Avec la physique quantique, des technologies nouvelles pour le futur

Michèle Leduc[1] (michele.leduc@lkb.ens.fr) et **Sébastien Tanzilli**[2]
(1) Directrice de recherche émérite CNRS au Laboratoire Kastler-Brossel (ENS, UPMC, CNRS) à Paris.
Ancienne directrice de l'IFRAF (Institut Francilien de Recherche sur les Atomes Froids).
(2) Directeur de recherche CNRS au Laboratoire de Physique de la Matière Condensée à l'Université Côte d'Azur (UCA) et directeur du GDR IQFA (Ingénierie Quantique des aspects Fondamentaux aux Applications).

La seconde révolution quantique utilise aujourd'hui les concepts quantiques de superposition ou d'intrication d'objets microscopiques que l'on a appris à contrôler individuellement.

Les capteurs tels que gyromètres, gravimètres, horloges à atomes froids fournissent déjà des outils d'une sensibilité insurpassable. Des problèmes impliquant un grand nombre d'objets quantiques en interaction, inaccessibles aux supercalculateurs, trouvent des solutions avec des méthodes de simulation quantique, tandis que les travaux sur l'ordinateur quantique se multiplient. Enfin, les communications à distance vont bientôt pouvoir être mieux sécurisées grâce aux progrès de la cryptographie quantique.

La seconde révolution quantique

La mécanique quantique a constitué, avec la relativité, une des deux révolutions majeures de la physique du XX^{e} siècle. C'est aujourd'hui une vieille dame de cent ans, pas encore réconciliée avec la gravitation relativiste et qui fait toujours beaucoup parler d'elle. Bien que cette théorie n'ait jamais été mise en défaut, la signification de ses concepts fait toujours débat. Pourtant ses applications, parfaitement maîtrisées, continuent de se multiplier.

Les découvertes fondamentales de la mécanique quantique résultent des travaux de Bohr, Heisenberg, Schrödinger, Dirac, Pauli, de Broglie et bien d'autres au XX^{e} siècle. Elles ont permis la compréhension des lois de la constitution de la matière et ont conduit à des avancées technologiques qui ont révolutionné notre vie quotidienne, telles que le transistor, les microprocesseurs, les lasers, le GPS, etc. Les extraordinaires progrès expérimentaux des dernières décennies permettent aujourd'hui d'observer des particules telles que des photons, des atomes ou des ions que l'on a appris à contrôler individuellement aussi bien que collectivement. On peut alors les préparer et les manipuler en utilisant les concepts de superposition d'états quantiques ou d'intrication (voir l'encadré, p. 30). Il en découle un ensemble de nouvelles applications si prometteuses que les États-Unis et la Chine en font des programmes prioritaires, tandis que la Commission européenne lance un nouveau *Flagship* (projet qui sera doté d'un milliard d'euros au total, dont 300 à 500 millions de fonds publics européens) sur le thème des *quantum technologies*, dont nous évoquons ici plusieurs secteurs où des résultats spectaculaires sont attendus à court ou long terme.

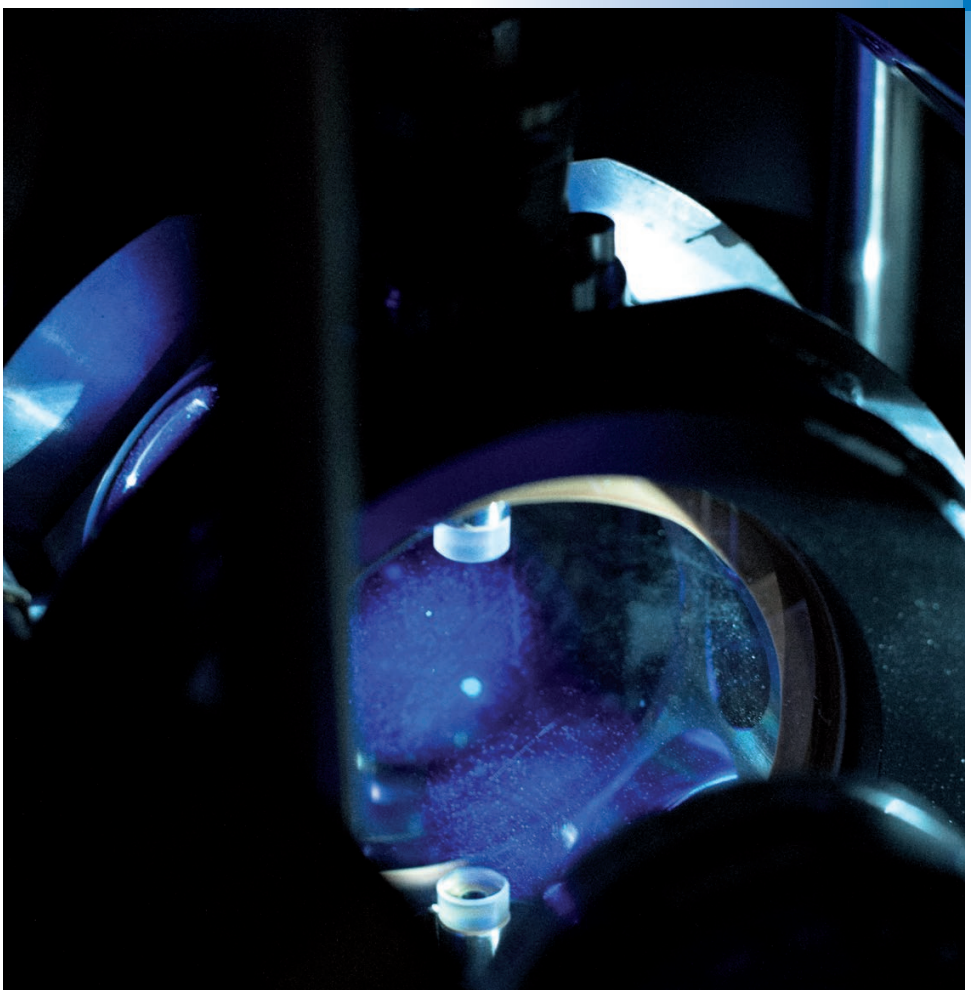
Des capteurs quantiques pour la métrologie de haute précision

La superposition d'états quantiques est très sensible à l'environnement classique et fournit des capteurs d'une grande précision. Les accéléromètres et gyromètres à atomes froids sont fondés sur l'interférométrie atomique. Ils détectent le déphasage entre les ondes de matière parcourant les deux bras de l'interféromètre (fig. 1). Ce déphasage varie lorsque l'appareil se déplace. On peut ainsi mesurer avec une grande précision l'accélération ou la rotation, et constituer des gyromètres ou des accéléromètres de grande fiabilité pour la navigation inertielle.

Le gravimètre est une variante de ces systèmes interférométriques quand ils sont disposés en position verticale : les atomes tombent sous l'effet de l'accélération de la pesanteur g que l'on mesure ainsi en valeur absolue en continu et sans limitation de durée, avec une incertitude relative inférieure au milliardième. Les applications attendues concernent la sismologie ou la prospection des ressources minières et pétrolières : l'important programme britannique *Quantum Technology Strategy Initiative* va jusqu'à inclure la relocalisation des canalisations d'eau oubliées dans le sous-sol de la ville de Londres.

Les horloges atomiques (photo ci-contre) sont des systèmes quantiques mesurant la fréquence d'une transition atomique, qui

Article disponible sur le site http://www.refletsdelaphysique.fr ou http://dx.doi.org/10.1051/refdp/201651028

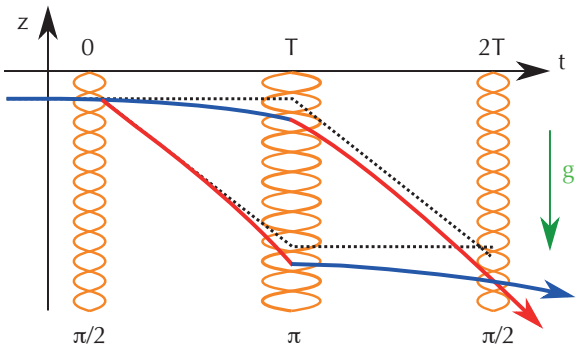


Photographie de l'horloge optique à strontium. La lumière bleue est la fluorescence, à une longueur d'onde de 461 nm, des atomes froids de strontium maintenus au centre d'une cavité en ultravide. Le nuage atomique (la petite tache bleue au centre) est placé dans un réseau optique 1D créé par un faisceau laser rétroréfléchi de longueur d'onde 813 nm (non visible sur la figure), qui crée une onde stationnaire dans laquelle les atomes sont piégés. Les petits éléments circulaires blancs au-dessus et en dessous du nuage atomique sont des miroirs dichroïques qui permettent à la fois de former le réseau optique à 813 nm et une cavité à 461 nm pour la détection non destructive des atomes, ce qui va permettre de mettre en œuvre des méthodes d'ingénierie quantique.
(Courtoisie Rodolphe Le Targat, Laboratoire SYRTE, Observatoire de Paris.)

font également usage de l'interférométrie. Les nouvelles générations d'horloges à atomes ou ions froids fonctionnent maintenant dans le domaine optique et atteignent des exactitudes spectaculaires (une seconde de dérive par rapport à l'âge de l'Univers !). Leurs applications sont multiples, couvrant la définition du temps universel impliquant la synchronisation de toutes les horloges sur la Terre, l'amélioration du GPS et la navigation spatiale. Leur sensibilité au déplacement gravitationnel en fait des instruments complémentaires des gravimètres, qui seront utilisés dans le futur pour améliorer notre connaissance du géoïde. Tous ces instruments quantiques de laboratoire vont être rendus plus compacts. Ils sont pour certains en phase de valorisation, comme les gravimètres fabriqués par la société *Muquans* à Bordeaux.

Les progrès croissants dans le contrôle et la réduction des sources de bruits classiques permettront bientôt d'amener la sensibilité de ces capteurs à la limite fondamentale du bruit quantique standard. Les recherches actuelles portent sur la façon de dépasser cette limite en exploitant certains états quantiques du rayonnement ou de la matière, par exemple des états de *spin* dits « comprimés » (*spin squeezing*) : on peut en effet, par des méthodes optiques appropriées, réduire les fluctuations d'intensité d'un faisceau lumineux au détriment de celles de la phase, ou encore celles de la position des atomes d'un gaz au détriment de celles de leur vitesse. Notons que ces mêmes idées de compression des fluctuations quantiques vont être mises en œuvre prochainement pour augmenter la sensibilité

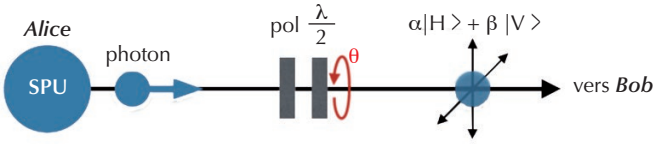
›››



1. Schéma de principe d'un interféromètre à atomes froids en chute libre. L'axe z est orienté selon la direction verticale d'accélération de la pesanteur g. Les ondes de matière qui arrivent de gauche interagissent trois fois avec des ondes laser stationnaires (en orange sur la figure), qui leur communiquent des impulsions. Après une première impulsion laser, l'onde de matière subit un déphasage de $\pi/2$ (on parle alors d'impulsion $\pi/2$), lui offrant deux voies de propagation matérialisées par les faisceaux rouge et bleu. Les deux couleurs représentent les deux états quantiques couplés par les lasers, qui diffèrent par leur état d'impulsion. L'impulsion laser π suivante joue le rôle d'un miroir qui redirige les deux composantes de l'onde de matière. Après l'impulsion laser $\pi/2$ finale, les ondes de matière sortantes interfèrent avec la différence de phase accumulée le long des deux bras de l'interféromètre. Ce déphasage serait nul sans la gravitation (trajets en pointillés). Mais les atomes tombent verticalement : le déphasage est proportionnel à l'accélération de la pesanteur g, et on le mesure par le déplacement des franges d'interférence. On réalise ainsi un gravimètre.
(Courtoisie : Franck Pereira dos Santos, laboratoire SYRTE, Observatoire de Paris.)

Superposition cohérente d'états, qubits et intrication

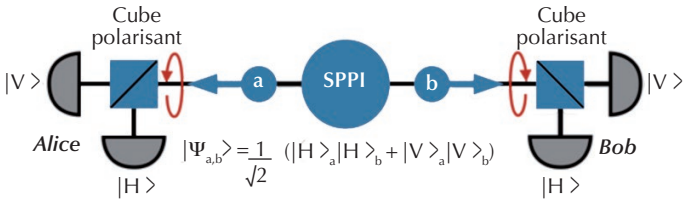
L'informatique classique fonctionne à l'aide de bits qui peuvent prendre des valeurs 0 ou 1, correspondant à des états notés |0> et |1>. La physique quantique offre une infinité de possibilités, grâce à l'ensemble des combinaisons données par la *superposition cohérente de deux états de base* |0> et |1>. Par exemple, considérons un photon de polarisation horizontale après avoir traversé un polariseur (fig. E1). Si l'on ajoute une lame demi-onde qu'on fait tourner d'un angle θ (indiqué en rouge sur la figure E1), on obtient une superposition sinθ |H> + cosθ |V> des états de polarisation horizontale |H> et verticale |V>. Ceci se traduit par l'obtention d'un *qubit* (contraction des mots *quantum bit*) sous la forme α |0> + β |1>, les poids relatifs α et β variant avec l'angle θ tout en respectant la règle de normalisation $|\alpha|^2 + |\beta|^2 = 1$.



E1. Obtention d'un qubit photonique par superposition cohérente de deux états quantiques. SPU représente une source de photons uniques, située ici chez Alice. La flèche bleue représente la direction de propagation des photons depuis Alice jusque vers Bob. Les flèches à 90° l'une de l'autre sur le photon envoyé vers Bob représentent les deux états de polarisation horizontale et verticale. Les qubits sont codés sur l'observable polarisation par le biais d'un polariseur (pol) et d'une lame demi-onde (λ/2).

Les qubits photoniques codés sur l'observable polarisation sont couramment utilisés pour la cryptographie quantique, au même titre que les observables temps et fréquence. Des qubits peuvent être constitués à partir de tout système quantique, particule naturelle ou artificielle, présentant deux états distincts qu'on peut produire dans un état de superposition.

L'*intrication* représente la généralisation à deux ou plusieurs systèmes quantiques de la superposition cohérente d'états définis pour la constitution d'un qubit. Pour rester dans le domaine optique (fig. E2), considérons une source (SPPI) qui émet des paires de photons intriqués. La façon la plus courante pour créer une telle source est d'utiliser un cristal non linéaire (non représenté sur la figure E2) qui transforme un photon unique en une paire de photons d'énergie moitié. La paire de photons intriqués doit être considérée comme un tout, c'est-à-dire un système quantique unique composé de deux sous-systèmes, depuis son instant de création jusqu'aux instants où les photons sont détectés, même s'ils sont à grande distance l'un de l'autre. Lorsqu'une mesure est effectuée sur l'un des deux photons, le résultat de la mesure sur l'autre est immédiatement déterminé.



E2. Obtention d'une paire de qubits photoniques intriqués.

Ici une source (SPPI) émet une paire de photons (a et b) intriqués, sur laquelle l'information quantique est codée sur l'observable polarisation. La paire de photons est alors préparée dans un état bien défini $|\Psi_{a,b}\rangle$, alors que les états des photons individuels ne le sont pas. En d'autres termes, l'information quantique est codée sur l'objet quantique composé des deux photons, depuis la création de la paire jusqu'à sa détection : on parle de *qubits intriqués*. Expérimentalement, les photons sont envoyés à deux utilisateurs distants, Alice et Bob, qui possèdent chacun un cube séparateur de polarisation suivi de deux détecteurs à 90° l'un de l'autre. Ceci leur permet de projeter l'état du photon reçu dans une base d'analyse, ici la base des polarisations horizontale et verticale. En tournant la lame demi-onde (flèche rouge), ils peuvent changer de base d'analyse. Le point crucial est que tant que Bob n'a pas fait de mesure, le photon d'Alice ne possède aucune polarisation définie, puisque seul l'état de la paire compte du point de vue de l'information. Ces propriétés peuvent être exploitées par les deux interlocuteurs pour établir des clés secrètes utiles aux opérations de cryptographie.

›››

des grands interféromètres optiques LIGO et Virgo qui détectent les ondes de gravitation. Enfin, mentionnons que des techniques spécifiques aux capteurs formés d'objets quantiques uniques sont aussi étudiées en utilisant des effets d'intrication quantique, fournissant des méthodes nouvelles pour l'imagerie ou la résonance paramagnétique électronique.

La simulation quantique de phénomènes complexes

La conception de nombreux objets complexes de la vie courante, tels que les voitures, les avions, ou les bâtiments publics, fait appel à des ordinateurs très puissants, les supercalculateurs. À l'inverse, ceux-ci sont impuissants pour décrire le comportement de systèmes formés de plus de quelques dizaines d'atomes et pour prédire s'ils vont conduire l'électricité, devenir magnétiques ou produire des réactions chimiques inattendues. L'objectif des programmes de simulation quantique est de répondre à ces questions inaccessibles en mettant en œuvre des méthodes de simulation « à la Feynman », qui parlait déjà de construire *"a quantum machine that could imitate any quantum system, including the physical world"*. Différentes plateformes peuvent être utilisées pour mieux comprendre le comportement de systèmes formés d'objets quantiques en interaction dans des conditions inatteignables avec le système initial. Dans ce domaine, théoriciens et expérimentateurs travaillent conjointement. L'idée générale est que le système artificiel de la simulation quantique obéit aux mêmes équations de la physique quantique que le système initial : il fournit ainsi un résultat transposable pour les propriétés de ce dernier, pour lequel *a priori* le contrôle de chaque élément individuel ne serait pas possible.

Parmi les différentes approches exploitées aujourd'hui pour la simulation quantique, le domaine des atomes froids fournit des outils de choix, autorisant la mise en œuvre d'expériences modèles. En effet, on piège les atomes dans des réseaux optiques créés par des ondes stationnaires issues de faisceaux laser rétroréfléchis, idéalement un par site du réseau, ou encore on les maintient individuellement en position de réseau avec des pinces optiques (fig. 2). On peut partir d'atomes bosoniques, par exemple initialement dans un état condensé de Bose-Einstein, ou bien d'atomes fermioniques, dégénérés si la température est

abaissée en dessous de la température de Fermi. On simule ainsi les propriétés des électrons fortement corrélés et mobiles à l'intérieur d'un matériau solide.

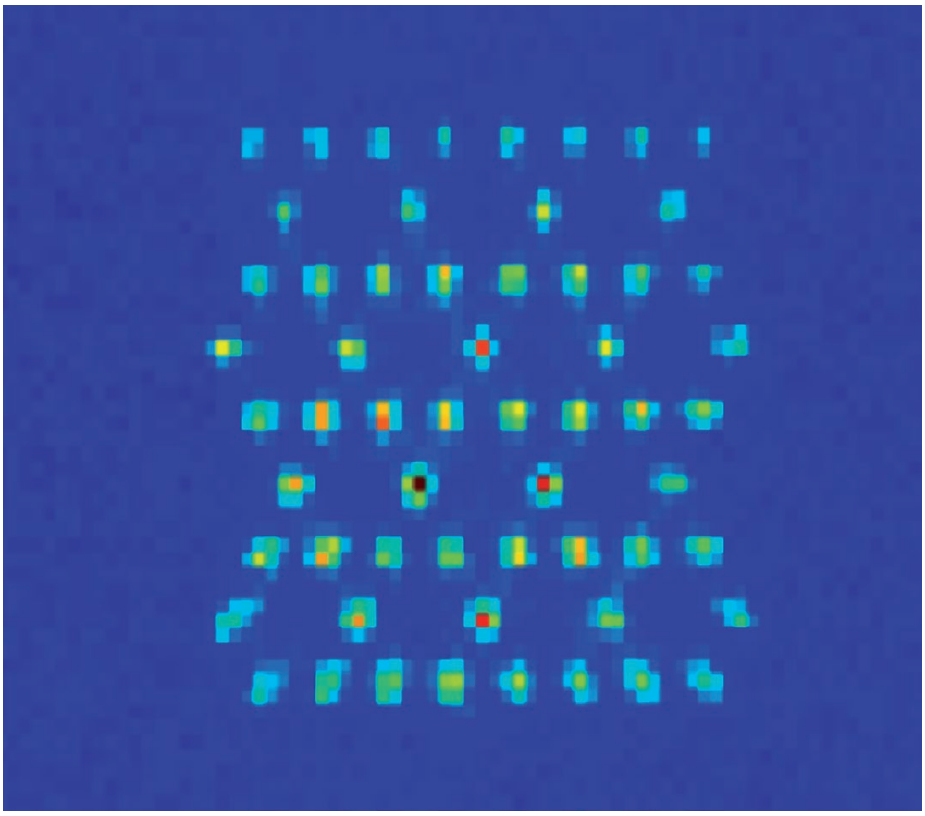
Il existe bien d'autres plateformes expérimentales pour la simulation quantique : des ions froids piégés (fig. 3) ou des molécules froides, des polaritons ou des excitons dans les semi-conducteurs, des réseaux de qubits supraconducteurs ou de boîtes quantiques, ou encore des photons intriqués dans des réseaux de guides d'onde couplés.

Chacune des plateformes mentionnées ci-dessus permet de faire varier à volonté un certain nombre de paramètres associés à la simulation (la température, le nombre des particules, la géométrie du réseau, la portée et même le signe des interactions entre les particules, le couplage éventuel à l'environnement, etc.), mais aucune d'entre elles, et ce quelle que soit l'approche, ne les maîtrise tous à la fois.

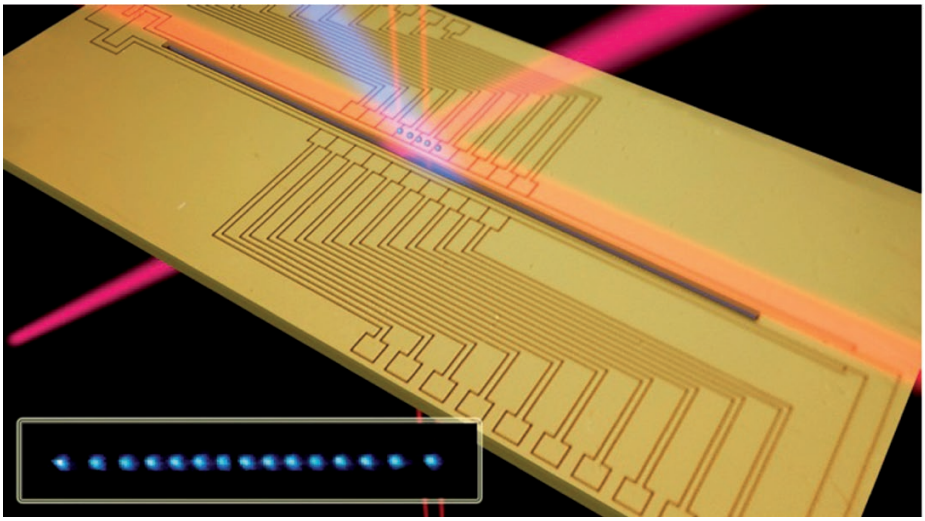
On peut simuler ainsi de nombreuses propriétés de la matière : les nouvelles phases quantiques à basse température, le magnétisme, les systèmes quantiques hors équilibre, notamment le transport en présence de désordre, les phases topologiques, les matériaux, etc. Le *Graal* est d'approcher les conditions d'apparition de la supraconductivité à haute température critique, dont l'origine reste encore mystérieuse. L'enjeu est évidemment considérable, car on entrevoit la possibilité de concevoir de nouveaux matériaux capables de conduire l'électricité sans perte à température ambiante, ce qui aurait d'énormes conséquences dans le domaine du transport de l'énergie. Des interfaces se développent aussi avec la chimie quantique, les hautes énergies ou l'astrophysique.

Le rêve de l'ordinateur quantique

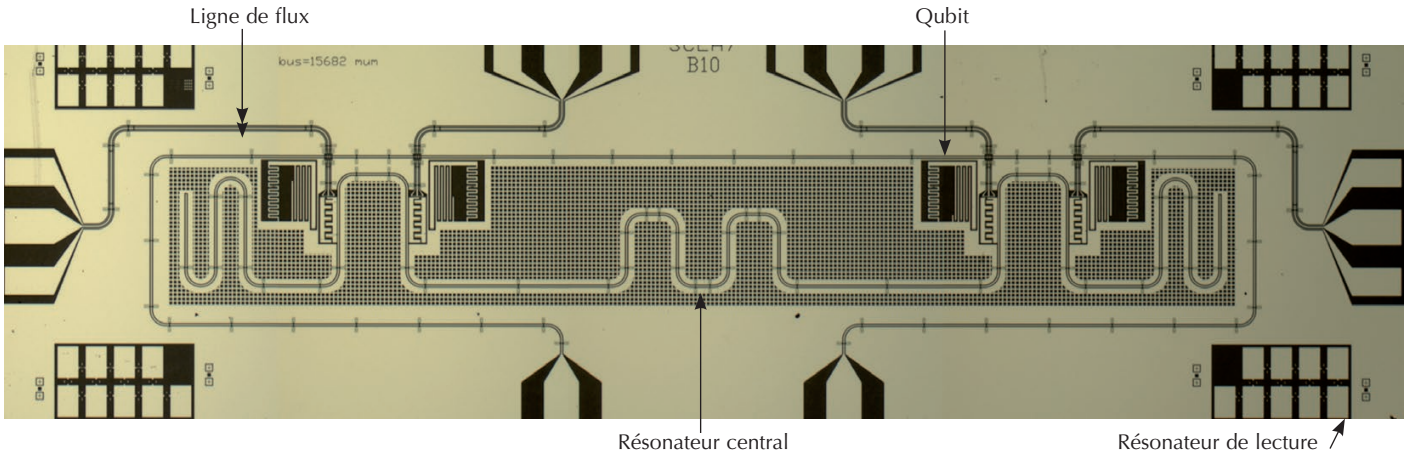
À côté de la simulation quantique, d'autres voies sont aujourd'hui étudiées avec l'ordinateur quantique pour dépasser les limites bientôt atteintes des supercalculateurs classiques. Les enjeux de l'ordinateur quantique sont tels qu'ils suscitent des efforts de recherche considérables dans le monde entier, aussi bien dans le milieu académique que dans les grandes entreprises de l'informatique comme IBM et même d'internet comme Google, qui y investissent des moyens considérables. L'idée est de réaliser des calculs massivement parallèles, ›››



2. Image de fluorescence d'atomes froids de rubidium maintenus en position par des pinces optiques. On peut construire avec ces atomes des réseaux 2D de taille micrométrique en choisissant à volonté la géométrie du réseau, ici hexagonal. Deux atomes voisins piégés dans le réseau sont séparés par une distance d'environ 5 µm. Le gradient de couleur au sein des sites (du bleu au rouge) indique la probabilité de présence d'un atome.
(Courtoisie : Antoine Browaeys, laboratoire Charles Fabry, Institut d'Optique Graduate School. Voir aussi son article dans le numéro **47-48** de *Reflets de la physique*, pp. 36-40.)



3. Image d'ions calcium en ligne, refroidis et contrôlés dans un piège électromagnétique (on parle de piège de Paul). Au sein du piège, deux ions voisins sont séparés par 10-20 µm. Le piège est réalisé sur une puce électronique, où des fils parcourus par des courants créent les champs électriques et magnétiques nécessaires au piégeage. Les ions à l'intérieur du piège sont détectés par fluorescence à l'aide d'un faisceau laser (ici en bleu). Le système sert pour la simulation et le calcul quantiques.
(Courtoisie : Rainer Blatt, IQOQI, Innsbruck.)



4. Prototype de processeur quantique supraconducteur universel à quatre qubits, muni d'une lecture individuelle des qubits. Des jonctions Josephson entre éléments supraconducteurs et des photons micro-ondes sont les ingrédients de ce processeur, dont la longueur totale est d'environ une dizaine de mm. Chacun des quatre qubits (les petits rectangles au milieu de la figure) est une boîte à paires de Cooper réglable indépendamment en fréquence par une ligne de flux connectée à gauche, en haut ou à droite de la puce. Pour la lecture, la fréquence d'un qubit est approchée de celle du résonateur micro-onde anharmonique auquel il est couplé (carrés avec des zones isolantes noires aux quatre coins de la figure). Chaque qubit est ajustable en fréquence, est équipé d'un résonateur permettant de lire son état quantique et est couplé à un résonateur central utilisé pour les portes logiques à deux qubits.
(Courtoisie : Daniel Estève, groupe Quantronique, SPEC, CEA-Saclay. Voir Dewes *et al., Phys. Rev. B* **85** (2012) 140503.)

›››

avec un nombre exponentiellement croissant d'opérations effectuées en même temps. Toutefois, pour définir un champ d'application à ce type d'ordinateur, il faut construire en même temps l'algorithme de calcul quantique approprié. Pour l'instant, on n'a trouvé qu'un petit nombre d'algorithmes pour lesquels le calcul quantique se montre plus efficace que son équivalent classique : les plus connus sont celui de Shor pour factoriser des grands nombres, et celui de Grover pour trouver rapidement une entrée dans une base de données non triées.

Le concept sous-jacent repose sur l'exploitation de qubits (voir l'encadré). Pour construire un calculateur quantique, on fait évoluer avec des portes logiques quantiques un registre des qubits intriqués. Le problème principal réside dans le phénomène de décohérence, qui tend à détruire l'intrication des qubits pendant l'opération de calcul sous l'effet des interactions avec l'environnement. Des briques de base très variées sont explorées pour réaliser ces qubits élémentaires et construire des systèmes suffisamment résistants à la décohérence. Beaucoup s'apparentent aux systèmes déjà décrits plus haut pour la simulation quantique. Le record actuel consiste en une chaîne linéaire d'une vingtaine d'ions calcium refroidis, avec lesquels divers processus élémentaires ont été démontrés (fig. 3). Récemment, des processeurs quantiques avec des portes logiques à deux qubits ont été réalisés, avec des systèmes supraconducteurs utilisant l'effet Josephson (fig. 4) ou encore à l'aide de systèmes photoniques. Pour tous les systèmes envisagés, une première difficulté est dans la montée en taille du dispositif. Une autre difficulté est de maîtriser les erreurs introduites par les constituants imparfaits du dispositif expérimental, qui font chuter la fiabilité du système. Le nombre d'erreurs augmente extrêmement vite avec le nombre de portes logiques, et des algorithmes de plus en plus sophistiqués sont construits théoriquement pour détecter et corriger ces erreurs. Ajoutons que la programmation d'un ordinateur quantique diffère profondément de celle d'un ordinateur classique et nécessite des recherches nouvelles de la part des informaticiens.

En résumé, si les technologies à développer pour l'ordinateur quantique semblent d'une difficulté extraordinaire, aucune loi fondamentale de la physique n'interdit de les envisager. La compagnie *D-wave* s'est d'ailleurs déjà lancée sur ce marché. Quant aux applications, elles restent encore à déterminer ; certains pensent que c'est la chimie quantique qui devrait en être un important bénéficiaire, d'autres supposent que la puissance de calcul d'un tel ordinateur permettra un jour de casser les méthodes de chiffrement à clé publique de la cryptographie classique.

Les communications quantiques sécurisées entre villes

Les modes de communication et de traitement de l'information classique ont révolutionné la société depuis quelques décennies : les cinq continents sont reliés par des câbles optiques, l'information est manipulée à très haut débit sans perte sur des distances quasi illimitées. Toutefois, une limitation forte existe s'il s'agit de communiquer l'information de façon sécurisée. Aujourd'hui, elle intervient à chaque instant dans de très nombreux domaines de la vie privée ou publique et devient un problème de société d'importance stratégique pour les particuliers, les entreprises et l'État.

Le domaine de la cryptographie a un long passé qui remonte à l'Antiquité. Les protocoles utilisés pour le chiffrement et le déchiffrement des messages utilisent des codes de plus en plus complexes avec des clefs de plus en plus longues, à mesure qu'augmente la puissance des ordinateurs capables de les casser. Une autre stratégie est nécessaire, et la physique quantique intervient alors pour assurer l'inviolabilité des communications à distance sur le long terme.

À l'instar du chiffrement classique, la cryptographie quantique repose sur l'échange de bits générés aléatoirement, sauf que les bits 0 ou 1 deviennent des

superpositions d'états (ou qubits) (voir l'encadré). Pour envoyer des qubits sur de grandes distances, il est approprié d'utiliser des photons comme support, en encodant l'information sur des observables telles que la polarisation de la lumière (voir les figures de l'encadré). Les photons sont émis un à un par des sources dites de photons uniques, à partir par exemple de centres colorés dans le diamant ou d'atomes artificiels basés sur des boîtes quantiques semi-conductrices (*quantum dots*). Les protocoles variés d'établissement quantique de clés de chiffrement utilisent des qubits individuels, d'autres des paires de qubits intriqués, ce qui permet alors de doubler la distance de propagation possible.

L'inviolabilité de la cryptographie quantique résulte de deux théorèmes très fondamentaux, qui régissent les lois suivies par les états quantiques et empêchent leurs utilisateurs de prédire, connaître, ou manipuler le système à leur guise : le premier prédit qu'une mesure unique produit un résultat aléatoire sur un objet quantique préparé dans une superposition de deux états ; le second, dit théorème de non-clonage, montre qu'il n'est pas possible de cloner parfaitement une superposition d'états inconnue au préalable.

La cryptographie quantique sert à générer des clés utilisées ensuite dans des protocoles classiques. C'est une technologie déjà relativement au point, qui donne lieu à des dispositifs produits par quelques petites entreprises. La société suisse ID-Quantique l'a utilisée à plusieurs reprises dans la « vraie vie » et l'a testée, par exemple, pour la distribution des informations sur le vote en ligne dans le canton de Genève. Notons aussi que la ville de Tokyo bénéficie depuis 2011 d'un véritable réseau de cryptographie quantique permanent et éprouvé, et que la Chine vise une connexion quantique entre Pékin et Shanghai. Pourtant la méthode ne peut fonctionner actuellement que sur des distances limitées à quelques dizaines de km (un record de 200 km a été enregistré), en l'absence de répéteurs sécurisés. Toute une recherche se développe pour concevoir de tels répéteurs quantiques permettant par exemple de stocker des états intriqués photoniques bipartites en deux endroits distants, puis de synchroniser la réémission des photons.

Les recherches actuelles visent à augmenter l'efficacité des sources de photons uniques et de paires de photons intriqués, et aussi de perfectionner leurs détecteurs, dont les pertes peuvent créer des failles dans l'inviolabilité. Aussi, grâce aux récents progrès expérimentaux relatifs à la manipulation cohérente de l'intrication, les chercheurs envisagent aujourd'hui des protocoles quantiques de communication indépendants des systèmes matériels employés (sources et détecteurs). Par ailleurs, de nouveaux protocoles informatiques sont sans cesse inventés : certains visent à introduire la cryptographie quantique dans les systèmes télécom, d'autres envisagent des solutions postquantiques à base de cryptographie classique actuellement non attaquables par l'ordinateur quantique. Enfin, évoquons le rêve que les distances de transmission sécurisée deviennent sans limite avec la téléportation quantique par satellite, envisagée déjà par la Chine. Des années de R&D sont encore nécessaires avant que le grand public dispose d'un internet quantique sécurisé.

Quel progrès pour l'humanité ?

Pour conclure, on constate que toutes les technologies quantiques évoquées ici étaient inimaginables il y a seulement trente ans. Elles représentent des rêves de physiciens et d'informaticiens, impliquant théories subtiles et expérimentations sophistiquées. On ne sait pas à quelle échelle de temps elles vont déboucher sur des produits commerciaux, mais il est certain qu'elles vont modifier notre vie quotidienne. Est-ce que ce sera pour le plus grand bien de l'humanité ? La sécurité totale et garantie des communications est-elle réellement souhaitable actuellement à l'heure du terrorisme ? À l'inverse, s'il devient possible de casser un jour les clefs classiques de sécurité des secrets des États, la géopolitique mondiale s'en trouvera bouleversée. À l'extrême, si la sécurité de l'internet classique utilisé par chacun de nous n'est plus garantie, quelles en seront les conséquences pour le monde dans lequel nous évoluons aujourd'hui ? Les règles éthiques d'utilisation pertinente de toutes ces nouvelles technologies quantiques restent encore à définir. ▮

Pour en savoir plus

- M. Le Bellac, *Le monde quantique*, EDP Sciences (2010).
- F. Bretenaker et N. Treps, *Le laser*, EDP Sciences (2016)
- J. Dalibard, Cours du Collège de France *« Atomes et rayonnement »*, www.college-de-france.fr/site/jean-dalibard/ .
- S. Tanzilli, Thèse d'habilitation à diriger des recherches, https://tel.archives-ouvertes.fr/tel-00845762/document .
- M.H. Devoret et R.J. Schoelkopf, "Superconducting Circuits for Quantum Information: An Outlook", *Science* **339** (2013) 1169.