# Le monde, à l'aube d'un avenir quantique

Par le Pr Baddari Kamel(*)

La formulation de nouvelles théories scientifiques, l'émergence de nouvelles méthodes expérimentales et théoriques stimulent la création de nouveaux équipements expérimentaux, puis de nouvelles technologies et produits. Dans le cadre du concept de Thomas Kuhn, une révolution scientifique est une étape qualitativement nouvelle dans le développement des connaissances sur le monde, elle se définit comme un passage d'un paradigme à un autre. L'édification de la mécanique quantique (MQ) qui fut certes une rupture épistémologique, mais aussi l'une des plus grandes révolutions scientifiques de tous les temps. Mais, sans doute, elle doit être considérée comme la plus grande percée sociohistorique dans le sens de la rationalisation de l'existence humaine et de ses constructions intellectuelles. Elle révèle le fonctionnement intime du monde microscopique et de la nature. Son formalisme a permis de faire des prédictions qui ont été confirmées par l'expérience et rapidement transformées en nouvelles technologies : c'est la première révolution quantique. La deuxième est en cours.

## Que sont les technologies quantiques ?

En ce premier quart du XXe siècle, l'humanité est entrée dans une nouvelle étape de son développement – l'étape d'élaboration de la relativité restreinte (1905) et la relativité générale (1915-1917), puis de l'édification de la mécanique quantique (MQ) (1925-1927). Comme un clin d'œil de l'Histoire, la théorie quantique, destinée à comprendre et expliquer le comportement de la matière au niveau des atomes et des particules, a connu un succès éclatant, son formalisme a permis de faire des prédictions, qui ont été confirmées par l'expérience et rapidement transformées en nouvelles technologies. Le caractère révolutionnaire de la MQ se manifestait sous deux aspects. Dans l'aspect ontologique, de nouvelles idées sur la nature des phénomènes quantiques ont été proposées. De nouveaux concepts, objets et principes fondamentaux ont été introduits, il a été proposé soit d'abandonner les anciens, soit de limiter leur application. Les postulats concernant les modes d'existence, la causalité et le hasard ont été remis en question. Dans l'aspect épistémologique, la MQ a suggéré d'abandonner les postulats méthodologiques et les logiques habituels, les schémas de recherche et les explications. De nouveaux principes de connaissance, d'observabilité, de complémentarité des diverses descriptions, de correspondance des théories ont été proposés, le rôle de l'observateur a été révisé. La découverte de la mécanique quantique a finalement donné à l'humanité la plupart des technologies dont on se souviendra pour ce siècle : armes nucléaires, lasers, horloges atomiques, accélérateurs de particules, IRM, les microscopes à tunnel à balayage et toute l'électronique à semiconducteurs en général, des transistors et LED aux ordinateurs, et plus tard aux communications mobiles, GPS et à internet. Le volume du marché des produits connexes dans le monde est de 3 billions de dollars par an.

Toutes ces technologies et dispositifs reposent sur la gestion de phénomènes quantiques collectifs, c'est-à-dire ceux qui impliquent des interactions au niveau des flux de particules (atomes, molécules, photons ou électrons), des champs et des environnements divers observés. Cette période de développement de la physique et de la technologie est généralement appelée la première révolution quantique. À la toute fin du XXe siècle, les scientifiques ont appris à contrôler des systèmes quantiques complexes au niveau de leurs composants les plus élémentaires, c'est-à-dire à manipuler des atomes et même des particules élémentaires, comme les photons, ce qui a permis de créer des systèmes de cryptage et de calcul quantiques. Et cela a ouvert la voie à l'ère de la deuxième révolution quantique, au tout début de laquelle nous vivons aujourd'hui. Une description détaillée de la deuxième révolution quantique est donnée dans le *Manifeste quantique de l'Europe* (2016).

## Quand l'ordinateur devient quantique

L'informatique quantique sera l'une des technologies clés susceptibles d'apporter la révolution moderne de la MQ. L'ordinateur à transistors traditionnels est fondamentalement différent de ses frères aînés basés sur des puces de silicium. Nous parlons de la capacité d'effectuer des calculs probabilistes d'une telle complexité qui n'est pas disponible pour les supercalculateurs modernes. En informatique traditionnelle, l'information est stockée et manipulée sur un bit - c'est le nom de la plus petite unité d'informations qui ne peut prendre que deux valeurs: zéro (bloquant) ou une (passant). Un ordinateur moderne traditionnel, le même processeur de smartphone, contient des milliards de registres, dont chacun au même moment ne peut être que dans l'un des deux états - soit 1 ou 0. Un peu peut-être comparé à une ampoule qui est soit allumée (1) soit éteinte (0). Un fichier sur le disque ressemble à un ensemble d'ampoules pour un ordinateur, dont certaines sont allumées et d'autres pas. Mais lorsque l'appareil résout un problème, il allume et éteint les lumières, enregistrant et effaçant constamment les résultats des calculs intermédiaires afin qu'ils ne bouchent pas la mémoire. Cela prend du temps, donc si la tâche est très difficile, l'ordinateur prendra beaucoup de temps à réfléchir. La base théorique de la technologie des ordinateurs quantiques a commencé à être posée dans les années 1980, avec notamment les travaux de Richard Feynman. Entre la fin des années 1980 et le début des années 1990, le physicien David Deutsch et le mathématicien Richard Jozsa mirent en évidence le premier algorithme quantique, c'est-à-dire une suite d'opérations logiques exploitant les principes de superposition et d'intrication, et résolvant un problème plus rapidement que tous les algorithmes traditionnels connus. En 1994, l'intérêt reprit autour d'un algorithme mis au point par Peter Shor. En effet, cet algorithme, conçu pour fonctionner sur un ordinateur quantique, pourrait décomposer rapidement de grands nombres en facteurs premiers (une tâche nécessaire pour casser les chiffrements modernes). Les ordinateurs conventionnels résolvent ce problème en énumérant les diviseurs possibles, de sorte que les ordinateurs modernes peuvent traiter des nombres longs pendant des années. Un ordinateur quantique ferait une telle tâche en quelques minutes, voire quelques secondes, selon les performances. Contrairement aux appareils traditionnels, les ordinateurs quantiques stockent et traitent les données à l'aide de bits quantiques (qubits) - superposition des états 1 et 0, c'est-à-dire simultanément dans une valeur de 1 et 0, ce qui donne une combinaison linéaire des états 1 et 0. Pour illustrer cet état de superposition quantique, nous pouvons utiliser l'analogie célèbre du «chat de Schrödinger» souvent évoquée en MQ. Soulignons que les particules élémentaires ou leurs amas créés artificiellement - en fait, des atomes artificiels - sont utilisés comme qubits. Ces derniers permettent d'effectuer des calculs des milliards de fois plus vite, pratiquement inaccessibles aux ordinateurs numériques classiques. De façon plus surprenante, cela permet à un ordinateur quantique de gérer des tâches qu'un ordinateur numérique typique prendrait des millions d'années à accomplir. À mesure que le nombre de qubits combinés augmente, le système connaît une croissance exponentielle de sa puissance de calcul. Les ordinateurs quantiques les plus avancés aujourd'hui contiennent des dizaines de qubits, tandis qu'une percée révolutionnaire en matière de performances nécessitera des ordres de grandeur supplémentaires, allant de milliers à des millions.

## La communication quantique : rendez-vous du futur

Après la création d'un ordinateur quantique, la cryptographie classique deviendrait un moyen inefficace de protéger les informations. C'est pourquoi, la cryptographie quantique est apparue. Cette technologie de protection cryptographique de l'information utilise des particules quantiques individuelles pour transférer des clés. La communication quantique exploite le concept d'intrication, c'est-à-dire l'existence de corrélations dans les propriétés physiques des particules d'un système quelle que soit la distance qui les sépare. Toute modification de ces informations ne peut être passée inaperçue. Cela signifie qu'aucun hacker ne peut extraire des informations quantiques sans laisser de trace. L'internet actuel est loin d'être sécurisé. Le film *Die Hard 4.0*, tourné il y a 13 ans, décrit les conséquences d'un piratage des infrastructures de Washington pendant que toute la ville était paralysée. Imaginez simplement qu'à un moment donné, tous les flux d'informations seront attaqués, les lumières s'éteindront, les supermarchés et les feux de signalisation cesseront de fonctionner, le système de transport échouera, la collecte des ordures s'arrêtera, l'approvisionnement en eau ne fonctionnera pas, et les services, en général, cesseront de fonctionner. Cela permet de dire que la destruction des flux d'informations est une menace très grave pour la société. La plupart de la technologie en est à ses débuts. La plupart des scientifiques imaginent une première version de ce Net à qubits pour 2024-2025.

## Des investissements dans le monde entier

Depuis quelques années, le volume de données généré chaque jour est tout simplement énorme, notamment avec l'explosion récente du «big data» et les ordinateurs modernes ne suivent plus toujours de tels volumes : la loi de Moore n'est plus valide - il n'y a pas de doublement de la puissance de calcul tous les deux ans. Les supercalculateurs sont encore trop lents pour certaines des tâches scientifiques les plus importantes, comme tester les effets de nouveaux médicaments au niveau moléculaire. Beaucoup de gouvernements suivent ces développements et investissent pour le leadership des technologies quantiques. Ainsi, en août 2020, Trump alloue un milliard de dollars, en plus des 237 millions destinés à l'informatique quantique, pour créer sept institutions de recherche en intelligence artificielle et cinq centres de recherche en informatique quantique. L'Inde a alloué 1,12 milliard de dollars au développement d'ordinateurs quantiques. L'Union européenne a prévu de consacrer un milliard d'euros sur 10 ans aux technologies quantiques, via un programme «FET Flagship». L'Allemagne, jusqu'à la fin 2021, investirait 650 millions d'euros pour le transfert de technologie de la recherche fondamentale vers des applications prêtes à l'emploi. Du coup, les grandes entreprises investissent dans cette direction, comme l'américain Google, Microsoft, Intel, Honeywell et IBM (ce dernier offre déjà aux clients l'accès à son ordinateur quantique via le cloud ), le japonais Toshiba et le chinois Alibaba et Baidu. L'un des ordinateurs quantiques les plus avancés du moment a été créé par Google - il s'appelle Sycamore et comprend 54 qubits (53 d'entre eux fonctionnent simultanément). En octobre 2019, les employés de l'entreprise ont publié un rapport dans *Nature* sur les résultats d'une expérience, au cours de laquelle Sycamore a fait face à des calculs en 200 secondes, ce qui aurait pris 10 mille ans à un supercalculateur puissant. Ainsi, Google a été le premier de l'Histoire à atteindre la «suprématie quantique» en laboratoire. En juin 2020, Honeywell a annoncé le lancement de ce que la société prétend être l'ordinateur quantique plus puissant de l'Histoire (64 qubits). À l'aide d'hélium liquide, le système est refroidi à une température proche du zéro absolu (–262,7 ° C). Plusieurs clients ont déjà commencé à utiliser le système, dont la banque JP Morgan Chase. La Chine est en phase de créer son laboratoire quantique national d'un budget de l'ordre de douze milliards de dollars. Elle affirme avoir un ordinateur quantique de

100 billions de fois plus rapide que le supercalculateur le plus avancé.

## Comment l'Algérie peut s'impliquer dans le développement quantique ?

Les technologies quantiques sont l'un des métiers d'avenir, l'un des domaines prometteurs de l'emploi de masse. Elles seront des innovations dans le secteur manufacturier, des communications routières, des systèmes de navigation, de la lutte contre la cybercriminalité, de diagnostic des maladies, de développement des médicaments, de la métallurgie, etc. Pour ne pas rater ce «virage technologique», notre pays, en tout cas, doit y croire, et préparer un «plan national», qui fera partie du projet national d'économie numérique. Il comprendra les tâches de formation de ressources humaines pour la sphère quantique et le développement de l'ensemble de l'écosystème de l'industrie. Cela dit, entre autres, la création d'une base d'infrastructure, de programmes éducatifs et de consortiums avec des partenaires industriels. Les secteurs pilotes de développement des technologies quantiques sont l'informatique quantique, la communication quantique et enfin les capteurs quantiques. Pour réveiller l'université algérienne sur le quantique, elle peut participer à l'avancée de la recherche en développant l'aspect Software (nouveaux algorithmes), et investir dans les start-up dans la communication et les solutions de cryptographie quantique. On peut d'ores et déjà programmer des formations initiales et développer des formations continues dans ce sens. A moyen terme, il est nécessaire de préparer les enfants aux métiers du futur dès les premiers stades de leur parcours éducatif. L'âge scolaire est l'âge où les rêves sont faits. Une percée dans la science et dans les professions futures devrait commencer précisément à cet âge.

## Et pour ne pas conclure

Les conséquences de la deuxième révolution quantique ne se sont pas encore pleinement manifestées. Les gouvernements comme les grandes entreprises de différents pays enjambent la révolution et lancent des plans ambitieux pour anticiper les changements et répondre aux futurs besoins. Cela devrait conduire à de nombreuses avancées dans une grande variété de domaines, en particulier de l'informatique et des ordinateurs quantiques, de la cryptographie quantique et post-quantique, ainsi que des industries de la défense, de l'automobile, de l'espace, de la simulation des nouveaux matériaux, des capacités de contrôle automatique et bien plus encore, sans parler de la science fondamentale. Fin XXe - début XXIe siècle devrait devenir l'ère de l'approbation des nouvelles technologies dans le domaine de la production, de la vie quotidienne, de l'organisation sociale, de la politique, de la communication et de la culture. L'Algérie a des atouts à mettre en valeur pour appréhender les enjeux de cet avenir.

**B. K.**

***Professeur des universités, expert en stratégie de l'ESRS et conduite de changement, Université de M'sila**