rieur de chacun, l'information quantique est convertie en information classique puis à nouveau sous forme quantique. Et pour éviter tout risque d'espionnage lorsque le signal est mis sous forme classique, chaque bâtiment est gardé par un bataillon de l'armée chinoise…

Moins gourmande en soldats et plus intéressante est l'idée d'utiliser un satellite, situé à quelque 500 kilomètres d'altitude, de sorte que la plus grande partie du parcours des photons émis vers la terre se fait dans le vide. Seuls les 10 kilomètres d'épaisseur de l'atmosphère donnent lieu à une absorption. C'est à ce jour l'unique méthode pour envoyer deux photons intriqués à 1200 kilomètres l'un de l'autre d'une traite. Je trouve ça très beau.

Faisons un peu de pédagogie. À quoi cela peut-il servir ?

Alain Aspect : À la cryptographie quantique ou à la téléportation quantique à grande distance, dans les deux cas en utilisant une paire de photons intriqués. Pour la cryptographie quantique, il s'agit de distribuer à deux partenaires, Alice et Bob, deux suites identiques de 0 et de 1, qui serviront de clés de cryptage et de décryptage. Les corrélations quantiques entre photons intriqués garantissent que les clés sont identiques, et qu'il est impossible, pour des raisons fondamentales, d'en obtenir une troisième copie.

Quant à la téléportation quantique, l'idée – très subtile – est la suivante. L'état d'un objet quantique est décrit, en mathématiques, par un vecteur dans ce que l'on appelle un espace de Hilbert. Cependant, la totalité de l'information sur cet état (disons les composantes de ce vecteur) est inaccessible à la mesure ; seule une partie de l'information (une projection du vecteur sur une base de dimension limitée) est à portée d'instrument. Dans ces conditions, il semble *a priori* impossible de connaître la totalité de l'état quantique d'un objet et d'envoyer l'information correspondante à distance. Eh bien la téléportation quantique, fondée sur l'intrication, permet de contourner ce problème !

Avec une paire de photons intriqués, on peut d'abord faire interagir le premier photon avec le système dont on veut téléporter l'état. Cet état se trouvera copié sur le second photon de la paire au terme d'une série d'opérations. De la sorte, l'état quantique aura voyagé. Cependant, il y a un prix à payer. L'état quantique du système de départ, téléporté, a été complètement modifié à l'issue des opérations : il a été « coupé-déplacé » sur le second photon et a été effacé du système de départ. Mais c'est quand même extraordinaire si l'on songe que l'état a été déplacé en totalité alors qu'on ne peut pas le connaître.

Cette téléportation rend possible un internet quantique, en tout cas un réseau d'ordinateurs quantiques qui échangeraient des états quantiques. Ce n'est pas la téléportation de matière, à la Star Trek, mais celle d'une information quantique. L'idée est fascinante.

Un problème encore mal résolu réside dans la nécessité d'une mémoire quantique, indispensable pour rendre vraiment efficace la téléportation quantique, car il faut garder en attente, jusqu'à la fin du processus, l'information partielle sur l'état quantique transférée « instantanément » lors de l'interaction avec le premier photon. Une mémoire quantique efficace aurait bien d'autres applications : elle permettrait de développer des répéteurs quantiques basés sur des photons intriqués, permettant de régénérer le signal quantique atténué dans les fibres optiques sans passer par un signal classique intermédiaire. Avec de tels répéteurs quantiques, on pourrait dépasser la limite des 100 kilomètres sans recourir à des satellites. Mais il n'existe pas encore de très bonne mémoire quantique, bien que sur le plan fondamental, rien ne semble s'y opposer.

L'autre grande information qui fait un peu de bruit est l'annonce de Google sur la suprématie quantique qu'ils auraient atteint. Comment y voir clair ?

Alain Aspect : Il faut d'abord dire que l'expérience réalisée est remarquable. On la doit à un scientifique exceptionnel, John Martinis, de l'université de Californie, à Santa Barbara, aux États-Unis, qui a longtemps travaillé avec Daniel Estève, un des leaders des supraconducteurs dans son laboratoire du CEA à Saclay, ainsi qu'avec Michel Devoret, maintenant à Yale. Mais il faut distinguer l'annonce tonitruante de Google de la conférence donnée par John Martinis à l'institut de technologie de Californie, dans un contexte universitaire : il est à juste titre très fier de son résultat, mais il ne le survend pas.

Peut-on rappeler ce qu'est la suprématie quantique ?

Alain Aspect : D'abord, le vocabulaire fait polémique. Le terme « suprématie » implique l'élimination de tous les concurrents. Je préfère parler d'« avantage », c'est-à-dire une supériorité seulement dans certains types d'applications. Quoi qu'il en soit, avantage ou suprématie, c'est l'idée théorique selon laquelle on pourrait mettre en œuvre le parallélisme massif offert par l'intrication quantique pour réaliser des calculs beaucoup plus vite qu'avec une machine classique. Par « beaucoup plus vite », il faut entendre exponentiellement plus vite, au vrai sens scientifique du terme.

Pour éviter tout risque d'espionnage, chaque bâtiment est gardé par un bataillon de l'armée chinoise

Prenons l'exemple de la factorisation des nombres entiers. Pour un nombre de 100 chiffres, un ordinateur classique aura besoin d'un temps T, et ce temps doublera pour un nombre de 101 chiffres, et doublera encore pour 102, etc. Le temps croît de façon exponentielle, et c'est cette croissance exponentielle qui permet de se mettre à l'abri des espions au fur et à mesure des progrès des ordinateurs.

Or on peut démontrer qu'en mettant en œuvre un algorithme particulier (celui de Shor) sur un ordinateur quantique, le temps de calcul d'une factorisation croît notablement plus lentement avec le nombre de chiffres. Ainsi, en renversant le point de vue, l'ordinateur quantique va exponentiellement plus vite que l'ordinateur classique.

Démontrer l'avantage quantique consiste à pouvoir dire : « J'ai résolu, avec un système quantique, un problème dont >

la résolution demanderait un temps considérablement plus long avec un ordinateur classique.»

C'est ce que revendique Google…

Alain Aspect : Oui, mais, d'une part, le problème qu'ils disent avoir résolu est sans utilité, et, d'autre part, ils n'ont pas préparé eux-mêmes ce problème. Schématiquement, ils ont connecté leurs circuits quantiques et observé un résultat sur une configuration déterminée plus par le système que par eux, et ont mis au défi des ordinateurs classiques de calculer ce résultat… Je reconnaîtrai volontiers un avantage quantique le jour, sans doute pas très lointain, où le problème résolu d'une façon beaucoup plus efficace qu'avec un ordinateur classique aura un minimum d'utilité, comme celui du voyageur de commerce (trouver le chemin le plus court passant par plusieurs villes) et sera choisi par un tiers. Aujourd'hui, nous avons une magnifique expérience, mais qui n'a pas dépassé une étape intermédiaire.

Google la présente aussi comme un générateur de nombres aléatoires, mais il y a tellement plus simple pour obtenir un nombre aléatoire avec un système quantique ! Un photon envoyé sur une lame semi-réfléchissante va soit la traverser et être détecté dans la voie transmise, et vous notez le résultat 1, soit être réfléchi et détecté dans la deuxième voie, et vous avez un 0. En recommençant l'opération, vous obtenez un nombre aléatoire, sous forme binaire, aussi grand que vous le souhaitez ! Le comportement du photon est totalement imprévisible, car dans le cas contraire, des variables cachées existeraient dans le système quantique. Or plusieurs expériences, dont celles menées à l'Institut d'optique, montrent que ce n'est pas le cas.

Dans ce domaine, on distingue simulateur quantique et ordinateur quantique. Quelle est la différence ?

Alain Aspect : Elle se situe entre le réel imparfait et le théoriquement parfait. Le domaine du calcul quantique en général a été initié par Richard Feynman en 1982, quand il a réalisé que l'intrication est un phénomène révolutionnaire dont il avait jusque-là sous-estimé l'importance. Dès lors, il lance les premières idées sur le calcul quantique, qui sont d'abord celles d'un simulateur quantique : simuler sur un ensemble de particules quantiques faciles à observer et à manipuler un ensemble de particules intriquées difficiles à observer et à manipuler, et dont il est impossible de calculer le comportement, comme des électrons dans un matériau. Un des meilleurs exemples de simulateur est un ensemble d'atomes ou d'ions ultrafroids que l'on sait aujourd'hui très bien contrôler et observer avec des lasers.

Les grands progrès qui ont suivi l'article initial de Feynman ont été la découverte de l'algorithme de Shor et d'autres, comme l'algorithme de Grover, qui permet de chercher rapidement un élément dans une base de données. Au milieu des années 1990, ces avancées se sont faites sur la base d'un ordinateur quantique parfait. Aura-t-on un jour un ordinateur quantique parfait et universel ? La réponse est évidemment non. Mais des théoriciens, là encore extrêmement créatifs, ont imaginé des codes correcteurs quantiques d'erreur, analogues à ceux qui existent dans nos ordinateurs classiques. Cette découverte fut une grande surprise puisque beaucoup de spécialistes pensaient que la décohérence empêcherait d'y parvenir.

Mais le coût à payer est très élevé ! Pour simuler un bit quantique parfait avec des bits quantiques réels, même avec les meilleurs disponibles aujourd'hui, il n'en faut pas deux ni même 10, mais 1000, voire 10000. Pour un ordinateur quantique à 100 qubits parfaits, prévoyez probablement un million, peut-être un peu plus, de qubits réels de très bonne qualité. Or, le record du monde est de l'ordre de 50 aujourd'hui.

L'ordinateur quantique universel est-il donc hors de portée ?

Alain Aspect : Ma position sur le sujet ressemble à celle que j'avais il y a quarante ans sur la détection des ondes gravitationnelles. Je regarde le problème en tant que physicien, et je constate qu'aucune loi physique fondamentale ne fait obstacle à sa résolution. C'est bien le cas de l'ordinateur quantique parfait. Rien ne l'interdit, mais quand on contemple les sauts technologiques à accomplir, on ne voit pas bien aujourd'hui à quelle échéance on y parviendra. J'ai l'intime conviction que c'est une affaire de décennies.

Je peux toutefois me tromper. Demain, un progrès inattendu, par exemple dans la compréhension des espaces de Hilbert dans lesquels sont décrites les particules intriquées, peut changer la donne. En attendant, on essaye d'utiliser au mieux les simulateurs quantiques qui fonctionnent avec des qubits imparfaits, et profiter d'une percée conceptuelle due notamment à John Preskill, lui aussi à l'institut de technologie de Californie (et inventeur du terme de suprématie quantique) : on peut faire des choses intéressantes avec une évolution des simulateurs quantiques qu'il nomme des *noisy intermediate scale quantum computers* (NISQ)*, c'est-à-dire des ordinateurs quantiques imparfaits de taille intermédiaire. On peut espérer résoudre un certain nombre de problèmes avec des ordinateurs de ce type. Et tout un essaim de start-up se crée sur cette idée.

Que proposent-elles ?

Alain Aspect : L'idée de ces start-up est de reprendre des montages complexes de laboratoire manipulés par plusieurs docteurs ès sciences et ingénieurs, de les rendre fiables et faciles d'utilisation par des non-spécialistes afin de résoudre des problèmes d'optimisation, comme celui du voyageur de commerce déjà évoqué et celui, que je trouve particulièrement intéressant, de la grille électrique. Dans une zone où la production d'électricité est décentralisée (centrales nucléaires, photovoltaïque, éolien, hydraulique…) et où la consommation varie selon l'endroit, le moment de la journée, les saisons, il s'agit d'optimiser la distribution pour satisfaire tout le monde.

C'est un problème majeur à l'heure du réchauffement climatique, dont le calcul avec un ordinateur classique est très gourmand en temps. Or la réponse doit être rapide, de l'ordre de la minute. On a des raisons de penser que l'on peut aborder ce genre de problèmes avec des NISQ. Pour ce faire, vous devez maîtriser quelques dizaines de qubits intriqués. C'est le cas, par exemple ici, à l'Institut d'optique d'Antoine Browaeys et son équipe, qui contrôlent une cinquantaine d'atomes de Rydberg intriqués. Une start-up va bientôt commercialiser un tel système pour le mettre à la disposition de clients. Les fournisseurs d'énergie sont intéressés.

D'autres exemples de calculateurs NISQ reposent sur des ions, des circuits supraconducteurs, des photons… et de plus en plus de chercheurs se lancent dans la création de start-up afin de rendre disponibles des machines permettant de résoudre des problèmes réels. Cette démarche est extrêmement intéressante.

D'ailleurs, puisque l'on parle de réchauffement climatique, on peut envisager l'avantage quantique sous un autre angle. Imaginez un ordinateur quantique qui en performance serait équivalent aux machines classiques, mais en consommant cinq fois moins d'énergie. Ce serait aussi un sérieux avantage.

Toutes ces idées sont dans l'air et en cours d'évaluation dans le monde entier, aux États-Unis, au Canada, en Chine, en