LES TECHNOLOGIES QUANTIQUES, de la recherche fondamentale à l'innovation

Michèle LEDUC[1], **Sébastien TANZILLI**[2]
[1] Directrice de recherche émérite au Laboratoire Kastler-Brossel (ENS, UPMC, CNRS) à Paris, et directrice de l'IFRAF (Institut Francilien de Recherche sur les Atomes Froids)
[2] Directeur de recherche à l'Institut de Physique de Nice (CNRS et Université Côte d'Azur), directeur du GDR IQFA (Ingénierie Quantique, des aspects Fondamentaux aux Applications) du CNRS, et chargé de mission « Technologies Quantiques » auprès de l'Institut de Physique du CNRS
sebastien.tanzilli@unice.fr

Après la physique quantique, les technologies quantiques. La mécanique quantique et la relativité ont constitué les deux révolutions majeures de la physique du XX^{e} siècle. Bien que la théorie quantique n'ait jamais été mise en défaut, la signification et l'interprétation de ses concepts continuent de faire débat. Pour autant les applications qui en découlent sont parfaitement maîtrisées et continuent de se multiplier.

Les découvertes fondamentales de la physique quantique résultent des travaux de Bohr, Heisenberg, Schrödinger, Dirac, Pauli, de Broglie et bien d'autres au siècle dernier. Elles ont permis la compréhension des lois qui régissent à la fois la matière, la lumière et leurs interactions. Au-delà des concepts, la physique quantique est à l'origine d'avancées technologiques sans précédent qui ont révolutionné notre vie quotidienne, telles que le transistor, le microprocesseur, le laser, etc. Les extraordinaires progrès expérimentaux de ces dernières décennies permettent aujourd'hui d'observer des objets quantiques tels que les photons, les atomes ou les ions que l'on a appris à contrôler individuellement aussi bien que collectivement. On peut ainsi les préparer et les manipuler en utilisant les concepts de superposition d'états quantiques et d'intrication (voir l'encadré). Il en découle un ensemble de nouvelles applications si prometteuses que plusieurs pays, notamment les États-Unis et la Chine, en ont fait des programmes prioritaires. Dans ce contexte, la commission européenne a lancé cette année, via un premier appel à projet, un nouveau programme de type *Flagship* sur le thème des *quantum technologies*. Nous évoquons dans cet article les quatre thématiques principales de ce programme, qui relèvent de la communication, du calcul, de la simulation et de la métrologie quantiques, où des résultats spectaculaires sont attendus à court, moyen, ou long terme.

La communication quantique sécurisée entre villes et entre continents

Les modes de communication et de traitement de l'information classique ont révolutionné la société au cours des dernières décennies : les cinq continents sont reliés par des câbles optiques sous-marins, les territoires sont maillés par de nombreuses liaisons terrestres ou satellitaires, permettant de véhiculer et router l'information sans perte et à très haut débit sur des distances quasi illimitées. Toutefois, une limitation forte existe lorsqu'il s'agit de communiquer l'information de façon ultra-sécurisée. En effet, la sécurisation des données intervient à chaque instant dans de très nombreux domaines de la vie privée ou publique et représente un enjeu stratégique pour les entreprises, les grands groupes industriels, les banques ou l'État. Aujourd'hui, les protocoles utilisés pour le chiffrement et le déchiffrement des messages utilisent des codes de plus en plus complexes avec des clefs publiques de plus en plus longues, à mesure qu'augmente la puissance des ordinateurs (classiques) capables de les casser. Une stratégie plus efficace est donc nécessaire : la physique quantique intervient alors pour garantir l'inviolabilité des communications à distance et sur le long terme.

À l'instar du chiffrement classique, la cryptographie quantique repose sur l'échange de bits générés aléatoirement, à ceci près que les bits 0 ou 1 deviennent des superpositions d'états (ou qubits, contraction des mots *quantum bits*, voir l'encadré). Pour envoyer des qubits sur de grandes distances, le support privilégié est le photon, qui autorise l'encodage de l'information sur des observables telles que la polarisation de la

https://doi.org/10.1051/photon/20189118
Article publié sous les conditions définies par la licence Creative Commons Attribution License CC-BY (http://creativecommons.org/licenses/by/4.0), qui autorise sans restrictions l'utilisation, la diffusion, et la reproduction sur quelque support que ce soit, sous réserve de citation correcte de la publication originale.

lumière (voir les figures de l'encadré). Les photons sont émis un à un ou par paires par des sources dites de photons uniques (centres colorés dans le diamant, boîtes quantiques) ou de paires de photons (sources paramétriques en optique non-linéaire). Les protocoles variés d'établissement quantique de clés de chiffrement utilisent ainsi des qubits individuels, d'autres des paires de qubits intriqués (voir article d'Eleni Diamanti).

La cryptographie quantique sert à générer des clés utilisées ensuite dans des protocoles de chiffrement classiques. C'est une technologie déjà relativement au point qui donne lieu à des systèmes développés et commercialisés par quelques petites entreprises. La société Suisse ID-Quantique l'a utilisée à plusieurs reprises en situations réelles, comme par exemple pour le relevé des informations sur le vote en ligne dans le canton de Genève. Notons également que la ville de Tokyo bénéficie depuis 2011 d'un véritable réseau de cryptographie quantique permanent et que la Chine vise une connexion quantique par fibre optique entre Pékin et Shanghai sur le long terme (~1200 km). Pourtant la méthode ne peut fonctionner actuellement que sur des distances limitées à quelques centaines de km en l'absence de répéteurs sécurisés. Toute une recherche se développe pour concevoir de tels répéteurs quantiques permettant de stocker des états intriqués photoniques bi-partites en deux endroits distants, puis de synchroniser la réémission des photons. Parallèlement à ces recherches, la communication quantique vient de faire ses premiers pas dans l'espace : une source embarquée sur un satellite chinois a en effet permis de distribuer des photons intriqués entre deux stations sol séparées par une distance record de 2000 km. Une ère nouvelle, celle de la communication quantique intercontinentale, s'ouvre donc aux chercheurs et aux « ingénieurs quantiques ».

Afin d'augmenter les débits, la portée et la sécurité des liens de communication quantique, les recherches actuelles se tournent volontiers

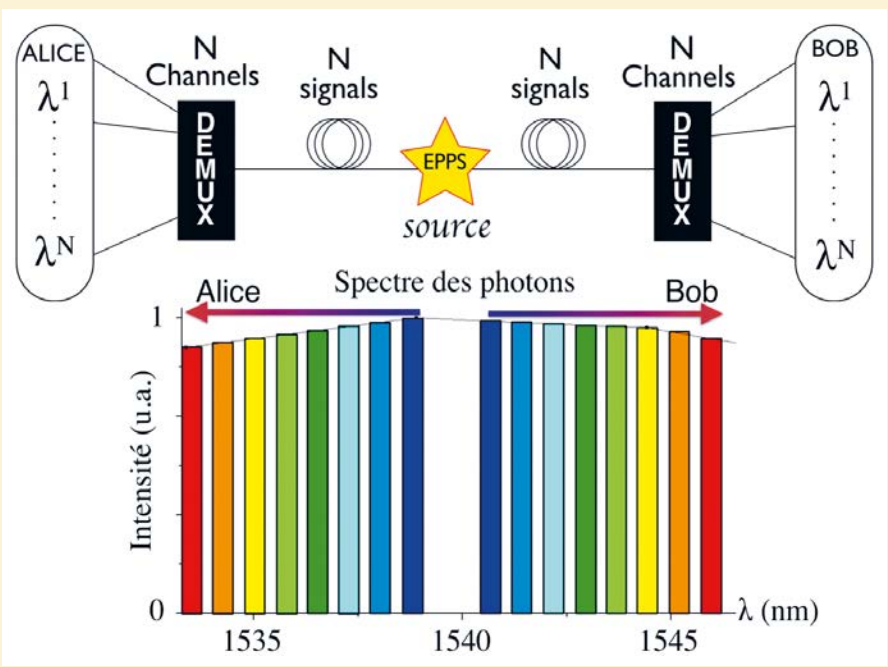
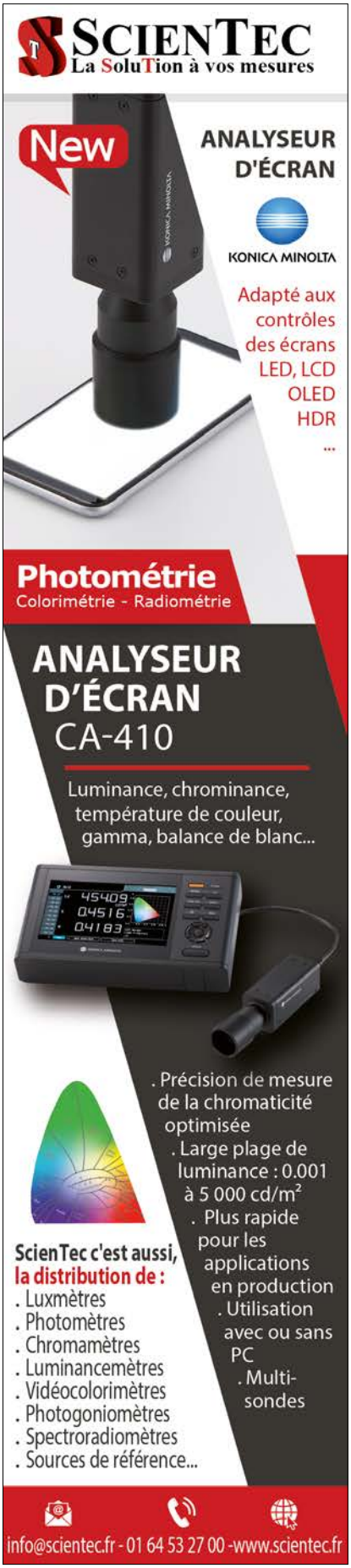


Figure 1. Principe de fonctionnement d'un lien de cryptographie quantique établi sur 150 km à démultiplexage spectral placé chez les deux utilisateurs (Alice et Bob). La source délivre des paires de photons intriqués dont le spectre couvre toute la bande des télécommunications. Comme l'indique le code couleur, les étages de démultiplexage permettent à Alice et Bob d'établir des clés secrètes dans chaque paire de canaux spectraux complémentaires. Grâce à cette stratégie, le débit total de clés secrètes est multiplié par le nombre de paires de canaux exploité. (courtoisie Djeylan Aktas, Institut de Physique de Nice, voir Aktas *et al.*, *Lasers & Photon. Rev.* **10**, 451-457, 2016)



vers les dernières innovations technologiques en photonique et en micro-électronique. Ceci devrait permettre la mise en place de véritable crypto-systèmes quantiques, allant du prototype au dispositif éprouvé. Aussi, grâce aux récents progrès expérimentaux relatifs à la manipulation de l'intrication aux longueurs d'onde des télécommunications, les chercheurs envisagent aujourd'hui des protocoles quantiques de communication à grande échelle, que ce soit en termes de nombre d'utilisateurs connectés que de distances qui les séparent (voir *figure 1*). Aussi, l'intrication devrait permettre le développement de crypto-systèmes certifiés, ou en d'autres termes, indépendants du matériel employé (sources et détecteurs). Par ailleurs, de nouvelles idées d'hybridation émergent sans cesse : certaines visent à introduire la cryptographie quantique dans les systèmes télécoms existants, d'autres envisagent des solutions post-quantiques à base de cryptographie classique actuellement non attaquables par l'ordinateur quantique. Si des années de R&D sont encore nécessaires avant que le grand public dispose d'un internet quantique universel, l'établissement des clés privées ultra-sécurisées entre sites distants est vu aujourd'hui comme la façon de contourner la menace de l'ordinateur quantique qui « pèse » sur les systèmes de chiffrement classique.

Vers un ordinateur quantique ultra-puissant ?

La perspective initiale de l'ordinateur, ou calculateur, quantique « universel » réside dans le dépassement des limites bientôt atteintes par les supercalculateurs classiques. Les enjeux sous-jacents sont tels que l'ordinateur quantique suscite des efforts de recherche considérables dans le monde entier, aussi bien dans le milieu académique qu'au sein de grands groupes industriels de l'informatique et d'Internet tels Google, IBM, Intel ou Microsoft, qui y investissement des moyens considérables.

L'idée est de réaliser des calculs massivement parallèles, avec un nombre exponentiellement croissant d'opérations effectuées en même temps. Toutefois, pour définir un champ d'application à ce type d'ordinateurs il faut construire en même temps les algorithmes de calcul quantique appropriés. Pour l'instant, seul un petit nombre d'algorithmes ont été trouvés, pour lesquels les calculs quantiques se montrent plus efficaces que leurs équivalents classiques. Les plus connus sont ceux de Shor et de Grover : le premier est capable de factoriser des grands entiers en leur facteurs premiers et le second capable de trouver une entrée dans une base de données non triées.

Le concept sous-jacent repose sur l'exploitation d'un registre de qubits intriqués (voir l'encadré) correctement initialisé et que l'on fait évoluer à l'aide de portes logiques quantiques. Le résultat du calcul est alors produit par un processus d'interférence qui dépend de l'initialisation du registre des qubits au problème donné et de son évolution au travers des portes logiques. Le problème principal réside dans le phénomène de décohérence qui tend à détruire l'intrication des qubits pendant les diverses opérations d'un calcul donné 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. Dans la course au nombre de qubits qui composent les calculateurs quantiques (50 étant le minimum requis pour démontrer un certain « avantage quantique »), les solutions les plus prometteuses sont les jonctions Josephson supra-conductrices (courant, voir *figure 2*), les ions piégés (états électroniques internes, voir *figure 3*) et le silicium cristallin (spin). Alors que Google, IBM et Intel ont très récemment annoncé les développements respectifs de calculateurs quantiques supra-conducteurs à 72, 50 et 49 qubits, le record actuel en laboratoire consiste en une chaine linéaire d'une vingtaine d'ions calcium refroidis, avec lesquels divers processus élémentaires ont été démontrés (voir *figure 3*). Récemment des processeurs quantiques avec des portes logiques à deux qubits ont

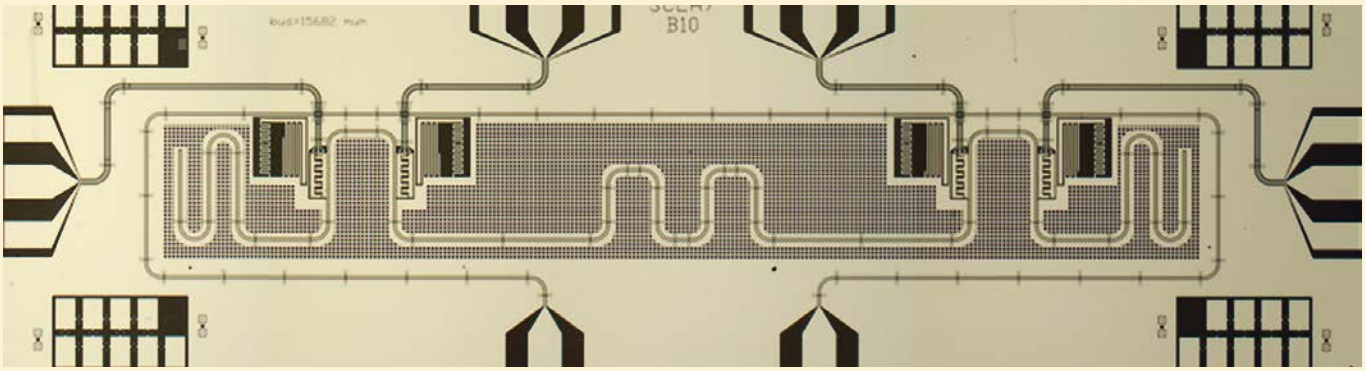


Figure 2. Prototype de processeur quantique supraconducteur universel à 4 qubits en aluminium muni d'une lecture individuelle des qubits. Des jonctions Josephson entre éléments supraconducteurs et des photons micro-ondes sont les ingrédients de ce processeur dont la longueur totale est d'environ une dizaine de mm. (courtoisie Daniel Estève, groupe Quantronique, CEA-Saclay, voir Dewes *et al.*, *Phys. Rev. B* **85**, 140503, 2012)

https://doi.org/10.1051/photon/20189118

été démontrés avec des systèmes supraconducteurs utilisant l'effet Josephson, des qubits de spin dans le silicium ou encore à l'aide de systèmes photoniques intégrés.

Pour tous les systèmes envisagés, une première difficulté réside dans la montée en taille des dispositifs. Une autre difficulté est de maîtriser les erreurs introduites par les constituants imparfaits des dispositifs expérimentaux 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.

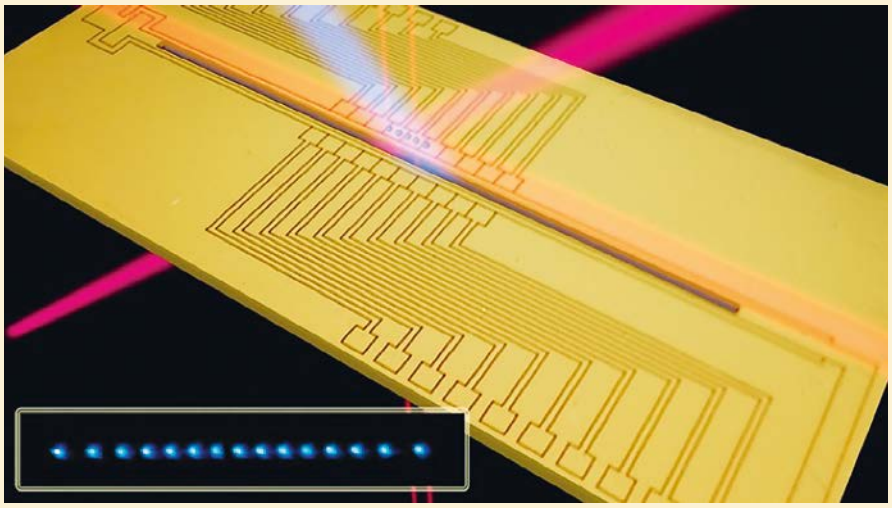


Figure 3. Image d'ions calcium en ligne, refroidis et contrôlés dans un piège électromagnétique (on parle de piège de Paul). Au sein du piège, deux ions voisins sont séparés par 10-20 µm. Le piège est réalisé sur puce électronique où des fils parcourus par des courants réalisent les champs électriques et magnétiques nécessaires au piégeage. (courtoisie Rainer Blatt, IQOQI, Innsbruck)

Quant aux applications, elles restent encore à déterminer. Au-delà de la « menace » qui pèse sur les méthodes de chiffrement à clé publique de la cryptographie classique, les principaux

Sources laser, photomètre, contrôleur de polarisation et atténuateur optique réunis en une seule plate-forme

wavetel

Plate-forme de test modulaire

coherent solutions

Source laser accordable

MTP1000

La solution MTP 1000 est une plate-forme qui intègre des modules couvrant l'ensemble des besoins de test optique.
Cette modularité assure la pérennité de votre système de test et son évolutivité.

- Un logiciel intuitif et facile, utilisable pour tous les modules.
- Interfaces Ethernet ou USB.
- Automatisation simple des tests.
- Évolutivité et configurations illimitées.

Modules optiques disponibles

Module laser accordable
Module photomètre
Module atténuateur optique variable
Module laser DFB
Module conversion opto-électrique
Module contrôleur de polarisation
Module source large bande
Module de commutation

IQ-TLS

L'IQ-TLS est une source laser accordable extrêmement compacte et aisément transportable. Très fine spectralement, elle couvre les bandes C et L avec des pas d'accordabilité de 0,01 pm.

- Bande C : 1527 à 1567 nm.
- Bande L : 1567 à 1609 nm.
- Puissance en sortie : >15 dBm.
- Largeur spectrale (FWHM) : 25 kHz.
- Dimensions : 115 x 222 x 332 mm.

Pour toute information ou démonstration, contactez Arnaud Bout : Email : about@wavetel.fr - Phone : +33 (0)2 99 14 69 65 - +33 (0)6 83 55 19 47 - www.wavetel.fr

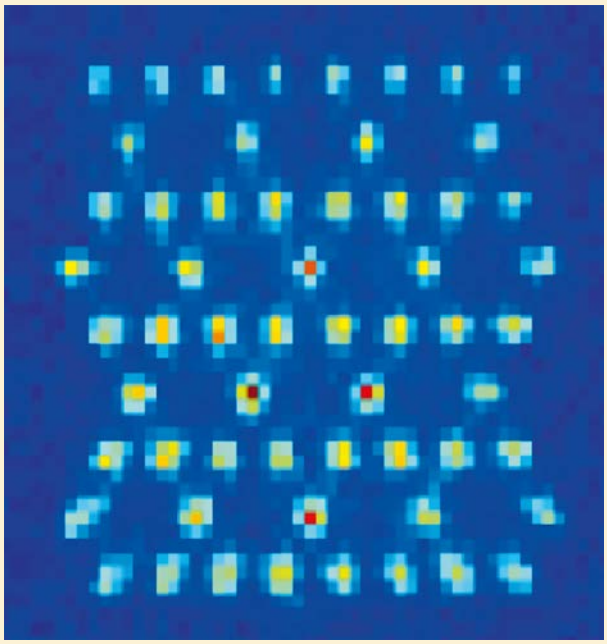


Figure 4. Image de fluorescence d'atomes froids de rubidium maintenus en position par des pinces optiques. On peut construire avec ces atomes des réseaux 2D selon un motif (ici hexagonal) et un pas (ici 5 µm) au choix. Le gradient de couleur au sein des sites (du bleu au rouge) indique la probabilité de présence d'un atome. (courtoisie Antoine Browaeys, laboratoire Charles Fabry, Institut d'Optique Graduate School)

champs bénéficiaires devraient être la chimie quantique via la découverte de nouvelles molécules, ou encore la supra-conductivité haute température. Aussi, la puissance du calcul quantique devait permettre un jour d'optimiser les flux des ressources (maillage du transport de l'énergie, du trafic routier, des individus, etc.).

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 lorsqu'il s'agit de décrire le comportement de systèmes formés de plus de quelques dizaines d'atomes et de prédire s'ils vont conduire l'électricité, devenir magnétiques ou supraconducteurs, ou encore produire des réactions chimiques inattendues. L'objectif des recherches en simulation quantique est de répondre à ces questions importantes, notamment pour la science de la matière condensée, 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, ou systèmes artificiels, peuvent être exploitées pour mieux comprendre le comportement de systèmes réels formés d'objets quantiques en interaction dans des conditions inatteignables directement. Dans ce domaine, théoriciens et expérimentateurs travaillent conjointement afin de concevoir ces systèmes artificiels flexibles et ajustables, c'est-à-dire dont on peut contrôler tout ou partie des paramètres, l'idée générale étant qu'ils obéissent aux mêmes équations de la physique quantique que les systèmes réels qu'ils simulent.

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 rétro-réfléchis, en plaçant idéalement un atome par site du réseau, ou encore on les maintient individuellement en position de réseau avec des pinces optiques (voir *figure 4*). 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. Il existe bien d'autres plateformes expérimentales pour la simulation quantique : des ions (voir *figure 3*) froids piégés, ou des molécules froides, des polaritons ou des excitons dans les semiconducteurs, 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 permet de faire varier un certain nombre de paramètres de simulation (température, nombre de particules, portée et signe des interactions, couplage à l'environnement, etc.), mais aucune d'entre elles ne les maîtrise tous à la fois.

On peut ainsi simuler 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 répercussions dans le domaine du transport de l'énergie. Des interfaces se développent aussi avec la chimie quantique, les hautes énergies ou l'astrophysique.

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 (voir *figure 5*) qui varie lorsque l'appareil se déplace ; ils sont capables de mesurer avec une grande précision l'accélération ou la rotation et constituer ainsi des gyromètres ou des accéléromètres de grande fiabilité pour la navigation inertielle.

https://doi.org/10.1051/photon/20189118

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 perspectives et les applications attendues avec de tels systèmes concernent la sismologie ou la prospection des ressources minières et pétrolières.

Les horloges atomiques sont des systèmes quantiques mesurant la fréquence d'une transition atomique qui 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 (1 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 conçus et fabriqués par la société Muquans à Bordeaux.

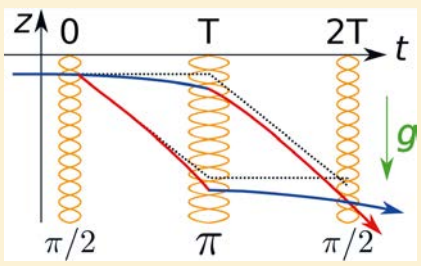


Figure 5. Schéma de principe d'un interféromètre à atomes froids en chute libre. L'axe *z* est orienté selon la direction verticale d'accélération de la pesanteur *g*. Les ondes de matière qui arrivent de gauche interagissent trois fois avec des ondes laser stationnaires qui leur communiquent des impulsions. Après une première impulsion, l'onde de matière subit un déphasage de π/2 (on parle alors d'impulsion π/2), lui offrant deux voies de propagation matérialisées par les chemins rouge et bleu. Les deux couleurs représentent les deux états quantiques couplés par les lasers, qui diffèrent par leur état d'impulsion. L'impulsion π suivante joue le rôle d'un miroir qui redirige les deux composantes de l'onde de matière. Après l'impulsion π/2 finale de recombinaison, l'interférence produite dépend de la différence de phase accumulée le long des deux bras de l'interféromètre. Ce déphasage serait nul sans la gravitation (trajet en pointillés). Mais les atomes tombent verticalement : le déphasage est proportionnel à 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)

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 des grands interféromètres optiques LIGO et VIRGO qui détectent les ondes de gravitation.

Enfin, les techniques de mesure de précision basées sur la photonique émergent également, avec notamment l'utilisation de paires de photons intriqués permettant de caractériser certaines spécificités des matériaux pour l'optique, telles que l'indice de réfraction et la dispersion chromatique. On parle déjà d'interférométrie quantique en lumière blanche qui pourrait être à l'origine de nouveaux systèmes à fibre optique, étendus à de nouvelles longueurs d'ondes, tels que les lasers pour la médecine ou pour la spectroscopie moléculaire.

EKSMA OPTICS
Design fiable pour les lasers industriels de forte puissance
Cellule de Pockels en BBO double ou quadruple cristaux

Fonctionne à 1 MHz (taux de répétition)
Système de sélection d'impulsions ultra-rapide

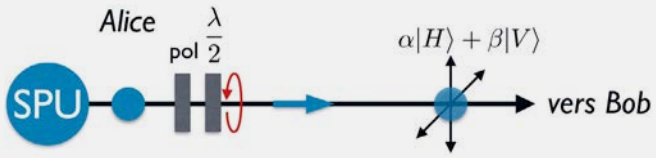
Sélection d'impulsion >1 Mhz
Système synchronisé sur votre laser avec des taux de répétition >100 MHz
www.eksmaoptics.com
Représenté en France par:
ARDOP INDUSTRIE
+33 1 69 63 26 09 | sales@ardop.com
www.ardop.com

Quels retours pour la société ?

Pour conclure, on constate que toutes les technologies quantiques évoquées ici étaient inimaginables il y a seulement trente ans. Elles ont pu représenter des rêves de chercheuses et de chercheurs, issu(e)s de nombreuses disciplines telles que la physique et l'informatique. Aujourd'hui, ces technologies impliquent théories subtiles et expérimentations sophistiquées. On ne sait pas à quelle échelle de temps elles vont déboucher sur des produits commerciaux à grande ou petite échelle, 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 ? A l'inverse, s'il devient possible de casser un jour les clefs classiques de sécurité de certains 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. Un point certainement positif, toutefois, réside dans les perspectives d'optimisation des procédés grâce au calcul et aux algorithmes quantiques, ainsi que dans l'évaluation toujours plus précises de nombreux paramètres physiques grâce aux capteurs quantiques.

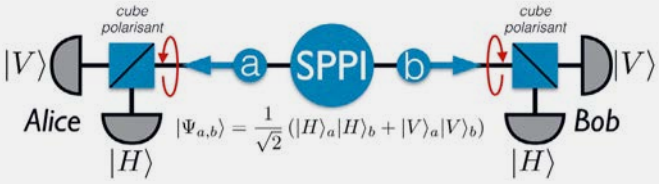
Superposition cohérente d'états, qubits et intrication

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



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. Ils sont émis à partir de sources de photons uniques (SPU), située ici chez Alice qui code les qubits sur l'observable polarisation par le biais d'un polariseur (P) et d'une lame demi-onde. La flèche bleue indique la direction de propagation des photons depuis Alice jusque chez Bob.

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 (voir la figure ci-dessous), considérons une source qui émet des paires de photons intriqués (SPPI). La façon la plus courante pour créer une telle source est d'utiliser un cristal non linéaire qui transforme un photon unique en une paire de photons d'énergie moitié (non représenté sur la figure). 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.



Ici, une source émet une paire de photons intriqués (SPPI), 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. En exploitant cette stratégie, les deux interlocuteurs peuvent révéler des corrélations non locales ou établir des clés secrètes utiles aux opérations de cryptographie.

https://doi.org/10.1051/photon/20189118