

Une nouvelle révolution quantique



par **Alain Aspect**
Membre de l'Académie des sciences,
directeur de recherche au CNRS,
professeur à l'École polytechnique

Le développement de la physique quantique, au $XX^{\text{ème}}$ siècle, est l'une des aventures intellectuelles les plus extraordinaires de toute l'histoire humaine.

Cette théorie physique a modifié de fond en comble notre conception du monde, puisqu'elle nous force, par exemple, à accepter qu'une particule puisse se trouver à la fois ici et là, où qu'une porte quantique puisse être à la fois ouverte et fermée. Et elle a tout autant bouleversé notre mode de vie par ses applications innombrables : lasers, transistors, circuits intégrés, qui sont les composants de base des technologies de l'information et de la communication...

Une telle accumulation de succès aurait pu laisser craindre un épuisement du domaine : il n'en est rien. Qu'il s'agisse du comportement des électrons dans les solides, de l'interaction lumière matière, des fluides quantiques ultra-froids, on voit apparaître des phénomènes, certes compréhensibles dans le cadre de la physique quantique, mais tellement nouveaux et inattendus que l'intérêt rebondit sans cesse, ponctué par l'attribution de nombreux prix Nobel.

De façon sans doute encore plus imprévue, tant était grand le sentiment que « les pères fondateurs » (Niels Bohr et ses élèves) avaient totalement clarifié le sujet (essentiellement en répondant aux objections d'Einstein), c'est au niveau du cœur conceptuel de la théorie quantique qu'une nouvelle phase de progrès majeurs a débuté en 1960 avec les travaux de John Bell, suivis d'expériences de plus en plus fines. La violation des inégalités de Bell a apporté l'évidence irréfutable de l'*inséparabilité quantique*, propriété extraordinaire d'une paire d'objets intriqués qui se comportent comme un système quantique unique, même si les deux objets sont très éloignés l'un de l'autre.

C'est peu de temps après que l'on a appris à manipuler un par un des électrons, puis des ions, des atomes ou des photons. Il a alors fallu clarifier la façon d'appliquer le formalisme quantique fondamentalement probabiliste, à des objets individuels, et pas seulement à de très grands ensembles. Il n'est sans doute pas exagéré de dire que ces deux avancées conceptuelles de la fin du $XX^{\text{ème}}$ siècle – la compréhension et la maîtrise des états intriqués, la compréhension et la maîtrise de la dynamique des objets quantiques individuels – signent le début d'une *nouvelle révolution quantique*. Et il n'est pas interdit d'imaginer qu'au delà des progrès en physique fondamentale dont nous n'avons sans doute observé que les prémices, et des questions d'interprétation qui restent plus ouvertes que jamais, cette nouvelle révolution quantique pourrait à son tour bouleverser notre société en débouchant sur une *nouvelle révolution technologique*, la *révolution de l'information quantique*...

La première révolution quantique

L'émergence de la mécanique quantique a exigé des révisions conceptuelles déchirantes, comme le renoncement au concept classique de trajectoire, traduit par les relations de Heisenberg, ou la dualité onde particule. Mais la nouvelle théorie a permis de comprendre la structure de la matière à des échelles de plus en plus petites (liaison chimique, atome, noyau, particules élémentaires). La mécanique quantique a aussi permis de comprendre des propriétés beaucoup plus exotiques de la matière : la supraconductivité, c'est-à-dire la disparition de la résistivité électrique de certains conducteurs à très basse température, et la superfluidité de l'hélium liquide, c'est-à-dire la disparition de sa viscosité. Ces deux effets remarquables sont une conséquence de la « condensation de Bose-Einstein », phénomène imaginé par Einstein à l'époque des débuts de la mécanique quantique, qui se traduit par la condensation de toutes les particules dans la même onde de matière géante, que l'on a pu observer directement dans des expériences récentes.

Au delà de ces progrès sans précédents dans notre compréhension du monde, la physique quantique a permis l'émergence de technologies nouvelles, la microélectronique et l'optoélectronique, qui ont permis la montée en puissance de la société de l'information et de la communication. C'est en effet en s'appuyant sur la description quantique de la matière que les physiciens allaient inventer de nouveaux objets qui n'existaient pas dans la nature, et que les ingénieurs surent bientôt produire en grande série. Le transistor et ses descendants, les circuits intégrés, inventés par un groupe de brillants physiciens du solide à partir d'une réflexion fondamentale sur la nature quantique de la conduction électrique, ont permis la multiplication des possibilités de calcul, de traitement

et de stockage de l'information. Le laser, d'abord un instrument de physicien, est devenu omniprésent dans les applications les plus diverses, du guidage des engins de travaux publics aux lecteurs de code barre ou de disques compacts. Les télécommunications par laser et fibres optiques ont multiplié le débit d'information que l'on peut faire circuler à l'échelle de la planète et les autoroutes de l'information permettent aujourd'hui à l'humanité de partager les informations stockées dans les ordinateurs du monde entier, ou de mettre en commun leurs puissances de calcul.

La place prise par les applications des lasers ne doit pas faire croire que les progrès dans la compréhension et la maîtrise de l'interaction matière-lumière se seraient arrêtés en 1960. On a vu par exemple apparaître l'optique quantique dont la plupart des concepts étaient ignorés en 1960, et qui permet de repousser les limites des méthodes d'observation et de mesure optiques. On citera aussi la découverte *a priori* paradoxale, couronnée par le prix Nobel 1997 attribué à Steven Chu, Claude Cohen-Tannoudji, et Bill Phillips, du refroidissement par laser des vapeurs atomiques à des températures proches du zéro absolu. Ces progrès de la recherche fondamentale ont déjà débouché sur une amélioration spectaculaire de la précision des horloges atomiques, dont la précision conditionne celle de la localisation par satellite du système GPS. Ils ont aussi permis le développement d'interféromètres atomiques capables de détecter d'infimes anomalies de la pesanteur, ouvrant la voie à de nouvelles méthodes d'analyse du sous-sol. Et puis, par ce mouvement de balancier dont ils sont coutumiers, les physiciens projettent aujourd'hui d'utiliser ces nouveaux instruments à base d'atomes froids pour revenir sur des problèmes de physique fondamentale, comme des tests de relativité générale, ou la recherche d'éventuelles modifications des lois physiques à l'échelle de l'âge de l'Univers.

Ainsi, après bientôt un siècle, la *première révolution quantique* n'en finit pas de produire ses effets. La théorie quantique élaborée dans les années 1905-1925, et raffinée à la fin des années 1940, reste le cadre naturel dans lequel les physiciens continuent de découvrir et de comprendre les propriétés exotiques de la matière dans des situations extrêmes, ou même dans des conditions inconnues dans la nature. C'est aussi le cadre dans lequel doivent se placer les ingénieurs qui cherchent à pousser les technologies à leurs limites ultimes, de nature quantique. Mais au-delà de cette physique quantique bien établie, on assiste aujourd'hui à ce que l'on peut sans doute appeler une « *seconde révolution quantique* », qui a débuté avec les travaux de John Bell sur le problème d'Einstein-Podolsky-Rosen.

Dossier

Des objections d'Einstein aux photons jumeaux : l'intrication quantique

Le débat Bohr-Einstein

Les renoncements ayant permis l'émergence de la mécanique quantique étaient si radicaux que plusieurs physiciens, dont Einstein et de Broglie, et dans une certaine mesure Schrödinger, n'admettaient pas leur caractère définitif, à la différence de Bohr qui en avait fait la clef de voûte de l'interprétation de la nouvelle théorie connue sous le nom « d'interprétation de Copenhague ». Einstein ne remettait pas en cause le formalisme mathématique de la mécanique quantique, ni ses prévisions, mais il semblait penser que les renoncements préconisés par Bohr dans son interprétation ne traduisaient que l'état d'inachèvement de la théorie quantique. Cette position allait donner lieu des débats homériques entre eux, en particulier celui qui débuta avec la publication, en 1935, de l'article d'Einstein, Podolsky, et Rosen (EPR). Dans cet article, Einstein et ses coauteurs montrent que le formalisme quantique prédit l'existence d'états particuliers de deux particules, par exemple deux électrons, caractérisés par de très fortes corrélations à la fois des vitesses et des positions.

Plus précisément, pour un état EPR, le formalisme quantique prédit que des mesures de position sur chacun des deux électrons donneront des valeurs symétriques par rapport à l'origine, et que des mesures de vitesses donneront de même des résultats toujours identiques. Les deux électrons étant éloignés l'un de l'autre au moment de la mesure, on est conduit, pour comprendre ces corrélations, à admettre que chacun des électrons possédait avant la mesure une valeur parfaitement déterminée de vitesse et de position. Mais le formalisme quantique ne donne pas de valeur précise à ces quantités tant que la mesure n'est pas faite, et EPR concluent que le formalisme quantique ne rend pas compte de la totalité de la réalité physique, et qu'il faut donc s'attacher à essayer de le compléter. Niels Bohr fut, semble-t-il, bouleversé par cet argument qui s'appuie sur le formalisme quantique lui-même pour en montrer le caractère incomplet, provisoire. Ses écrits mon-

trèrent une conviction profonde que si le raisonnement EPR était correct, compléter le formalisme quantique ne serait pas suffisant, c'est toute la physique quantique qui s'effondrerait. Bohr contesta donc immédiatement le raisonnement EPR, en affirmant que dans un état quantique de ce type, « non factorisable », on ne peut parler des propriétés individuelles de chaque électron, et cela même s'ils sont très éloignés l'un de l'autre. Avec Schrödinger, qui découvrit au même moment ces états étonnants, on allait désormais parler « d'état intriqué », pour indiquer que les deux électrons sont indissolublement enchevêtrés, qu'ils forment un objet unique quelle que soit leur éloignement.

On pourrait penser que ce débat entre deux géants de la physique du XX^{ème} siècle eut un immense écho chez les physiciens. En fait, lorsque l'article EPR parut en 1935, la mécanique quantique allait de succès en succès et, mis à part Bohr, la plupart des physiciens ignorèrent une discussion qui leur paraissait académique : il semblait que l'adhésion à l'un ou l'autre des positions fût une affaire de goût personnel (ou de position épistémologique) sans aucune conséquence pratique sur la mise en œuvre du formalisme quantique, ce qu'Einstein lui-même ne semblait pas contester. Il fallut attendre presque trente ans pour voir paraître un démenti à cette position relativement consensuelle.

Les tests expérimentaux des inégalités de Bell

C'est en 1964 que John Bell, physicien théoricien irlandais travaillant au CERN à Genève, publie un court article qui va bouleverser la situation. En quelques lignes de calcul, il montre que si l'on prend au sérieux l'argument EPR, et donc qu'on introduit explicitement des variables supplémentaires (complétant le formalisme quantique) spécifiant la totalité de la réalité physique au sens d'Einstein, par exemple à la fois les positions et les vitesses des électrons intriqués, alors on aboutit à une contradiction avec les prédictions quantiques. Pour établir cette contradiction, John Bell montre que tout modèle dans l'esprit des idées d'Einstein ne peut prédire que des corrélations dont les valeurs sont limitées par des inégalités – aujourd'hui appelées « inégalités de Bell » – que violent certaines prévisions quantiques. Le choix entre les positions d'Einstein et de Bohr n'est alors plus une question de goût personnel, puisque les deux positions conduisent à des prévisions quantitativement différentes. Il devient possible de trancher le débat par l'expérience, en mesurant les corrélations dans des paires intriquées, et en confrontant les résultats aux inégalités

de Bell. En 1964, il n'existait aucun résultat expérimental permettant de conclure. Les expérimentateurs se mirent donc au travail pour construire une expérience « sensible », dans une des rares situations où la mécanique quantique prédit une violation des inégalités de Bell. Les expériences les plus convaincantes ont été réalisées avec des paires de photons, sur lesquels des mesures de polarisation – suivant deux directions distinctes – jouent un rôle analogue aux mesures de position et de vitesse dans le schéma EPR originel. Après une première génération d'expériences pionnières, une nouvelle série d'expériences conduites à Orsay au début des années 1980, suivant des schémas de plus en plus proches de « l'expérience de pensée » idéale, donnèrent un ensemble de résultats incontestables, en excellent accord avec la mécanique quantique, et violant nettement les inégalités de Bell. Une troisième génération d'expériences entreprises à partir du début des années 1990 sont venues conforter ces résultats. Il faut se rendre à l'évidence : *les photons intriqués jumeaux ne sont pas deux systèmes distincts portant deux copies identiques d'un même ensemble de paramètres (à la différence des jumeaux humains dont les ressemblances s'expliquent par l'identité de leurs chromosomes). Une paire de photons intriqués doit en fait être considérée comme un système unique, inséparable, décrit par un état quantique global, impossible à décomposer en*

deux états relatifs à chacun des deux photons : les propriétés de la paire ne se résument pas à la réunion des propriétés des deux photons.

L'inséparabilité quantique se manifeste même si les deux photons sont éloignés l'un de l'autre, et qu'aucune interaction ne peut *a priori* connecter causalement les mesures, sauf à se propager plus vite que la lumière, ce qui est interdit par la relativité. Ce point a été vérifié pour la première fois dans l'une des expériences réalisées à l'Institut d'optique d'Orsay en 1982, et confirmé en 1998 par une équipe autrichienne. Dans les expériences récentes, des sources d'un nouveau type permettent d'injecter les photons intriqués dans deux fibres optiques partant dans des directions opposées, et une équipe genevoise a pu vérifier que l'inséparabilité subsiste à des distances de plusieurs dizaines de kilomètres. Même à de pareilles distances, tout se passe donc comme si les deux photons restaient toujours en contact, et si le résultat de la mesure effectuée sur l'un affectait instantanément l'autre. Bien qu'on ne puisse utiliser ce phénomène pour transmettre de l'information plus vite que la lumière, les propriétés troublantes des états intriqués continuent à interpeller les physiciens qui sont loin d'avoir atteint un consensus sur la façon de comprendre l'inséparabilité quantique. Nul ne peut dire aujourd'hui si les progrès viendront de nouvelles expériences, de percées théoriques, ou de ruptures épistémologiques.

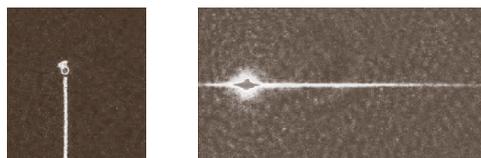


Figure 1. Lasers à atomes. À partir d'un condensat de Bose-Einstein, on peut extraire une onde de matière cohérente, constituée d'atomes tous décrits par la même fonction d'onde, comme un faisceau laser est une onde électromagnétique cohérente formée de photons tous dans le même mode du champ. Dans la figure de gauche, l'onde de matière (longueur de l'ordre du millimètre) tombe sous l'effet de la pesanteur, tandis que dans la figure de droite elle est guidée dans un guide d'onde atomique horizontal, comme un faisceau laser peut être guidé par une fibre optique. [Cliché Laboratoire Charles Fabry de l'Institut d'Optique].

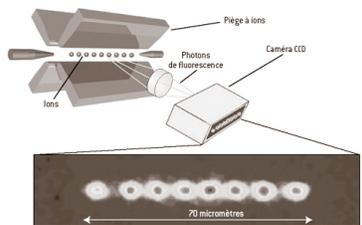


Figure 2. Chaîne d'ions piégés constituant un ensemble de qubits (bits quantiques). Par manipulation individuelle de ces ions, on peut les faire interagir et aboutir à un état intriqué. On réalise ainsi des opérations élémentaires du calcul quantique. [Cliché Université de Innsbruck].

Dossier

La mécanique quantique et les systèmes individuels

Jusqu'à la fin des années 1970, les situations expérimentales où la mécanique quantique était impliquée concernaient de très grands ensembles d'objets microscopiques sur lesquels on observait un signal moyenné. Ainsi, la lumière émise par une lampe à décharge, dont les propriétés spectrales ont conduit à la première révolution quantique, est-elle émise par les millions de milliards d'atomes d'un gaz. De même, la superfluidité de l'hélium liquide, ou la supraconductivité de certains métaux, s'observent-elles sur des quantités macroscopiques, où le nombre d'atomes est de l'ordre du nombre d'Avogadro (6×10^{23} , six cent mille milliards de milliards). Dans ce type de situation, il n'y a aucune difficulté à utiliser les résultats probabilistes des calculs quantiques. A partir des années 1970, les physiciens ont inventé des méthodes pour manipuler et observer un seul électron, ou un seul ion, conservé pendant des heures (voire des jours, des mois) à l'aide de champs électriques et magnétiques qui le maintiennent loin de toute paroi, dans une enceinte à vide : on parle alors de particule unique « piégée ». Puis est apparue la microscopie de champ proche (microscopie à effet tunnel, microscopie à force atomique), qui a permis d'observer et de manipuler des atomes individuels déposés sur une surface. A la même époque, les progrès conceptuels et expérimentaux de l'optique quantique ont conduit au développement de sources où les photons sont émis un par un. Ces avancées expérimentales, couronnées par plusieurs prix Nobel, ont d'abord eu des conséquences importantes en physique fondamentale. C'est ainsi que le piégeage d'objets élémentaires uniques a fait considérablement progresser la précision des mesures de certaines grandeurs microscopiques, dont la valeur fournit souvent un test sévère de la théorie. En parallèle avec les progrès expérimentaux, le piégeage d'objets microscopiques individuels a obligé les physiciens à se reposer la question, soulevée elle aussi par Einstein, de la signification de la théorie quantique lorsqu'on l'applique à un objet unique. Même si la question apparaissait totalement académique dans les années 1930, où l'on était loin de penser qu'on pourrait un jour observer des objets microscopiques uniques, les physiciens de l'école de

Copenhague ne l'éluadaient pas : pour y répondre, ils invoquaient le « postulat de réduction du paquet d'onde » qui affirme que lorsqu'un système quantique interagit avec un appareil de mesure, ce système quantique cesse d'être dans une superposition d'états et « saute » dans l'un ou l'autre d'entre eux. Appliqué à un ion unique piégé soumis à des faisceaux lasers convenablement choisis, ce raisonnement conduit à prédire l'existence de sauts quantiques aléatoires entre un état « brillant » ou l'ion diffuse beaucoup de photons observables à l'œil nu et un état « noir » ou aucun photon n'est diffusé. L'existence de ces « sauts quantiques », qui implique une évolution discontinue du système, avait été violemment contestée par nombre de physiciens parmi les plus grands (tel Schrödinger), qui y voyaient tout au plus un artifice commode, à valeur pédagogique, et semblaient penser que la description quantique ne s'appliquait qu'aux grands ensembles. Au milieu des années 1980, on a pu observer les sauts quantiques sur un ion unique piégé, dont la fluorescence varie brutalement lorsque l'atome saute d'un état à l'autre. Cette observation a beaucoup frappé les physiciens, et elle a déclenché de nouveaux progrès à la fois dans le domaine expérimental et dans le domaine théorique.

Du microscopique au mésoscopique et au macroscopique : la décohérence

Sachant que la mécanique quantique peut décrire le comportement des objets individuels microscopiques, on peut évidemment se demander si elle s'applique à des objets plus gros. On sait bien

qu'il n'y a pas besoin d'elle pour décrire le mouvement des planètes ou d'une pomme qui tombe : la physique classique s'en acquitte parfaitement, ce qui explique d'ailleurs sans doute la difficulté de comprendre les concepts quantiques à partir d'une intuition forgée dans le monde macroscopique. Mais il existe une échelle intermédiaire, l'échelle mésoscopique, où c'est l'objet lui-même – et pas seulement son matériau – qui doit être décrit par la mécanique quantique. On sait ainsi réaliser aujourd'hui des anneaux conducteurs mésoscopiques (à ne pas confondre avec les fils supraconducteurs), dont la taille est de l'ordre du micromètre, et dont la résistance électrique nulle ne peut être comprise qu'en considérant la fonction d'onde globale de l'ensemble des électrons de ce nanocircuit. Un autre exemple célèbre (prix Nobel 2001) d'objet mésoscopique est celui des condensats de Bose-Einstein gazeux, ensemble d'atomes (typiquement quelques millions) qui eux aussi doivent être décrits par une fonction d'onde quantique globale. Si ces objets mésoscopiques où une description quantique s'impose sont encore des curiosités des laboratoires de recherche fondamentale, il ne fait guère de doute que les progrès des nanotechnologies, en particulier la miniaturisation ininterrompue des composants semi-conducteurs, obligeront bientôt l'industrie de la microélectronique à utiliser une approche complètement quantique pour maîtriser ces nanocomposants.

Mais alors, si l'on observe un comportement quantique avec des objets de plus en plus gros, où se situe la frontière ? A vrai dire, on ne connaît pas la réponse à cette question, l'une des plus impor-

tantes qui soient posées aux physiciens du début du XXI^{ème} siècle. L'une des propriétés spécifiques de la physique quantique est l'existence des *superpositions d'états* : si un système possède plusieurs états quantiques possibles, il peut non seulement se trouver dans l'un d'eux, mais il peut également se trouver dans un état hybride formé à partir de ces états de base, une « *superposition cohérente* » de ces états. Ainsi, un atome arrivant sur une séparatrice à atomes, analogue à une lame semi-réfléchissante pour les photons, peut soit être transmis, soit être réfléchi, ce qui conduit à des trajectoires distinctes. Mais il peut aussi être dans une *superposition des états transmis et réfléchis*, c'est-à-dire *présent à la fois en deux points différents de l'espace*. On peut démontrer expérimentalement que cet état existe vraiment, en recombinant les deux trajectoires et en observant des interférences, qu'on ne peut interpréter qu'en admettant que l'atome a suivi les deux chemins à la fois. Un tel comportement a effectivement été observé avec des objets microscopiques (électrons, photons, neutrons, atomes, molécules), ou mésoscopiques (courants électriques dans des nanocircuits), mais jamais avec des objets macroscopiques, alors que rien ne l'interdit *a priori* dans le formalisme quantique. Ce problème a attiré l'attention de nombreux physiciens, à commencer par Schrödinger qui en a donné une illustration amusante sous la forme du fameux chat qui pourrait à la fois être mort et vivant, ces deux états représentant un exemple particulièrement frappant d'états incompatibles. Pourquoi, dans le monde réel, n'observe-t-on pas la superposition cohérente des états « mort » et « vivant » ?

Est-il mort, est-il vivant ?



Dossier

Les physiciens invoquent généralement la *décohérence quantique* pour expliquer l'impossibilité d'une superposition cohérente d'états d'objets macroscopiques. La décohérence doit se manifester dès qu'un système quantique interagit avec le monde extérieur. Reprenons l'exemple de l'atome dont les trajectoires se sont séparées puis sont recombinées pour donner des interférences. Si on l'éclaire avec de la lumière laser, il devient possible d'observer sa trajectoire et de dire s'il suit un trajet ou l'autre. Mais la lumière d'éclairage perturbe l'atome, et les interférences disparaissent. On retrouve une situation classique, sans superposition cohérente : l'atome suit un chemin ou l'autre, pas les deux à la fois. Or, plus un objet est complexe et gros, et plus il est, en général, sensible aux perturbations extérieures qui font disparaître les interférences. La décohérence par interaction avec le monde extérieur serait donc la clef du passage entre comportements quantique et classique. Même si ce raisonnement est séduisant, de nombreuses questions restent posées. A l'heure actuelle, on n'a aucun argument vraiment convaincant permettant de savoir s'il existe une taille limite fondamentale au-dessus de laquelle la décohérence serait inévitable et les superpositions quantiques cesseraient d'exister. Une réponse à cette question aurait des implications immenses, tant sur le plan conceptuel que pour les technologies du futur basées sur l'hypothétique ordinateur quantique.

L'information quantique

Nous avons suggéré plus haut que la prise de conscience du caractère extraordinaire de l'intrication quantique, couplée à la maîtrise des objets microscopiques individuels, avait marqué le début d'une nouvelle révolution quantique. La portée de cette nouvelle révolution quantique pourrait aller bien au-delà des concepts, et conduire à des applications révolutionnaires dans le traitement et la transmission de l'information. C'est le domaine de l'*information quantique*, qui vise à mettre en œuvre ces concepts physiques nouveaux pour aboutir à deux types d'applications : d'une part la cryptographie quantique, qui commence à être opérationnelle, et d'autre part le calcul quantique, qui n'en est qu'à une phase de recherche fondamentale encore très éloignée des éventuelles applications.

La cryptographie a pour but de communiquer des informations codées sur un canal public sans que des tiers puissent les déchiffrer. Les progrès dans le codage et les tentatives de déchiffrement s'appuient d'une part sur des avancées mathématiques, d'autre part sur la puissance croissante des ordinateurs, et on

comprend que la sécurité d'un code repose sur l'hypothèse que l'espion qui tente de déchiffrer un message n'a pas un niveau de développement en mathématiques ou en informatique beaucoup plus avancé que l'expéditeur. Seule fait exception la méthode par clef de codage à utilisation unique : il s'agit d'une suite aléatoire de caractères, existant en deux exemplaires identiques entre les mains de l'émetteur et du récepteur. On montre, par un théorème à la rigueur toute mathématique, qu'il est alors possible de réaliser un codage inviolable d'un message, pourvu que sa longueur soit inférieure ou égale à celle de la clef secrète, qui ne doit être utilisée qu'une fois. La *cryptographie quantique* va permettre de renouveler la clef en distribuant à deux partenaires éloignés deux suites identiques de bits, avec la garantie qu'aucun espion n'a pu intercepter cette clef et en faire une copie. L'idée de base est qu'il est possible de détecter un espion tentant de prendre connaissance de la clef secrète par la trace qu'il laisse nécessairement, et que la mécanique quantique permet de préciser. Par exemple, dans l'un des schémas qui utilise des paires de photons intriqués pour engendrer les deux clefs identiques, on montre que la présence éventuelle d'un espion sur la ligne peut être démasquée par un test des inégalités de Bell.

Le *calcul quantique* a été lancé, au début des années 1990, par une découverte théorique : la démonstration mathématique que si l'on disposait d'ordinateurs quantiques, capables d'utiliser le phénomène d'intrication, on pourrait mettre en œuvre des algorithmes radicalement nouveaux permettant d'effectuer certaines opérations difficiles, comme la décomposition d'un nombre (grand) en facteurs premiers, dans des temps exponentiellement plus courts qu'avec les méthodes habituelles. Cette découverte a une portée conceptuelle considérable, puisqu'elle montre que la façon de faire les calculs (l'algorithme)

n'est pas indépendante du type de machine utilisé. Elle pourrait aussi avoir des conséquences pratiques immenses, puisque le cryptage (classique) des informations (par exemple sur la télé) repose aujourd'hui sur l'impossibilité de factoriser les très grands nombres en un temps raisonnable.

Encore faut-il être capable de construire un ordinateur quantique. De nombreux groupes dans le monde se sont lancés dans le développement de systèmes physiques réalisant la variable quantique élémentaire, le qubit, et l'unité de calcul de base, la porte logique quantique. Une porte logique quantique doit pouvoir combiner plusieurs qubits en donnant pour résultat un état intriqué. D'intrication en intrication, on obtient des états représentant simultanément un nombre immensément grand de situations, et il est possible d'effectuer des calculs massivement parallèles, même avec un nombre modéré de portes logiques quantiques. Plusieurs pistes sont en cours d'exploration, avec des bits quantiques reposant sur les systèmes les plus divers : atomes, ions ou photons uniques, mais aussi molécules complexes manipulées par les méthodes de la résonance magnétique nucléaire, ou jonctions Josephson, systèmes artificiels réalisés par les techniques de nanofabrication. L'ordinateur quantique existera-t-il un jour ? Il serait présomptueux de répondre, mais la recherche expérimentale sur les portes logiques quantiques est très active et a déjà obtenu des résultats intéressants. Il demeure une grande inconnue : saura-t-on maîtriser le problème de la *décohérence*, dont les effets sont d'autant plus dévastateurs que le système est plus grand ? Ce n'est qu'à cette condition que l'on pourrait croire en l'avenir de l'ordinateur quantique. Mais même si l'on n'aboutit pas à une réalisation concrète telle qu'on peut en rêver aujourd'hui, nul doute que cet effort de recherche marquera une étape importante dans l'histoire de l'informatique aussi bien que dans celle de la physique quantique.

La physique quantique : un défi pour l'intuition, une source de ruptures technologiques

Un siècle après son émergence, la physique quantique occupe toujours une position singulière. Elle met en jeu des concepts absolument étrangers à une intuition forgée par l'observation des objets et des phénomènes à notre échelle. Même si les physiciens s'y sont habitués, et même si l'on maîtrise le formalisme mathématique permettant d'en rendre compte, ces concepts restent déroutants. Aux difficultés originelles s'est ajouté le concept d'intrication. Par ailleurs, la question de la frontière entre le monde quantique et le monde classique, plaisamment illustrée par la parabole du chat de Schrödinger, reste un des problèmes conceptuels majeurs sur lesquels butent les physiciens, même si des progrès dans la compréhension des phénomènes de décohérence ouvrent des pistes intéressantes.

L'existence de questions non résolues ne doit pas nous faire oublier les succès extraordinaires de la physique quantique. La première révolution quantique, d'abord conceptuelle, a permis une avancée sans précédent dans la compréhension du monde au niveau microscopique, et a été à l'origine d'une révolution technologique formidable qui nous a fait plonger dans la société de l'information et de la communication. Peut-être revivons-nous aujourd'hui une histoire analogue, avec une nouvelle révolution quantique d'abord conceptuelle, mais qui pourrait avoir un immense impact sur la société si l'information quantique tient ses promesses. Certes nous en sommes loin. Mais on peut parier, sans trop de risques, que des applications que nous ne soupçonnons pas aujourd'hui émergeront tôt ou tard, car comment des phénomènes aussi extraordinaires ne stimuleraient-ils pas l'imagination des chercheurs et des inventeurs ? ■

Pour en savoir plus

Demain la physique (éditions Odile Jacob, 2004).

Einstein aujourd'hui (EDP sciences) : chapitre 2

(A Aspect et P. Grangier).

Bell's theorem : the naive view of an experimentalist (A. Aspect) : téléchargeable librement sur <http://hal.ccsd.cnrs.fr/ccsd-00001079> ; version française sur http://www.institutoptique.fr/telechargement/inegalites_Bell.pdf.

Speakable and unspeakable in quantum mechanics (J. S. Bell, Cambridge University Press, 2ème édition, 2004).

Cours et séminaires de la chaire de Physique Atomique et Moléculaire du Collège de France (C. Cohen-Tannoudji, 1973-2003) disponibles sur : [http://www.phys.ens.fr/cours/college-de-france/Cours-et-seminaires-de-la-chaire-de-Physique-Quantique-du-Collège-de-France\(S.Haroche\)](http://www.phys.ens.fr/cours/college-de-france/Cours-et-seminaires-de-la-chaire-de-Physique-Quantique-du-Collège-de-France(S.Haroche)) disponibles sur :

<http://www.lkb.ens.fr/recherche/qedcav/college/college.html>

Article publié dans la Lettre n°15 de l'Académie des Sciences Mai 2005
<http://www.academie-sciences.fr/activite/lettre/lettre15.pdf>