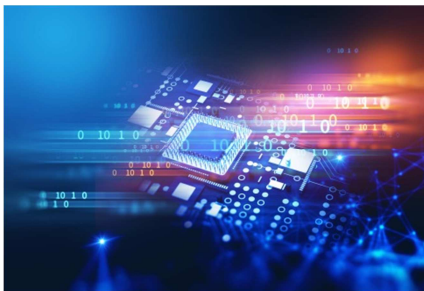


# Note n° 13 — Les technologies quantiques : introduction et enjeux

Mars 2019



© monsitj/ Adobe Stock

## Résumé

- De nombreuses technologies de notre vie quotidienne se basent sur les principes de la physique quantique : lasers, transistors, dispositifs de positionnement par satellite (GPS)...
- Depuis quelques années, les technologies quantiques au sens large connaissent un intérêt marqué aussi bien de la part des industriels que des gouvernements, en parallèle de progrès techniques de rupture.
- Les nouvelles technologies quantiques concernent des applications telles que les capteurs, le calcul ou les communications. Ces domaines s'appuient sur les principes de la physique quantique, en particulier l'intrication et la superposition d'états.
- En Europe, un programme d'envergure de type « flagship » a été lancé en 2018 pour soutenir les projets européens dans la course mondiale aux technologies quantiques, dont les principaux concurrents étatiques sont la Chine et les États Unis.

## M. Cédric Villani, Député, Premier vice-président

Les investissements dans le domaine des technologies quantiques ont connu une expansion forte au cours des dernières années. Ces projets, orientés aussi bien vers la recherche fondamentale que vers des innovations de rupture, et donnant lieu à une vive compétition scientifique et technologique internationale, appellent une attention particulière.

### Physique quantique et applications historiques

À l'échelle atomique, les lois de la physique classique peinent à décrire le comportement des particules telles que les atomes, électrons et photons. Dans les années 1920, Niels Bohr, Louis de Broglie, Erwin Schrödinger, Werner Heisenberg et beaucoup d'autres scientifiques mettent au point une théorie, dotée de son propre formalisme mathématique, pour mieux comprendre les phénomènes à l'œuvre à l'échelle de ces particules. Ces travaux marquent la naissance de la physique quantique.

En physique classique, un objet physique – un atome par exemple – d'une part, possède une énergie qui évolue de manière continue, d'autre part, peut-être modélisé par un point qui se trouve à une position précise à un temps donné. Il se distingue clairement des ondes, qui correspondent à la propagation d'une perturbation dans l'espace.

En physique quantique, les échanges d'énergie se font de manière discrète, ou discontinue, par paquets appelés « quantas<sup>(1)</sup> ». Ce principe de quantification, imaginé dès 1900 par Max Planck, pose les premiers fondements de la physique quantique, dans laquelle les concepts d'onde et d'objet ponctuel fusionnent pour expliquer le comportement des objets à

l'échelle atomique. Dans le cadre de cette dualité onde-corpuscule, on ne peut plus prédire la position exacte d'un corpuscule à un instant donné, mais seulement la probabilité de le trouver en un endroit donné à cet instant. Ces phénomènes, assez contre-intuitifs, se trouvent à l'origine des deux principaux concepts utilisés par la majorité des technologies utilisant la physique quantique : la superposition d'états et l'intrication.

Avec le principe de superposition, l'état global d'un système quantique à un instant donné devient une combinaison linéaire de tous ses états possibles à cet instant. Seule la probabilité de présence d'une particule à une position donnée peut-être prédite.

En parallèle, quiconque tente de mesurer avec exactitude l'état de la particule se heurte à la relation d'indétermination de Heisenberg<sup>(2)</sup>. Selon cette relation fondamentale, il est impossible de connaître simultanément la position et la vitesse d'une particule quantique. De manière plus générale, l'acquisition d'information sur une grandeur quantique implique nécessairement la perte d'information sur d'autres. En d'autres termes, en physique quantique, il est impossible d'effectuer une mesure sans perturber l'état de l'objet mesuré.

L'intrication consiste en la connexion entre deux, ou plusieurs, objets quantiques et entre leurs informations. Une modification d'état chez l'un entraîne un changement chez l'autre de manière instantanée. Il faut alors considérer la paire comme un système unique, inséparable et global : les propriétés de la paire ne sont pas simplement égales à la réunion des propriétés des deux corps.

**De nos jours, des dispositifs utilisés au quotidien se fondent déjà sur la physique quantique**, à l'instar du **GPS** (*Global positioning system*) : notre position est déterminée avec la précision du mètre (voire du cm) grâce aux **horloges atomiques**, créées dès les années 1960 et embarquées dans les satellites en orbite. Ces horloges, qui se fondent sur l'immutabilité des fréquences de transition d'états de certains atomes<sup>(3)</sup>, caractéristique de la physique quantique, permettent des corrections indispensables au bon fonctionnement des systèmes de positionnement par satellite de type GPS<sup>(4)</sup> et à leur précision. La technologie des **lasers**<sup>(5)</sup> a également été rendue possible grâce aux avancées dans le domaine quantique, notamment en optique et en électronique. Utilisés aujourd'hui dans une très large gamme d'applications, ils ont été mis au point dans la même période que les horloges atomiques. Enfin, **les transistors et les circuits électroniques intégrés**, qui forment aujourd'hui la base des technologies de la communication et de l'information, font aussi partie des premières applications qui marquent rétrospectivement la **première révolution quantique**.

**Il faudra attendre les années 1980 pour voir poindre les premières idées d'applications potentielles de la physique quantique en calcul et en informatique**, avec notamment les travaux de Richard Feynman<sup>(6)</sup> sur la puissance éventuelle d'un ordinateur qui aurait la capacité de simuler des phénomènes quantiques. Progressivement, la notion de calculateur quantique voit le jour, entre la fin des années 1980 et le début des années 1990, via les travaux du physicien David Deutsch et du mathématicien Richard Jozsa qui ont permis de créer le premier algorithme quantique<sup>(7)</sup>, 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 classiques connus. De manière très théorique, ils démontrent que **certains calculs seraient sensiblement accélérés si les principes de la physique quantique pouvaient être appliqués aux ordinateurs**. En 1994, la mise au point de l'algorithme de Shor renouvelle l'intérêt pour le sujet. En effet, cet algorithme, conçu pour fonctionner sur un ordinateur quantique, **pourrait décoder en un temps record les protocoles de chiffrement**<sup>(8)</sup> de données utilisés à la fois par les gouvernements et pour les usages civils. À l'époque, la menace demeure cependant théorique, car les technologies nécessaires à la conception d'ordinateurs quantiques n'existent pas encore. Mais cet épisode ouvre la voie aux scientifiques pour tenter de mettre au point des algorithmes quantiques plus performants que les algorithmes classiques usuels.

En parallèle, les progrès scientifiques et techniques continuent : dans les années 1960, des travaux majeurs sont initiés par John Bell avant d'être repris, au début des années 1980, par les expériences « EPR » d'Alain Aspect<sup>(9)</sup> qui prouvent de manière

irréfutable le phénomène d'intrication quantique, malgré le scepticisme de la communauté scientifique de l'époque. Ces expériences assez complexes vont permettre **de préparer et manipuler des objets quantiques (atomes, ions, photons) individuellement, ce qui ouvre un nouveau champ des possibles** pour avancer sur les principes théoriques de la physique quantique, mais aussi sur de potentielles applications en utilisant les principes de superposition et d'intrication quantique.

### Les propriétés quantiques à la base des technologies quantiques

La superposition permettrait de démultiplier la puissance des ordinateurs actuels. En informatique classique, l'information est stockée et manipulée sur un bit, c'est-à-dire un support physique de valeur 0 (bloquant) ou 1 (passant). Dans un état quantique, du fait du principe de superposition, l'état (ou la valeur) du support devient une combinaison linéaire des états 0 et 1. **Pour N bits quantiques, le système connaît une croissance exponentielle de sa puissance de calcul car il existe alors  $2^N$  états possibles**<sup>(10)</sup>. Quelques bits quantiques suffiraient donc à atteindre des capacités de calcul considérables.

En parallèle, **l'intrication permet de communiquer, c'est-à-dire, cette fois-ci, d'échanger de l'information, de manière sécurisée, à distance**. Les dernières expériences ont montré qu'une paire d'objets quantiques reste intriquée même à des centaines de kilomètres l'un de l'autre. Cela permet de détecter des « intrusions » (perturbations) sur une ligne de communication sensible par exemple, c'est pourquoi la cryptographie est devenue l'un des principaux domaines d'application de l'intrication.

Comme dans l'exemple des horloges atomiques, les **capteurs quantiques** reposent, eux, sur la reproductibilité d'un système quantique mais aussi sur sa sensibilité à l'échelle du système quantique unique. Concrètement, il s'agit, par exemple, de **manipuler des atomes isolés presque individuellement**<sup>(11)</sup> **pour effectuer des mesures de grande précision** (champ électrique, magnétique, de gravité etc...). C'est le cas, notamment, des systèmes à résonance magnétique, et en particulier de leur application à l'imagerie médicale, l'IRM<sup>(12)</sup>, qui permet d'observer l'intérieur du corps humain de manière non invasive avec un contraste et une précision sans équivalent. Les capteurs quantiques connaissent des développements depuis des décennies, notamment grâce à des progrès techniques qui permettent d'améliorer leur sensibilité et aussi d'élargir leur champ d'applications.

### L'informatique : nouveaux besoins et deuxième révolution quantique

Depuis quelques années, **la demande en puissance de calcul n'a cessé de croître**, notamment avec l'explosion récente du « big data »<sup>(13)</sup> et le besoin de simulations numériques toujours plus précises.

Jusqu'à maintenant, une des solutions pour répondre à cette demande consistait à utiliser des **supercalculateurs** en parallèle, avec des coûts élevés et une consommation électrique croissante<sup>(14)</sup>. La croissance de la demande pouvait aussi s'appuyer sur une **augmentation exponentielle de la densité de transistors des ordinateurs, suivant la loi de Moore**<sup>(15)</sup> (cf. encadré). **Ces paradigmes trouvent aujourd'hui leurs limites, rendant nécessaire une rupture technologique.**

#### La loi de Moore :

En 1965, Gordon E. Moore (un des trois fondateurs d'Intel) énonçait ce que nous appelons maintenant la **loi de Moore**, à savoir que la densité des transistors (nombre de transistors par unité de surface) – dont découle la puissance de calcul des ordinateurs classiques - **pourrait doubler tous les deux ans.**

Cette prédiction s'est révélée étonnamment exacte, et ces dernières années, les finesses de gravure n'ont cessé de diminuer jusqu'à atteindre 10 nm, (1 nm=10<sup>-9</sup> m) en 2017. Cependant, ces progrès atteignent des limites physiques du fait que l'on approche les dimensions de l'atome, et un **palier est attendu pour l'horizon 2020-2022.**

C'est pourquoi la course aux technologies quantiques est maintenant lancée. Au plan des technologies, les capteurs quantiques, déjà considérés comme matures, voient leur gamme d'applications s'élargir et leur précision atteindre des sommets ; les grands industriels américains (IBM, Microsoft, Google), français (Atos) ou asiatique (Alibaba), s'intéressent au calcul quantique, que ce soit pour de nouveaux supports physiques d'information de type quantique ou pour la mise au point d'une algorithmie innovante utilisant les principes quantiques. Enfin, le calcul quantique pourrait avoir des effets collatéraux dans le domaine de la cryptographie et de la sécurisation des données, en remettant en cause les méthodes de chiffrement actuelles, qui doivent être renouvelées par précaution. Ces technologies d'avant-garde mobilisent des investissements massifs, aussi en recherche fondamentale. Même si des grands axes d'applications ont déjà été identifiés (calcul, communications), des avancées ou des découvertes imprévues peuvent découler de cet engouement récent pour ce sujet complexe et pour lequel différentes pistes sont explorées<sup>(16)</sup>.

Les développements informatiques engagés depuis le début des années 2000 constituent la **deuxième révolution quantique**, correspondant à « *un point d'inflexion, passant de la recherche fondamentale théorique à une phase d'ingénierie et de développement* », ce que confirment les acteurs économiques<sup>(17)</sup>.

## Des programmes d'investissement dans le monde entier

**Les gouvernements suivent ces développements et investissent massivement dans le marché** afin de conforter leur influence sur la scène internationale. Ainsi, en 2018, **l'Union Européenne** a prévu de consacrer un milliard d'euros sur 10 ans aux technologies quantiques, via un programme « *FET flagship* »<sup>(18)</sup>, qui fait suite au « *Quantum Manifesto* »<sup>(19)</sup> déposé auprès de la Commission Européenne en 2016 par 3 000 membres de la communauté scientifique. Les fonds proviennent du programme Horizon 2020 mais aussi de sources nationales. L'intérêt est tel que des pays hors Union Européenne ont aussi rejoint le programme<sup>(20)</sup>. Le programme, qui vise à inclure tous les aspects des technologies quantiques, se divise en **quatre domaines d'intérêt, appuyés sur une base commune de science fondamentale :**

- **le calcul quantique**, dont la puissance et la vitesse se trouveraient décuplées grâce au principe de superposition ;

- **la simulation quantique** pour reproduire de manière simplifiée les interactions quantiques entre atomes au sein de molécules ou de cristaux ;

- **les communications** pour échanger de l'information via des protocoles et des supports quantiques ultra-sécurisés ;

- **les capteurs quantiques** dont la précision est telle qu'elle permet des applications industrielles et en recherche fondamentale.

Les résultats du premier appel à projets du *flagship* ont été rendus publics fin octobre 2018 : parmi les vingt projets retenus, treize incluent des laboratoires rattachés au CNRS, deux avec participation d'Atos (Pasquans et Aqtion), et deux coordonnés par des organismes français, Sorbonne Université (projet PhoQuS) et Thales (projet ASTERIQS). La France se place parmi les cinq pays ayant eu les meilleurs taux de réussite<sup>(21)</sup>.

En complément de leur bon classement, certains pays, tels que **l'Allemagne** ou le **Royaume-Uni**, définissent des programmes nationaux de plusieurs centaines de millions d'euros<sup>(22)</sup> avec par exemple 650 M€ pour l'initiative allemande et plus de 500 M€ côté britannique. Une partie de ces plans nationaux vise à regrouper des acteurs académiques et des entreprises américaines.

Aux **Pays-Bas**, l'initiative *QuTech*<sup>(23)</sup>, centre de recherche pour le calcul et l'internet quantique situé sur le campus de *TU Delft (Technische Universiteit Delft)*, dispose d'environ 150 M€ sur dix ans, provenant de fonds publics mais aussi des partenariats industriels avec Intel et Microsoft.

En 2016, dans la course internationale, **la Chine** a établi la première ligne de communication quantique depuis le satellite géostationnaire Micius du programme QUESS (*Quantum Experiments at Space Scale*). Ce lancement s'inscrivait dans le plan

quinquennal 2015-2020 comme une priorité pour la Chine, qui prévoit d'utiliser ce satellite pour sécuriser ses communications aussi bien militaires que commerciales. Selon le physicien Jian-Wei Pan, à la tête du projet, la Chine prévoit de mettre au point « un réseau mondial de communications quantiques d'ici 2030 »<sup>(24)</sup>. Le programme quantique chinois s'intéresse aussi à l'informatique quantique et aux capteurs avec un nombre élevé de brevets déposés depuis 2015 et en augmentation constante depuis 2010. On estime, avec une forte imprécision, les budgets consacrés à ces deux axes à un milliard d'euros chacun.

#### Les lignes de communication quantique :

Les récents progrès permettent d'échanger de l'information entre deux utilisateurs distants en utilisant des photons intriqués.

Il est maintenant possible d'envoyer les paires intriquées dans deux fibres optiques partant dans des directions différentes afin d'établir une ligne de communication terrestre.

L'expérience chinoise QUESS a, elle, établi une ligne de communication dite satellitaire entre un satellite en orbite, émetteur de photons intriqués, et deux stations de réception au sol, séparées l'une de l'autre par 1 200 km.

Si les liaisons quantiques terrestres sont encore limitées à une centaine de kilomètres, les liaisons satellitaires ouvrent la voie à des échanges quantiques intercontinentaux et à plus grande échelle.

Aux **États-Unis**, si le secteur privé est déjà présent dans la course avec des investissements des géants des technologies (Google, IBM, Microsoft, Intel), la politique publique ne s'est mise en place que récemment. Ainsi le Congrès américain vient juste d'adopter, en décembre 2018, le *National Quantum Initiative Act*<sup>(25)</sup>: ce programme, étalé également sur 10 ans, débutera par un premier plan quinquennal de plus d'un milliard de dollars. Il s'agira **notamment de former rapidement des ingénieurs et des développeurs quantiques, encore peu nombreux face aux perspectives de forte croissance des besoins du secteur**. Le Royaume-Uni insiste également sur cet axe, en réservant près de 200 M€ de son programme national à des programmes de thèses en technologies quantiques et un peu moins de 15 M€ pour former de jeunes chercheurs<sup>(26)</sup>.

#### L'écosystème français

En France, depuis 2017, l'Agence nationale de la recherche (ANR) a instauré un Comité d'évaluation scientifique (CES 47) consacré aux technologies quantiques et doté d'environ 10 M€. À Grenoble, trois laboratoires (CEA-Leti, INAC et Institut Néel) se sont associés autour du projet QuCube afin de développer un processeur quantique à base de

silicium semiconducteur<sup>(27)</sup>. Leur projet a été lauréat d'un financement européen ERC *Synergy Grant*, et bénéficiera de 14 M€ sur 6 ans. La région Île-de-France a, elle, reconnu les technologies quantiques comme un « Domaine d'Intérêt Majeur » (DIM), et finance le projet SIRTEQ<sup>(28)</sup> doté d'environ 10 M€ sur 4 ans.

Quelques **initiatives privées se mettent en place en amont d'une initiative nationale d'envergure**, à l'instar du fonds Quantonation<sup>(29)</sup>, créée en septembre 2018. Celui-ci vise à lever un total de 40 M€ à investir en 4 ans afin de soutenir des start-up dès leurs débuts<sup>(30)</sup>. Atos, de son côté, a investi et commercialise sa QLM (Quantum Learning Machine), seule plateforme de simulation quantique du marché avec des clients aux États-Unis et en Europe. Par ailleurs, IBM a inauguré en décembre 2018 son septième pôle d'excellence mondial, dénommé IBM Q Hub et centré sur le calcul quantique à Montpellier<sup>(31)</sup>.

**Des efforts de transfert de technologie et de valorisation de la recherche se développent aussi dans la recherche française en physique quantique**. Ainsi, la start-up Muquans<sup>(32)</sup>, est spécialisée dans les gravimètres<sup>(33)</sup> quantiques et les horloges atomiques à très haute précision (dérive inférieure à 1 seconde sur 30 millions d'années). De même, la société Quandela<sup>(34)</sup>, issue du monde académique (CNRS et Université Paris Saclay), fabrique des sources de photons indiscernables<sup>(35)</sup> pouvant servir de support d'information à un ordinateur quantique dit « optique ».

#### Conclusions et perspectives

Avec l'engagement de la deuxième révolution quantique, les États comme les industriels de différents pays lancent des plans ambitieux pour anticiper les changements et les opportunités à venir. Ainsi que le montre le programme du *flagship* européen, et sans exclure l'identification d'éventuelles utilisations aujourd'hui inconnues, par sérendipité, cette révolution, d'importance stratégique pour la France et l'Europe, interviendra dans des domaines divers, à l'intersection entre la recherche fondamentale et l'ingénierie, qui feront l'objet de prochaines notes scientifiques, en particulier sur l'informatique et les ordinateurs quantiques, ainsi que sur la cryptographie quantique et post-quantique.

Sites Internet de l'OPECST :

<http://www.assemblee-nationale.fr/commissions/opecest-index.asp>

<http://www.senat.fr/opecest/>



---

## Experts consultés

---

M. Alain Aspect, physicien à l'Institut d'Optique, membre du Conseil scientifique de l'Office.

Mme Astrid Lambrecht, directrice de recherche au CNRS, directrice de l'Institut de physique du CNRS (INP/CNRS), membre du conseil scientifique de l'Office.

Mme Fanny Bouton, journaliste spécialisée dans les nouvelles technologies.

M. Antoine Browaeys, directeur de recherche à l'Institut d'Optique.

Mme Anne Canteaut, directrice de recherche à l'INRIA, groupe SECRET.

M. Philippe Chomaz, directeur scientifique exécutif de la Direction de la recherche fondamentale au CEA.

M. Thierry Debuisschert, ingénieur de recherche, Thalès.

M. Bruno Desruelle, PDG de la start-up Muquans.

Mme Eleni Diamanti, chargée de recherche au Laboratoire d'Informatique de Paris 6 (LIP6).

M. Philippe Duluc, directeur technique big data & security d'Atos.

M. Daniel Estève, directeur de recherche et chef du groupe Quantronique au CEA.

M. Olivier Ezratty, consultant spécialisé en nouvelles technologies et auteur du blog "Opinion libres".

M. Adrien Facon, chef de file du Programme RISQ, Directeur du groupe Innovation chez Secure IC.

M. Philippe Grangier, Directeur de Recherche CNRS et Responsable du Groupe Optique Quantique à l'Institut d'Optique.

M. Serge Haroche, professeur émérite au Collège de France, prix Nobel de physique 2012.

M. Christophe Jurczak, directeur général du fonds d'investissement Quantonation.

M. Anthony Leverrier, chargé de recherche à l'INRIA, dans le groupe SECRET.

M. Grégoire Ribordy, co-fondateur et PGD de la start-up ID Quantique.

Mme Pascale Senellart, directrice de recherche au Laboratoire de photonique et nanostructures (LPN) du CNRS. Co-fondatrice de la start-up Quandela.

M. Sébastien Tanzilli, Directeur de recherche et chargé de mission au CNRS sur les technologies quantiques.

M. Georges Uzelberger, AI/Advanced Analytics Solution chez IBM France.

M. Benoît Wintrebert, Conseiller en Innovation au Ministère des Armées.

Coordination scientifique de Mme Sarah Tigrine, conseillère scientifique (avec la participation de M. Gaëtan Douéneau).

Ouvrages de référence consultés :

- « Comprendre l'informatique quantique » O. Ezratty, novembre 2018 (e-book)

- Rapport des Académies américaines : National Academies of Sciences, Engineering, and Medicine. 2018. Quantum Computing : Progress and Prospects. The National Academies Press, Washington, DC. DOI : <https://doi.org/10.17226/25196>.

- « Clefs du CEA » N° 66- juin 2018 « révolutions quantiques »

Nota : en accord avec la déontologue de l'Assemblée nationale, Cédric Villani s'est mis en retrait de sa participation au Conseil scientifique d'ATOS – organe non décisionnel – pour la durée de ses travaux pour l'Office portant sur les technologies quantiques.

---

## Références

---

(1) Au singulier « quantum », qui vient du latin et qui signifie « combien ». En physique, désigne une quantité insécable (en énergie, en masse...).

(2) Heisenberg a été lauréat du Prix Nobel de physique 1932 pour sa contribution à la création de la mécanique quantique.

(3) Les horloges atomiques se basent sur la fréquence immuable de la transition entre les niveaux d'énergie du césium 133. Depuis 1967, cette fréquence sert aussi de référence pour fixer la seconde qui devient ainsi la durée au cours de laquelle 9 192 631 770 oscillations à la fréquence de cette transition ont lieu

(4) Pour comparaison, une montre à quartz classique dérive de 1 seconde par jour tandis que pour une horloge atomique la dérive est de 10 ns par jour (dix milliardièmes de seconde). Une désynchronisation de 1 seconde induit une erreur de position GPS de 300 000 km.

(5) Le mot "laser" est l'acronyme de "light amplification by stimulated emission of radiation". Le principe de base du laser repose sur la désexcitation d'un atome, stimulée par un apport d'énergie (lumineuse) correspondant à l'énergie de transition entre deux états électroniques. La mécanique quantique pose que ces niveaux sont discrets et parfaitement définis. Le photon émis par désexcitation s'ajoute au champ lumineux incident, ce qui crée le phénomène d'amplification.

(6) Richard Feynman, « *Simulating Physics with Computers* », International Journal of Theoretical Physics, vol. 21, nos 6–7, 1982, p. 467–488

(7) L'algorithme de Deutsch-Jozsa, qui sert à résoudre un problème de classification et qui n'a pas un grand intérêt pratique, constitue néanmoins le premier exemple d'algorithme quantique « utile » concrètement mis en œuvre.

(8) L'algorithme de Shor permet de factoriser un nombre, i.e. l'écrire comme un produit de nombres premiers (par exemple  $15 = 3 \times 5$ ), en un temps exponentiellement plus rapide que les algorithmes classiques. Si cet algorithme venait à être implémenté sur une machine quantique performante, les protocoles de chiffrement actuels, qui reposent sur la difficulté du problème de factorisation, seraient alors mis en échec très rapidement.

(9) Les expériences menées par Alain Aspect au début des années 1980 sont souvent appelées les « expériences EPR » car elles répondent au paradoxe d'Einstein-Podolsky-Rosen (EPR), publié en 1935. Elles concernent le phénomène d'intrication quantique, avancé théoriquement par Niels Bohr. Einstein et ses collègues pensaient que l'intrication violait les lois de la physique, et plus particulièrement de la localité, et que le formalisme de la mécanique quantique était incomplet. Le débat est resté sans réponse jusqu'en 1964, quand John Bell, théoricien au CERN à Genève, publia un théorème, connu sous le terme « d'inégalités de Bell », qui permet de vérifier ce concept par l'expérience. C'est ce que fera Alain Aspect en 1981 en violant les inégalités de Bell et en apportant une preuve irréfutable de l'intrication entre une paire de photons.

(10) À titre d'exemple, pour  $N=10$  bits quantiques, il existe alors  $2^{10}=1024$  états possibles simultanément et pour  $N=50$ , on atteint  $2^{50} \approx 10^{15}$  états superposés, soit un million de milliards.

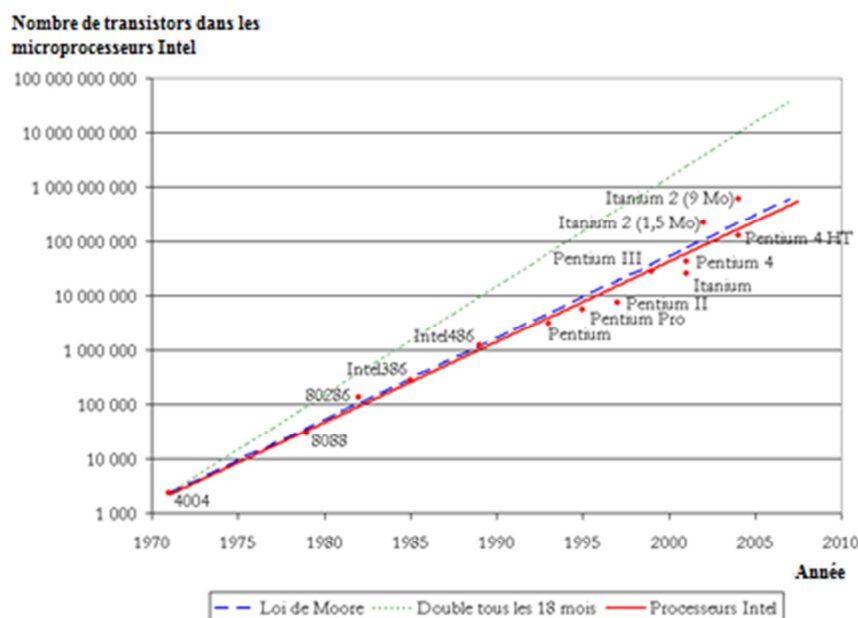
(11) Pour isoler un atome, deux techniques peuvent être mentionnées : le refroidissement (par hélium liquide à une température proche de  $-273$  K soit le zéro absolu) ou le piégeage de l'atome dans une matrice de cristal (principe des « centres NV », dans lesquels un atome d'azote N est piégé dans une matrice de diamant).

(12) Grâce à un champ magnétique puissant, produit par un aimant supraconducteur, les tissus humains sont magnétisés en alignant leurs spins magnétiques. Couplé à un champ magnétique moins intense et oscillant, les spins ont alors un mouvement de précession qui produit un signal électromagnétique mesurable. Réalisé pour la première fois sur des êtres humains dans les années 1970, le principe de l'IRM a valu à ses inventeurs, Paul Lauterbur et Peter Mansfield le prix Nobel de physiologie ou médecine en 2003.

(13) On estime que, d'ici 2020, 1,7 mégaoctet (Mo) de données seront créées par seconde et par personne. Ceci représente le poids d'un fichier au format compressé MP3 d'une chanson d'environ 2 minutes.

(14) Même si les États-Unis et l'Asie restent clairement les leaders sur le marché des supercalculateurs, la France, qui dispose de la machine BullSequana créée par ATOS et opérée par le CEA, se place au 16<sup>e</sup> rang mondial (données de novembre 2018). Sa consommation électrique, optimisée, s'élève à 4 MW ce qui correspond à la puissance maximale d'une éolienne offshore. La machine chinoise Taihulight, consomme elle 15 MW pour une facture énergétique de l'ordre de 22 millions d'euros par an (données 2017).

(15) Comparaison entre l'évolution réelle de la densité de transistors dans les processeurs informatiques (courbe rouge) et les prédictions de la loi de Moore depuis les années 1970 (courbe bleue, la courbe verte correspondant aux premières prévisions qui ont été réajustées depuis) :



Adapté de : Par Original téléversé par QcRef87 sur Wikipédia français. — Transféré de fr.wikipedia à Commons par Bloody-libu utilisant CommonsHelper., CC BY-SA 3.0, <https://commons.wikimedia.org/w/index.php?curid=16066564>

(16) À titre d'exemple, Microsoft mise sur le calcul quantique à base de « fermion de Majorana », approche dénommée « informatique quantique topologique » et décrite par l'équipe de Michael Freedman (lauréat de la médaille Fields 1986). L'existence de cette particule, qui serait sa propre antiparticule, a été proposée par le physicien E. Majorana, mais n'a encore jamais été détectée de manière certaine. Cependant, si elle venait à être découverte, elle permettrait de mettre au point l'ordinateur quantique le plus fiable et le plus performant du marché actuel. <https://experiences.microsoft.fr/technique/intelligence-artificielle-ia-technique/informatique-quantique-pari-fou/>

(17) <https://www.morganstanley.com/ideas/quantum-computing>

---

(18) FET : Technologies futures émergentes - <http://www.horizon2020.gouv.fr/cid123504/1er-appel-du-fet-flagship-sur-les-technologies-quantiques.html>

(19) [http://quope.eu/system/files/u7/93056\\_Quantum%20Manifesto\\_WEB.pdf](http://quope.eu/system/files/u7/93056_Quantum%20Manifesto_WEB.pdf)

(20) Turquie, Israël et Suisse.

(21) Avec, sans surprise, l'Allemagne, le Royaume Uni, l'Italie et l'Espagne.

<http://www.cnrs.fr/fr/premiers-laureats-pour-linitiative-europeenne-sur-les-technologies-quantiques>

(22)

Pays (UE)	Montant (millions d'euros)	Pays (Hors UE)	Montant (millions d'euros)
Allemagne	650	Chine	~2 000
Royaume Uni	450	États Unis	1 000
Pays Bas	150		

Plans nationaux de financement public des technologies quantiques en Europe et dans le monde

(23) <https://qutech.nl/>

(24) <https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-scientifique/veille-scientifique-et-technologique/chine/article/lancement-du-premier-satellite-a-communication-quantique-guess>

(25) <https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-scientifique/veille-scientifique-et-technologique/etats-unis/article/national-quantum-initiative-act-le-retour-des-etats-unis-dans-la-course-aux>

(26) <https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-scientifique/veille-scientifique-et-technologique/royaume-uni/article/financement-de-la-recherche-en-technologie-quantique>

(27) <http://www.cea.fr/presse/Pages/actualites-communiques/sciences-de-la-matiere/Un-ERC-Synergy-Grant-pour-la-recherche-grenobloise-sur-les-technologies-quantiques-.aspx>

(28) <http://www.sirteq.org>

(29) <https://www.quantonation.com/fr/>

(30) Quantonation a déjà réalisé des investissements en France en particulier dans LightOn et dans Pasqal, la toute première start-up nationale dédiée à la réalisation d'un ordinateur quantique, fondé sur la technologie d'excellence française du refroidissement d'atomes par laser.

(31) <https://www-03.ibm.com/press/fr/fr/pressrelease/54572.wss>. Ce projet ambitionne de fédérer un réseau d'entreprises, d'organisations publiques et d'acteurs de la recherche et de l'enseignement supérieur utilisant les ressources quantiques d'IBM disponibles dans le cloud.

(32) <https://www.muquans.com/>

(33) Un gravimètre est un instrument de mesure destiné à quantifier le champ de pesanteur terrestre.

(34) <http://quandela.com/>

(35) Des photons sont dits « indiscernables » quand ils sont considérés comme identiques à tout point de vue.