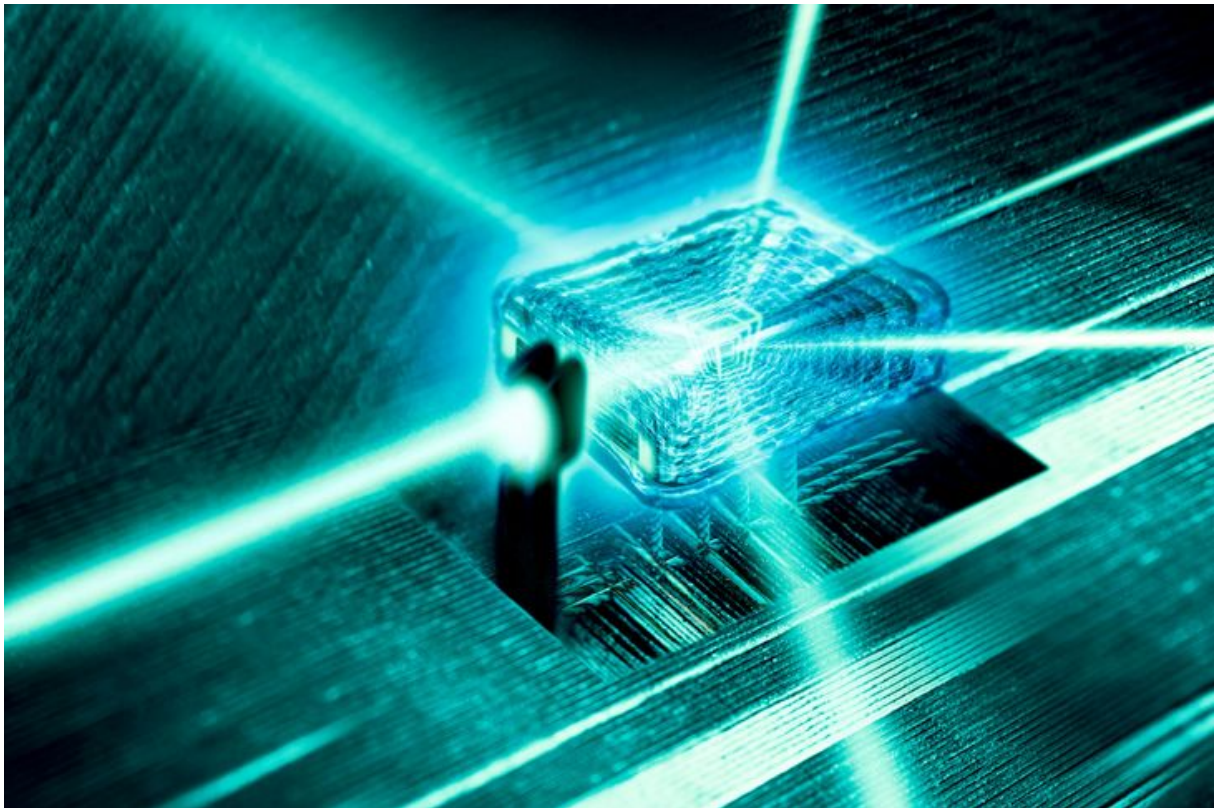
Comprendre (un peu mieux) l'ordinateur quantique

La France s'est dotée d'un plan stratégique sur l'informatique quantique, une technologie de pointe assez complexe à comprendre.

- Audrey Dufour,
- le 03/05/2021 à 14:41



Un cœur d'ordinateur quantique, utilisant des faisceaux lasers pour le transport d'informations.

Pas un mois sans qu'un grand groupe annonce une *« révolution »* concernant l'ordinateur quantique. Qu'il s'agisse d'un record de mystérieux *qubits*, de puissance de calcul inégalée ou de capteurs haute précision, le quantique est partout. Fin janvier, Emmanuel Macron a annoncé un « plan stratégique » dans le domaine, avec 1,8 milliard d'euros étalé sur cinq ans. Mais de quoi parle-t-on ?

► Quelle est la différence avec un ordinateur classique ?

Un ordinateur quantique fonctionne, comme son nom l'indique, grâce aux propriétés de la physique quantique, laquelle règne sur l'infiniment petit. *« Cette idée d'utiliser la mécanique quantique, connue depuis plus d'un siècle, a émergé dans les années 1980 »*, raconte Denis Vion, spécialiste en électronique quantique au Commissariat à l'énergie atomique de Saclay. L'ordinateur quantique s'appuie sur le phénomène de

superposition, qui veut qu'une particule quantique puisse être dans plusieurs états à la fois.

Pour comprendre, revenons à un ordinateur classique. Celui-ci fonctionne selon un système binaire où des bits, des unités d'information de base, ne peuvent prendre que la valeur 0 ou la valeur 1. Les machines classiques effectuent donc les opérations très rapidement, mais les unes après les autres. C'est comme si pour trouver les facteurs de 21, vous passiez en revue 1 × 1, 1 × 2, 1 ×3 etc. jusqu'à aboutir à 3 × 7. La physique quantique permet, elle, un parallélisme grâce à la superposition : un bit quantique, appelé *qubit*, peut être 0, 1, mais également *les deux à la fois*. Imaginez que vous ne possédez que des feutres bleu et jaune, et qu'on vous donne un feutre vert. Dessiner de l'herbe devient plus facile.

Dans le cas de deux qubits ou plus, on peut même obtenir des états superposés très particuliers, nommés « états intriqués ». Les qubits sont alors liés les uns aux autres d'une façon qui n'existe pas dans le monde classique et permettent d'accélérer le calcul. « *Sans intrication, on retombe sur un supercalculateur classique* », précise Christophe Vuillot, membre de l'équipe Mocqua (Modèles de calculs émergents), à l'Inria, Institut de recherche en technologies du numérique.

► À quoi sert une machine quantique ?

« À réaliser rapidement des opérations massivement parallèles et donc attaquer des mathématiques complexes avec un temps de traitement réduit, indique Sébastien Tanzilli, directeur de recherche au CNRS et spécialiste des technologies quantiques. *C'est comme si vous passiez d'une montagne avec une ascension à 45° à une petite colline en pente douce. »* Les deux premiers usages de l'informatique quantique se résument pour l'instant à la recherche dans de grandes listes de données non triées, et à la factorisation, notamment pour la cryptographie.

Pour les listes non triées, imaginez-vous chercher à qui appartient un numéro de téléphone avec un bottin papier. Vous devez parcourir un à un les noms pour voir si le numéro correspond, une tâche fastidieuse. Utiliser un ordinateur quantique reviendrait à utiliser l'annuaire inversé : vous rentrez le numéro et pouf, le nom correspondant apparaît. Une amélioration qui a de quoi intéresser Google !

L'ordinateur quantique, un rêve prochain

Pour la factorisation, si l'on reprend le 21, une machine quantique fera défiler toutes les possibilités en même temps, telle une machine à sous, pour aboutir directement à 3 × 7. À noter qu'avec une opération aussi simple, l'avantage quantique n'existe pas : un ordinateur classique va déjà bien assez vite. Dans l'ensemble, pour vous et moi, un futur ordinateur quantique ne servira à rien. « *L'ordinateur quantique servira uniquement pour des problèmes très complexes* », reconnaît Sébastien Tanzilli. Et attention, *« il existe plein de choses que le quantique ne sait pas ou pas bien faire et qu'il n'a pas vocation à calculer »*, rappelle Cyril Allouche, à la tête de la recherche et de l'innovation en quantique chez Atos. Le groupe français a d'ailleurs mis en place un « Q-Score » pour mesurer s'il y a réellement une « performance quantique ».

Sundar Pichai (à gauche), PDG de Google, visite l'un des laboratoires d'informatique quantique du groupe américain, à Santa Barbara, en Californie, en octobre 2019. / Handout/Reuters

Une fois pleinement opérationnels, ces ordinateurs pourront aussi résoudre des questions d'optimisation, comme « le problème du voyageur de commerce ». « *Si vous partez avec une liste de villes à visiter, il devient compliqué de calculer le trajet le plus court à partir de dix villes. Au-delà de 60 villes, même le plus puissant supercalculateur au monde bloquera, contrairement au quantique*, décrit Elie Girard, directeur général

d'Atos. *Les besoins de simulation justifient l'informatique quantique.* » Idéal pour la gestion logistique. En chimie, la synthèse de très grosses molécules, pour les médicaments par exemple, serait aussi grandement facilitée. Côté météo, on pourrait enfin tenir compte des multiples et fines variations pour améliorer les prévisions. Et en intelligence artificielle, certains imaginent déjà des robots raffinés, plus proches d'une intelligence humaine.

► Quelles sont les limites des machines quantiques ?

Déjà, rappelons qu'il n'existe pour l'instant aucun ordinateur quantique digne de ce nom, malgré certaines annonces tonitruantes. *« Les calculateurs quantiques restent de petite taille et ne corrigent pas leurs erreurs »,* abonde Sébastien Tanzilli.

Ensuite, il faut comprendre que le monde quantique est très fragile, et interagir avec lui provoque une perturbation. On parle de « décohérence » : dès que l'on observe la machine, qu'elle interagit avec l'extérieur, les superpositions quantiques disparaissent. *« Cette décohérence n'est pas grave lorsque l'on mesure, puisqu'on cherche le résultat*, intervient Denis Vion. *Par contre, si les qubits interagissent de façon incontrôlée avec leur entourage pendant le calcul, on perd l'information recherchée. »* Et en vertu de l'intrication, *« un seul qubit perturbé, et c'est potentiellement l'ensemble du système qui est affecté »,* renchérit Christophe Vuillot. Pour reprendre l'idée des feutres, c'est comme si vous aviez une boîte avec toutes les nuances de vert, de l'amande au sapin, mais dès que vous en sortez un, tous redeviennent soit bleu soit jaune. L'état quantique, le vert, n'existe plus.

Or plus un problème est complexe, plus il faut de qubits intriqués pour le résoudre efficacement, et plus le risque de décohérence est grand. Autrement dit, plus on en demande à l'ordinateur quantique, plus il se fatigue vite. *« Les algorithmes quantiques sont donc conçus pour minimiser la lecture des données*, indique Cyril Allouche. *Il faut bien comprendre que l'information quantique est par nature éphémère et ne peut pas être copiée. »*

L'ordinateur quantique serait-il donc à usage unique ? « *Non, pas plus que votre calculatrice*, répond Denis Vion. *Vous pouvez le réutiliser autant de fois que vous voulez,*

mais chaque calcul doit être fait dans un temps inférieur au temps de décohérence du processeur si vous voulez un résultat correct. »

► Comment fabrique-t-on une machine quantique ?

Pour l'instant, les tentatives d'ordinateur quantique ressemblent plus à de gigantesques frigos qu'à nos PC. *« Il n'y a d'ailleurs aucun intérêt à un ordinateur de bureau quantique*, tranche Cyril Allouche. *Ces machines seront réservées à des usages très particuliers dans l'industrie et la recherche. »*

Plusieurs techniques existent. *« Aucune solution n'a montré un avantage décisif par rapport à une autre*, estime Christophe Vuillot. *On peut utiliser des circuits supraconducteurs, qui ressemblent à des circuits électroniques spécifiques et très refroidis. On peut piéger des ions dans un champ électromagnétique ou se servir de photons, d'électrons, etc. » « Le challenge, c'est de réaliser des systèmes quantiques contrôlables et stables dans le temps »*, rappelle Cyril Allouche. *« La prochaine étape passera par un accélérateur, une machine hybride avec des qubits adjoints à un supercalculateur »*, décrit Elie Girard.

► Pourquoi parle-t-on beaucoup de cryptographie quantique ?

« L'ordinateur quantique représente une menace pour la façon dont sont chiffrées toutes nos données, de la banque à la santé, commence Sébastien Tanzilli. *Le chiffrement actuel repose sur l'incapacité d'une machine classique à factoriser un très grand nombre en ses facteurs premiers dans un temps acceptable. Les qubits d'une machine quantique permettraient, au contraire, de "casser" ce chiffrement dans un court délai. »*

Prenons l'un de ces jeux où il faut actionner une combinaison d'interrupteurs dans le bon ordre pour allumer une lampe. Imaginez maintenant une version bien plus complexe, avec des milliers d'interrupteurs dont les combinaisons allument des milliers de lampes différentes. Tout vérifier demanderait un temps tel que les joueurs abandonneraient. Avec un ordinateur quantique, ce temps de traitement serait considérablement réduit et le jeu deviendrait facile pour ceux qui ont accès à cette technologie.

Face à ce risque de déchiffrement, des chercheurs travaillent sur une cryptographie dite quantique. En utilisant l'inviolabilité des lois de la physique quantique, l'idée est que tout espion qui voudrait intercepter le message le perturberait. La manœuvre serait donc repérée.

Les mots du quantique

Un ordinateur quantique, pour l'instant inexistant, serait une machine semblable aux ordinateurs actuels mais fonctionnant selon les principes de la physique quantique.

Le principe de superposition veut qu'une particule dans un état quantique présente plusieurs valeurs possibles. C'est l'idée représentée dans l'expérience de pensée dite du « chat de Schrödinger ».

Le principe d'intrication veut que deux ou plusieurs particules dans un état quantique soient codépendantes quelle que soit la distance entre elles.

Le qubit est une unité de base de support de l'information dans un ordinateur quantique, sur le modèle des bits dans les ordinateurs classiques.