Ordinateur quantique

Description

Si l'on comparait l'avancement de la recherche en matière d'ordinateur quantique au domaine de l'aviation, nous en serions encore au premier vol du Français André Guillaume Resnier de Goué, lorsqu'il réussit à planer 300 mètres en Charente, en 1801. Mais l'intensité des recherches et l'abondance des financements font prédire à certains son arrivée dans les dix ou vingt prochaines années. Daniel Estève, responsable du groupe Quantronique au CEA-Saclay tempère néanmoins : *« L'ordinateur quantique n'existe pas ; on ne sait pas s'il existera un jour, et donc encore moins à quelle échéance, mais les lois de la physique l'autorisent »*. Il convient tout d'abord de distinguer un ordinateur d'un calculateur ou encore d'un simulateur quantique : *« Un ordinateur quantique, comme tout ordinateur, est censé pouvoir être programmable pour exécuter n'importe quel algorithme quantique. Un calculateur quantique ne peut exécuter qu'un seul algorithme ou pour le moins, une classe d'algorithme »*, explique Laurent Sacco, journaliste pour Futura Sciences. Quant au simulateur quantique, il s'agit d'une plateforme logicielle reproduisant en partie des capacités de calcul d'un ordinateur quantique, généralement exploitées sur un supercalculateur. L'effervescence actuelle dans l'informatique quantique concerne principalement les calculateurs et les simulateurs, et non les ordinateurs.

Historique

Le concept d'ordinateur quantique est attribué à Richard Feynman, prix Nobel de physique qui, dans les années 1980, propose *« plutôt que de tenter de faire des simulations de physique quantique sur des ordinateurs, ce qui demande beaucoup de temps et de puissance, d'appliquer les phénomènes quantiques à l'informatique »*. Le concept d'informatique quantique était né, reposant sur les principes de la physique quantique où l'information peut être attachée à une particule ou à une onde, et se retrouver dans deux états à la fois. Cette propriété, contraire au bon sens, n'est qu'une des facettes de la physique quantique et de ses propriétés sur le rayonnement électromagnétique, dont l'objet est de manipuler de l'information.

Comment ça marche ?

Les machines quantiques obéissent aux règles de l'infiniment petit, à l'échelle de l'atome, propres à la physique quantique : qubit, superposition, intrication, décohérence. Les phénomènes à partir desquels l'information est manipulée sont pour le moins déroutants.

Qubit

Les lois étranges, qui régissent la physique quantique, s'appliquent à une informatique développée à

l'échelle de l'infiniment petit ; l'information, exprimée en qubits, a pour support matériel un photon, un atome, un ion ou encore un élément supraconducteur. Comme le bit en informatique classique, un qubit (pour « quantum » et « bit ») est l'état quantique qui représente la plus petite unité de stockage d'information quantique. Alors qu'un bit d'information, qui vaut 0 ou 1, est soit ouvert soit fermé, un qubit superpose deux bits et peut être les deux à la fois, c'est-à-dire 0 et 1, à part égale ou non. Si un seul qubit encode deux bits d'information, trois qubits en encodent huit, N qubits équivalant à 2^N bits. Un calculateur quantique permet ainsi de démultiplier exponentiellement la puissance de calcul de l'informatique classique, puisqu'un calculateur d'une puissance de 50 qubits peut simultanément chercher une solution parmi 2^{50} possibilités (1 125 899 906 842 624).

La superposition

Pour comprendre comment se comporte un ordinateur quantique, Pascale Senellart-Mardon, directrice de recherche au CNRS et chercheuse en nanophotonique au Centre de nanosciences et de nanotechnologies du CNRS et de l'université Paris-Saclay, propose la métaphore suivante : *« Chercher la solution d'un problème revient à essayer de faire traverser un labyrinthe complexe par un personnage. Si c'est un ordinateur classique qui aide ce personnage, il lui fera, à chaque embranchement, essayer toutes les voies, rebrousser chemin au bout de chaque cul-de-sac, puis recommencer jusqu'à trouver la sortie.* […] *Si c'est un ordinateur quantique qui assiste le personnage, il le* « *superposera* », *à chaque embranchement, à un* alter ego *qui explorera l'autre voie. En d'autres termes, on aura simultanément l'état représenté par le personnage allant à gauche et l'état d'un* alter ego *allant à droite. Résultat : en une passe, l'ordinateur quantique fait essayer en parallèle toutes les voies au personnage. Il construit ainsi un état qui superpose tous les états d'*alter ego *effectuant tous les parcours possibles, y compris celui qui permet de traverser. Un témoin présent à la sortie permettra alors d'extraire, parmi la multitude d'*alter ego, *celui qui aura traversé le labyrinthe – autrement dit la solution au problème posé.* » Au phénomène de la superposition s'ajoute celui de l'intrication.

L'intrication

L'intrication est un phénomène quantique tout aussi surprenant selon lequel deux particules intriquées forment un système lié dont les états quantiques sont dépendants l'un de l'autre, quelle que soit la distance qui les sépare. Elles n'échangent pas d'information, qui voyagerait dans ce cas plus vite que la lumière, mais elles forment un seul système qui fait fi de leur éloignement.

Pour manipuler des qubits régis par les phénomènes de superposition et d'intrication, encore faut-il composer avec le frein de la décohérence : *« Pour qu'un ordinateur quantique fonctionne, il faut que ses qubits conservent leurs propriétés quantiques le temps du calcul. Or, du fait des interactions avec l'environnement (champ magnétique, lumière, agitation thermique…), tout pousse un système quantique à perdre ses propriétés. Et cela est d'autant plus vrai que le système contient plus de qubits »*, explique Sébastien Tanzilli, de l'Institut de physique de Nice. C'est le principal obstacle à la construction de tels ordinateurs. Selon Pascale Senellart-Mardon, *« la difficulté technique essentielle à franchir pour obtenir un ordinateur quantique est triple : 1) disposer d'un grand nombre de qubits ; 2) parvenir à les combiner en des états intriqués ; 3) maintenir la cohérence de ces états assez longtemps pour que les calculs puissent*

aller à leur terme ».

À quoi ressemble un calculateur quantique ?

QTech, le plus grand laboratoire de recherche européen en informatique quantique, situé à Delft aux Pays-Bas, travaille depuis 2016 à la mise au point de prototypes d'ordinateurs quantiques. Quelque deux cents chercheurs travaillent dans des bureaux dont *« les expériences nécessitent des systèmes de refroidissement à l'hélium liquide, assez bruyants, qui sont regroupés sur un étage, séparé des ordinateurs permettant de les contrôler, pour plus de tranquillité »* rapporte David Larousserie, envoyé spécial à Delft pour le journal *Le Monde*. Ce sont d'immenses réfrigérateurs assemblés les uns avec les autres, qui occupent plusieurs étages et qui sont donc très loin de ressembler à un ordinateur classique ou à un supercalculateur. En janvier 2019, IBM a présenté un prototype de calculateur « Q System One », un cube de verre de 2,74 mètres de côté, suspendu au plafond d'une pièce du centre de recherche historique d'IBM à Yorktown Heights, situé dans les environs de New York. Quinze de ces machines ont été construites. Elles fonctionnent à une température proche du zéro absolu, à –273,5°C, et quatorze sont accessibles à distance, IBM proposant depuis 2016 du *« quantique dans les nuages »* à travers son programme Q System, principalement utilisé par des chercheurs qui auraient, selon IBM, publié quelque 72 articles scientifiques dont les calculs auraient été effectués en utilisant sa plateforme. Pour Florian Debès, journaliste aux *Echos*, 80 clients auraient déjà signé un contrat avec IBM.

Qui est impliqué, qui finance ?

Le Royaume-Uni (1 milliard d'euros entre 2014 et 2024), l'Allemagne (650 millions d'euros en 2018), les États-Unis (1,25 milliard de dollars entre 2018 et 2028), la Chine (10 milliards de dollars entre 2017 et 2027, mais dont seul 1 milliard aurait été dépensé en 2020), l'Europe (1 milliard d'euros entre 2018 et 2028), mais aussi le Japon, l'Australie, Singapour, les Pays-Bas, l'Autriche ou encore le Canada sont autant d'États engagés dans la course à l'ordinateur quantique. En plus de ces investissements publics, il faut également compter sur d'importants financements privés, notamment en Amérique du Nord. Selon le consultant indépendant Olivier Ezratty, *« plus d'un milliard de dollars à ce jour* [ont été investis] *dans les startups, dont plus de 200 millions d'euros dans D-Wave (Canada) et récemment, 230 millions de dollars dans PsiQuantum (États-Unis), 119 millions de dollars dans Rigetti (États-Unis) et 75 millions de dollars dans IonQ (États-Unis). Enfin, IBM, Intel, Google et Microsoft ont probablement investi au moins 100 à 400 millions de dollars chacun dans le calcul quantique ces cinq dernières années »*.

De plus, selon les chiffres du Centre commun de recherche de la Commission européenne à Ispra en Italie, *« plus de 43 % des innovations technologiques quantiques brevetées entre 2012 et 2017 »*, que ce soit dans les domaines des communications quantiques ou des ordinateurs et logiciels quantiques, sont le fait d'entreprises ou d'universités chinoises, suivies par les États-Unis, le Japon puis le Canada.

Une offre commerciale naissante

Google, IBM, Microsoft, Amazon, mais également Alibaba, Tencent, Huawei et Baidu, les géants du web et de l'informatique sont dorénavant tous engagés dans la construction de machines quantiques ou la mise au point de logiciels quantiques. En décembre 2017, Microsoft, par l'intermédiaire de son groupe QuArC (Quantum Architectures and Computation), a lancé un simulateur quantique ainsi qu'un kit de développement assorti d'un langage de programmation, le Q#, accessible gratuitement. Le 4 novembre 2019, la multinationale américaine a annoncé le lancement d'une offre quantique, Azure Quantum, qui s'appuie sur les machines construites par des partenaires, IonQ, QCI ou encore Honeywell. Un mois plus tard, Amazon Web Service faisait une annonce similaire, en s'appuyant, quant à lui, sur des machines élaborées par D-Wave, IonQ et Rigetti. Le géant de l'internet chinois, Alibaba, propose également une offre de quantique dans les nuages, en s'appuyant sur le calculateur d'un centre de l'Académie chinoise des sciences. Google, quant à lui, travaille depuis plusieurs années à l'élaboration d'une machine quantique. En octobre 2019, la firme de Mountain View annonçait avoir franchi une étape majeure en effectuant un calcul quantique en trois minutes et vingt secondes, au lieu de 10 000 ans s'il avait fallu mobiliser, Summit, le supercalculateur le plus performant au monde, produit par IBM. L'article, diffusé par erreur sur le site de la Nasa et retiré une heure plus tard, a ensuite été publié officiellement dans la revue *Nature* en octobre de la même année. En réalité, il ne s'agit pas d'un ordinateur quantique, mais bien d'un calculateur quantique, répondant au nom de Sycamore et disposant de 54 qubits. Les chercheurs d'IBM se sont empressés de minimiser l'annonce de Google en expliquant avoir mis au point un algorithme classique permettant l'exécution de l'algorithme quantique de Google en 2,5 jours, sans l'avoir vraiment optimisé. En France, Atos réalise avec le Commissariat à l'énergie atomique (CEA) un projet d'ordinateur quantique pour l'horizon 2030 et a lancé un programme, en mai 2019, dont l'objet est de se familiariser avec la programmation quantique en s'appuyant sur l'utilisation de supercalculateurs classiques qui simulent le comportement de processeurs quantiques.

Signe de l'immaturité du domaine : toutes ces entreprises proposent une « offre quantique » qui n'a, actuellement, aucune application pratique. Ce sont essentiellement des outils d'expérimentation. L'enjeu pour ces entreprises est d'occuper le terrain et de promouvoir un écosystème auprès des futurs utilisateurs de ces machines qui, le jour où elles seront suffisamment puissantes et stables, seront capables de résoudre des problèmes qui sont aujourd'hui insolubles avec des ordinateurs ou des supercalculateurs classiques. Airbus, BASF, Bayer, Daimler, EDF, Merck ou encore Total ont tous mis en place des groupes de recherche ou des collaborations académiques, par crainte de passer à côté des recherches en la matière.

Quelles sont les futures applications ?

Les calculateurs quantiques pourraient en effet trouver des applications dans de multiples domaines, notamment en chimie, en biologie et en médecine, pour la simulation de molécules, aujourd'hui trop complexe pour l'informatique classique. *« Cela ouvrirait la porte à la création de thérapies révolutionnaires comme pour traiter des maladies neuro-dégénératives »* explique Olivier Ezratty. Dans le domaine de l'industrie, des calculateurs quantiques pourraient développer des molécules de synthèse pour créer de nouveaux matériaux, mais également pour trouver des applications dans l'organisation de

systèmes complexes dans les domaines de l'énergie, de la logistique ou encore du transport.

Les algorithmes quantiques sont également destinés à être utilisés dans les domaines de la cryptographie et de la sécurité, à tel point que les experts se préparent, déjà depuis 2006, à la cryptographie post-quantique, (Post Quantum Cryptography), puisque les algorithmes actuels les plus puissants pourraient facilement être cassés. Aujourd'hui, le chiffrement dit RSA, du nom de ses trois inventeurs (Ronald Rivest, Adi Shamir et Leonard Adleman), est un algorithme de cryptographie décrit en 1977 – dont le brevet a expiré en septembre 2000 – sur lequel s'appuie la majorité des échanges de données confidentielles *via* internet ou encore le commerce électronique. Le chiffrement RSA repose sur le fait qu'il est très complexe de factoriser de grands nombres en nombre premier, ce dernier étant *« un entier naturel qui admet exactement deux diviseurs distincts entiers et positifs »*, par exemple, le nombre entier 11 est premier car 1 et 11 sont les seuls diviseurs entiers de 11. En présence d'un très grand nombre, un pirate essaiera de casser le chiffrement RSA en utilisant un algorithme de décomposition en facteurs premiers. Or, même avec un supercalculateur, le temps nécessaire pour calculer cette factorisation est excessivement long, ce qui fait la force du chiffrement RSA.

En 1994, le mathématicien américain Peter Shor a inventé un algorithme quantique, nommé algorithme de Shor, qui effectue des décompositions en nombres premiers de manière beaucoup plus rapide qu'avec un algorithme classique. Lorsqu'un ordinateur quantique suffisamment puissant pourra faire fonctionner l'algorithme de Shor, la sécurité du chiffrement RSA sera totalement remise en cause. Et c'est d'ailleurs le projet poursuivi par l'agence de sécurité américaine, la NSA, dont le programme secret « Penetrating Hard Targets », doté d'un budget de 79,7 millions de dollars et ayant pour but d'atteindre les cibles difficiles, a été révélé au grand public par Edward Snowden dans les colonnes du *Washington Pos*t en décembre 2013 (voir *La rem* n°28, p.69).

Une autre application concrète est également prévue dans le domaine des communications sécurisées, notamment par la Chine, qui dispose déjà d'une avance considérable en la matière. Lancée en août 2016, la mission spatiale QUESS (Quantum Experiments at Space Scale) a créé un canal de communication entre la Chine et l'Institut d'optique et d'information quantique de Vienne, en Autriche, qui équivaut à une distance au sol de 7 500 km et a permis de passer le premier appel vidéo quantique intercontinental sécurisé. Ces communications s'appuient sur la distribution quantique de clé QKD (pour *quantum key distribution*), dont l'objet est de transmettre entre deux participants une clé cryptographique commune leur permettant de chiffrer leurs communications. Ce type de communication repose sur l'impossibilité supposée de violer les principes de la physique quantique. En octobre 2017, une ligne de fibre optique de 2 000 km était opérationnelle entre Pékin, Jinan, Hefei et Shanghai. Ce réseau couplé au satellite en orbite basse de QUESS, le seul disposant d'un protocole de communication quantique complet, constitue le premier réseau quantique espace-sol au monde, impossible à écouter. La Chine prévoit d'envoyer dix satellites Micius/QUESS afin de mettre entre place un réseau crypté quantique entre l'Europe et l'Asie dès 2020, et un réseau mondial d'ici à 2030.

Enfin, dans le domaine du traitement massif de données, ce sont des pans entiers de la finance, de la

météorologie de précision, de la gestion du trafic routier, ou encore de l'apprentissage machine au sein de l'intelligence artificielle, qui bénéficieraient de ces nouveaux types de calcul.

La suprématie quantique

John Preskill, professeur au California Institute of Technology (Caltech) aux États-Unis, a utilisé pour la première fois en 2012 dans un article scientifique le concept de « suprématie quantique », qui consiste, pour un ordinateur quantique, à effectuer un calcul hors de portée d'un ordinateur classique. Cette suprématie quantique est ainsi l'objet d'une course effrénée entre chercheurs et acteurs privés et d'une surenchère médiatique. Pourtant, il se peut que celui qui l'atteindra, se gardera bien de le révéler, car il pourra alors casser tous les systèmes cryptographiques actuels. Si, comme l'explique le chercheur Christopher Monroe, professeur de physique à l'Université du Maryland et cofondateur de la start-up IonQ, *« l'informatique quantique est un marathon et non un sprint »*, le top départ théorique a bel et bien été donné dans les années 1980. En revanche, la ligne d'arrivée est encore lointaine.

Sources :

- « Quantum Key Distribution », en.Wikipedia.org
- « Les ordinateurs quantiques auront le pouvoir de briser le chiffrement asymétrique » qui est à la base de la sécurité de l'internet », Gilbert Kallenborn, 01net.fr, 28 mars 2015.
- « L'ordinateur quantique, un défi pour la cryptographie », Yann Verdo, *Les Echos*, 12 décembre 2016.
- « Aurons-nous un jour des ordinateurs quantiques ? » Podcast France Culture, Franceculture.fr, 25 mai 2017.
- « Le cantique des quantiques », Yann Verdo, *Les Echos Week-End*, 30 juin 2017.
- « Informatique : le grand saut quantique », David Larousserie, Cahier du Monde, n° 22542, 5 juillet 2017.
- « La Chine, leader des communications quantiques », David Larousserie, *Le Monde*, 15-16 août 2017.
- « La révolution quantique », Azar Khalatbari, *Sciences et Avenir*, n° 850, décembre 2017.
- « Le quantique, la prochaine révolution de l'informatique ? », Olivier Ezratty, latribune.fr, 24 juillet 2018.
- « IBM dévoile au CES le premier ordinateur quantique « compact » », Gabriel Nedelec, *Les Echos*, 9 janvier 2019.
- « Les ordinateurs quantiques vont-ils révolutionner le futur ? », Laure Beaudonnet, 20minutes.fr, 29 avril 2019.
- « La construction d'un ordinateur quantique : au-delà des coups de pub, un joli casse-tête », Fabien Soyez, Cnetfrance.fr, 13 mai 2019.
- « L'ordinateur quantique devient un enjeu politique », François Savatier, Pour La Science, n° 500, 27 mai 2019.
- « Des tests sans faille de l'intrication quantique », Ronald Hanson et Krister Shalm, *Pour La Science*, n° 504, 24 septembre 2019.
- « Tout comprendre à l'informatique quantique », Scott Fulton, zdnet.fr, 26 septembre 2019.
- « La révolution de l'informatique quantique », Lucie Ronfaut, *Le Figaro*, 28-29 septembre 2019.

- « Google réalise une percée dans le calcul quantique », David Larousserie, *Le Monde*, 24 octobre 2019.
- « Bataille mondiale pour la suprématie quantique », Zaour Mamediarov, *Courrier international*, n° 1 514, du 7 au 13 novembre 2019.
- « Les technologiques quantiques ou la nouvelle ruée vers l'or », Geneviève Fournier, siecledigital.fr, 14 novembre 2019.
- « Le calcul quantique à l'aube d'une révolution », Benoît Georges, *Les Echos*, 17 décembre 2019.
- « Ordinateur quantique : la première téléportation quantique entre deux puces au silicium a réussi », Laurent Sacco, Futura-sciences.com, 3 janvier 2020.
- « Ordinateur : les promesses de l'aube quantique », Julien Bourdet, CNRS, Lejournal.cnrs.fr, 15 mai 2019, mis à jour le 6 janvier 2020.
- « L'informatique quantique promet d'alimenter de belles batailles de géants », Florian Dèbes, lesechos.fr, 9 janvier 2020.
- « Les ambitions de la France dans le quantique », Olivier Ezratty, frenchweb.fr, 10 janvier 2020.
- « L'ordinateur quantique : tout comprendre en partant de zéro », Vincent Rollet, institut-pandore.com, 23 janvier 2020.

Categorie

1. A retenir

date créée
23 avril 2020
Auteur
jacquesandrefines