques d'acheminement des données de notre concept de RAM quantique s'appliquent aussi aux réseaux de commutation de l'ensemble de l'internet quantique. Les internautes navigueraient alors sur la Toile incognito, sans révéler ce qu'ils recherchent ni quels sites web ils visitent. Est-ce la fin annoncée de Google ?

chaque requête, par opposition au milliard de commutateurs actionnés pour chaque requête dans une mémoire RAM classique. Et les avantages de l'architecture en brigade de seaux, en termes à la fois de taux d'erreurs et d'économies d'énergie, augmentent exponentiellement avec le nombre de bits.

Dans un premier temps, nous pensions que l'idée de la brigade de seaux avait le potentiel de révolutionner l'industrie des RAM classiques. Mais nous découvrîmes bientôt que d'autres chercheurs avaient déjà eu des idées similaires et que de toute façon le concept était trop lent pour une RAM classique.

LA FIN ANNONCÉE DE GOOGLE

Mais le concept en brigade de seaux serait crucial pour les requêtes quantiques, parce que son architecture peut tolérer un taux d'erreurs de un pour 30, plutôt que de un pour un milliard. Le matériau à mémoire pour une RAM quantique pourrait être un support physique classique, comme un DVD classique. La partie véritablement quantique de la RAM quantique est le réseau de commutateurs, chacun devant aiguiller les bits quantiques le long des deux branches à la fois. De tels commutateurs quantiques existent déjà et atteignent des taux d'erreurs suffisamment faibles pour construire une RAM quantique dotée d'un milliard d'emplacements de mémoire, ou davantage.

Bien sûr, l'assemblage de commutateurs quantiques suffisamment nombreux pour obtenir une mémoire quantique de grande capacité sera probablement ardu, sans parler

— L'auteur —

> Seth Lloyd

est professeur de génie mécanique à l'institut de technologie du Massachusetts (MIT), à Cambridge, aux États-Unis.

— À lire —

> **M. Pompili et al.**, Realization of a multinode quantum network of remote solid-state qubits, *Science*, vol. 372(6539), pp. 259-264, 2021.

> **K. C. Chen et al.**, Scalable and high-fidelity quantum random access memory in spin-photon networks, *ArXiv*: 2103.07623, 2021.

> **T. Meunier**, La course aux bits quantiques, *Hors-Série Pour la Science*, n° 107, pp. 78-85, 2020.

À VISITER

Beauté intemporelle

Une exposition à Rodez réunit des statuettes de l'âge du Bronze et les confronte à des œuvres du xx^e siècle qu'elles ont influencées.

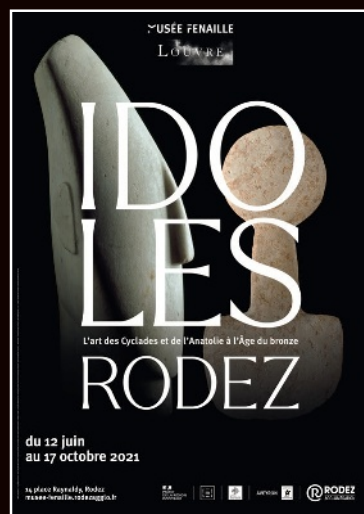
Découvertes au xix^e siècle dans les Cyclades grecques et en Anatolie (Turquie), des « idoles », ces statuettes anthropomorphes souvent en marbre, ont d'abord été attribuées à des sociétés peu évoluées, voire primitives.

Cette vision a changé au gré des découvertes archéologiques et on sait désormais qu'elles sont les vestiges précieux de civilisations complexes, prises dans des réseaux denses de commerce et d'échanges culturels.

En réunissant un ensemble unique d'œuvres prêtées par des institutions prestigieuses, comme le Louvre, le musée Fenaille, à Rodez, témoigne de ce revirement. En les associant aux pièces emblématiques de ses collections permanentes, notamment des statues-menhirs de plusieurs millénaires, l'établissement aveyronnais invite le visiteur à réfléchir à l'évolution de la représentation de la figure humaine et à son expression dans les sociétés du passé.

Avec le temps, la beauté de ces statuettes, très épurées ou au contraire plus naturalistes, s'est imposée aux yeux de tous, spécialistes comme profanes, ainsi qu'aux artistes modernes du début du xx^e siècle comme Constantin

Brancusi, Jean Arp, Alberto Giacometti, Ossip Zadkine ou Brassaï, dont certaines œuvres aussi exposées dénotent une influence de l'art cycladique évidente. Ce voyage dans le temps et l'espace révèle ce que le sculpteur britannique Henry Moore appelait un « langage mondial commun des formes ».



« Idoles. L'art des Cyclades et de l'Anatolie à l'Âge de bronze », musée Fenaille, 12000 Rodez. Jusqu'au 17 octobre 2021 <https://bit.ly/3i9cogV>

À ÉCOUTER

À quand le Covid-31?

Comment (bien) vivre avec les moustiques? Les zoonoses vont-elles s'intensifier? Quelle viande mangerons-nous demain? Les réponses sont à retrouver dans les premiers épisodes de *Zootopique*, un podcast d'anticipation conçu par l'Anses. L'idée est de projeter l'auditeur en 2031 pour interroger les liens entre santé humaine et santé animale. Pour ce faire, des chercheurs présentent les travaux les plus récents sur la façon de prévenir les risques de demain. Parce que la santé des uns passe par celle de tous.

<https://bit.ly/3g8h18G>



À LIRE

Six feet under

Nous marchons dessus tous les jours, et pourtant nous le connaissons si mal! Quoi? Le sol! Dans *Sous terre* (Dargaud, 176 pages, 19,99 euros, 2021), Mathieu Burniat, conseillé par Marc-André Selosse, met en scène cette fine couche à la surface de la Terre où la vie grouille. Cette bande dessinée dévoile à travers un palpitant récit d'aventures la richesse et l'importance de ce sol sur le climat, le cycle de l'eau, l'alimentation... En un mot, il est indispensable à la survie des humains. Alors autant en prendre soin! C'est le vœu que formule l'auteur.

<https://bit.ly/3uRyHdv>