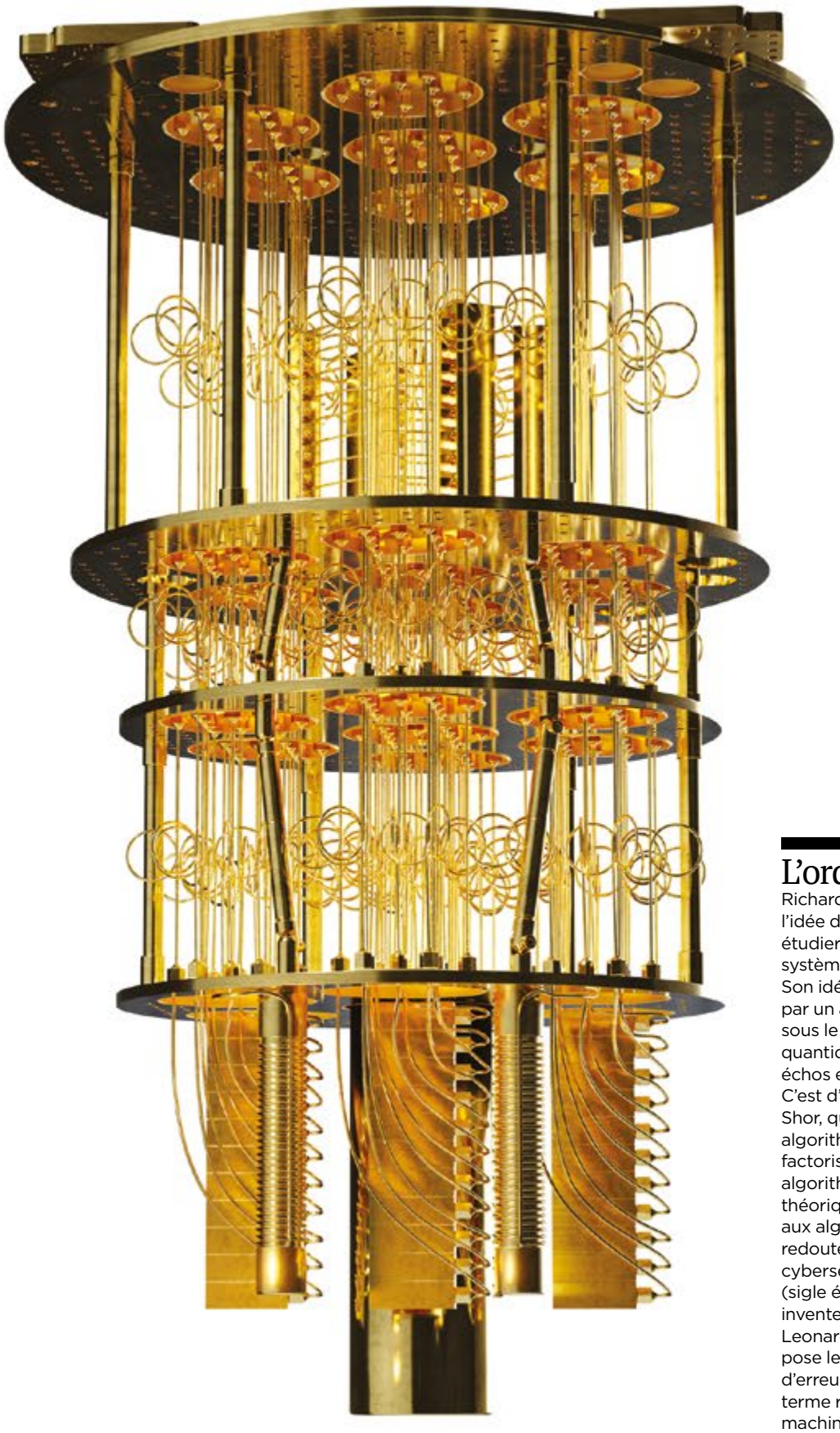

© DP

L'ordinateur quantique

Richard Feynman a suggéré en 1982 l'idée d'un « ordinateur quantique » pour étudier et prédire le comportement des systèmes régis par des lois quantiques. Son idée est formalisée trois ans plus tard par un autre physicien, David Deutsch, sous le nom de machine de Turing quantique. Le concept trouve vite des échos en mathématiques, par exemple. C'est d'ailleurs un mathématicien, Peter Shor, qui invente l'un des premiers algorithmes quantiques, permettant la factorisation en nombres premiers. Cet algorithme permet une accélération théoriquement exponentielle par rapport aux algorithmes classiques, faisant redouter des failles pour les systèmes de cybersécurité utilisant le cryptage RSA (sigle établi à partir des noms de ses trois inventeurs Ronald Rivest, Adi Shamir et Leonard Adleman). C'est aussi Shor qui pose les bases des codes correcteurs d'erreur, dont on pense qu'ils pourront à terme réaliser le plein potentiel des machines quantiques.

DES INGÉNIEURS QUANTIQUES À L'X : UN DÉFI PLURIDISCIPLINAIRE

LANDRY BRETHEAU (X05)
professeur à l'École polytechnique, chercheur en physique quantique au sein du Laboratoire de physique de la matière condensée (PMC)

THOMAS AYRAL (X07)
ingénieur-chercheur quantique (Atos Quantum Laboratory) & chargé de cours à temps partiel au département de physique de l'École polytechnique

La seconde révolution quantique, avec l'ordinateur quantique, permet d'envisager des usages nouveaux et prometteurs de ces nouvelles technologies. Mais, pour inventer les nouvelles techniques et imaginer les nouveaux usages, il faut des ingénieurs dotés de qualités originales. L'X est à cet égard bien placée pour jouer un rôle central dans la réponse à ce défi.

Quand on pense à la mécanique quantique, on songe souvent au chat de Schrödinger – à la fois mort et vivant. Mais aujourd'hui c'est à un autre « en même temps » qu'est confronté le domaine des technologies quantiques. Car depuis quelques années la physique quantique, grâce à l'avènement des premiers processeurs quantiques, a dépassé le domaine purement fondamental et académique. Elle intéresse désormais des domaines aussi divers que la chimie, la science des matériaux, l'informatique théorique et appliquée, les mathématiques – fondamentales et appliquées, l'optimisation, le calcul haute performance, la biologie, mais aussi le monde plus large de l'innovation. « L'ingénieur quantique » de demain devra donc savoir faire ce grand écart disciplinaire.

Un grand écart disciplinaire

Cette pluridisciplinarité est loin d'être nouvelle. La « première révolution quantique », qui utilise les effets statistiques de la mécanique quantique, a permis la création du transistor, du laser, de l'horloge atomique – utilisés dans des applications aussi variées que les ordinateurs classiques, les télécommunications, le système GPS ou Galileo. Quant à la « deuxième révolution quantique », celle qui utilise l'intrication entre les états quantiques individuels, elle est en gestation depuis les années quatre-vingt. Avec des démonstrations expérimentales – l'expérience d'Alain Aspect à l'Institut d'optique, par exemple – mais aussi avec des propositions théoriques, comme celle de Richard Feynman qui a suggéré en 1982 l'idée d'un « ordinateur quantique ». C'est la construction de prototypes expérimentaux d'ordinateur quantique qui attire aujourd'hui les autres disciplines vers l'informatique quantique. Dès la fin des années 90, de premiers qubits sont construits, avec des résultats précurseurs au CEA Saclay dans le groupe de Daniel Esteve et Michel Devoret. Environ vingt ans plus tard, en 2019, Google annonce à grand bruit avoir →

→ atteint la suprématie quantique avec un processeur composé de 53 qubits supraconducteurs. Google aurait ainsi exécuté, en 200 secondes, une tâche algorithmique qu'il aurait fallu 10 000 ans au meilleur ordinateur classique pour résoudre. Parallèlement, le géant du calcul haute performance IBM propose depuis 2016 des processeurs quantiques en libre-service sur le *cloud*.

La difficile quête d'une première application utile

Ces progrès expérimentaux ont lancé la quête de la première application utile de l'informatique quantique – celle qu'on appelle outre-Atlantique la *killer app*. Chaque domaine y va de son algorithme : la chimie quantique pour le calcul de taux de réaction, la science des matériaux pour la prédiction des transitions de phase, l'optimisation pour la résolution de problèmes combinatoires, la mécanique des fluides pour la résolution d'équations différentielles, la finance pour la prédiction de processus stochastiques, etc. Pour chacun de ces domaines, la traduction des équations à résoudre en programme quantique est loin d'être évidente : les règles de programmation à suivre sont bien différentes des règles des ordinateurs classiques, et ce pour des raisons fondamentales de physique. Il est par exemple impossible de copier des données, en raison du fameux théorème de non-clonage quantique. Il faut aussi affronter les subtilités liées aux propriétés de la mesure quantique, qui modifie l'état du qubit au moment où elle le mesure. Enfin, à cette difficulté intrinsèque vient s'ajouter le fait qu'il faut savoir mélanger (ou hybrider) des codes de calcul classique existants à des programmes quantiques. On utiliserait ainsi l'ordinateur quantique comme un coprocesseur (un *Quantum Processing Unit* – QPU – en somme), de la même façon que les cartes graphiques (GPU) sont aujourd'hui au cœur des progrès de l'intelligence artificielle et de l'apprentissage machine.

Des obstacles physiques

À toutes ces difficultés s'ajoute la réalité physique des processeurs quantiques. Si le modèle mathématique d'un processeur quantique prédit des accélérations algorithmiques (pourvu qu'on sache le programmer), la réalité physique se révèle plus ardue. Bien qu'ils soient censés être à la fois dans l'état 0 *et* dans l'état 1 (*i.e.* dans un état de superposition quantique), les qubits ont tendance, sous l'influence du monde extérieur, à repasser, après des temps relativement courts, à l'état 0 *ou* 1 – tout comme, en réalité, le chat de Schrödinger souvent cité. Ainsi, après quelques centaines d'opérations, l'ordinateur quantique redevient classique, perdant son avantage. Ces erreurs, dites de « décohérence », sont en constante diminution au cours des dernières années grâce aux progrès du *hardware*… Néanmoins, elles ne permettent pas encore de résoudre des problèmes utiles plus vite ou mieux que nos ordinateurs classiques actuels : les calculs réalisés en chimie, par exemple, se limitent à de petites molécules, les plus grosses molécules entraînant des erreurs qui ne permettent pas d'atteindre la précision nécessaire au calcul de taux de réaction. Les solutions à ces problèmes de décohérence sont multiples et multidisciplinaires : solutions, comme évoqué, au niveau du *hardware*, avec l'amélioration continue des machines ou la conception de nouveaux types de qubits ; solutions au niveau du *software*, avec l'invention d'algorithmes résistant au bruit, ou bien de techniques dites de mitigation d'erreur.

Un écosystème complexe

Cette quête semée d'embûches est poursuivie, au-delà du monde académique, par de grands groupes industriels (Google, IBM, Intel, Amazon aux États-Unis, Alibaba en Chine, mais aussi Atos en Europe) aussi bien que par des start-up – le plus souvent issues du monde académique. Pour ne citer que quelques jeunes pousses françaises spécialisées dans le *hardware* quantique : Pasqal et ses atomes de Rydberg, Quandela et ses processeurs photoniques, Alice&Bob et ses « qubits de chat », C12 et ses processeurs sur nanotubes de carbone. Tous ces acteurs – chercheurs, industriels, start-up – redoublent d'efforts pour communiquer, de façon plus ou moins étayée, sur les vertus de leur technologie. Les enjeux sont de taille, avec des « plans quantiques » nationaux (États-Unis, Chine, France, Allemagne…) et supra-nationaux (Union européenne) et des financements privés (investisseurs) substantiels. Il est ainsi difficile de faire la part entre la vraie avancée scientifique et technologique et l'annonce publicitaire. Par exemple, l'annonce par Google de la suprématie quantique a été remise en question par de nombreuses publications depuis 2019 – chaque contre-exemple nécessitant un effort de recherche conséquent.

Le besoin d'ingénieurs quantiques

Cet écosystème quantique a donc un besoin croissant d'ingénieurs quantiques bien formés : d'ingénieurs et

d'ingénieurs-chercheurs qui puissent se saisir des différents enjeux – scientifiques, technologiques, voire politiques – pour décider des pistes prometteuses. Or une telle denrée est rare sur le marché du travail. Non pas parce que les différentes disciplines ne sont pas enseignées, mais parce que peu de programmes universitaires proposent de les mélanger avec une exigence forte dans chacune des sous-disciplines. Non seulement faut-il être formé aux fondamentaux de la mécanique quantique, mais il faut aussi comprendre les subtilités de la programmation quantique et son hybridation avec le calcul classique – ce qui nécessite une bonne connaissance de l'informatique classique. En plus de cela, la compréhension des domaines d'application – chimie, physique, mathématiques, optimisation… – est cruciale pour juger de la pertinence de tel ou tel algorithme quantique. Comme évoqué plus haut, difficile de déchiffrer une publication scientifique ou une annonce sans en connaître en détail le domaine, ou même refaire un calcul ! Car, pour juger de la pertinence d'un algorithme, il faut non seulement le comprendre mais aussi pouvoir le comparer aux solutions algorithmiques classiques existantes. Enfin, et surtout, des ingénieurs sont nécessaires pour mettre au point de nouveaux algorithmes qui puissent dépasser les performances des algorithmes classiques – que ce soit du point de vue de la vitesse ou du point de vue des performances énergétiques.

Une offre de formation en expansion

L'offre de formations quantiques est encore balbutiante, mais en pleine expansion. L'École polytechnique fait bien sûr référence en matière d'enseignement de la mécanique quantique, et ce depuis des décennies, avec notamment un cours de tronc commun marqué par des professeurs de renom comme Jean-Louis Basdevant, Jean Dalibard, Philippe Grangier ou Manuel Joffre. Mais c'est plutôt au niveau master que l'offre en « ingénierie quantique » se développe, avec la création de nombreux programmes de niveaux master et doctorat dans les quelques dernières années. Pour ne citer que quelques programmes franciliens : un master de *Quantum Engineering* à l'université Paris Sciences & Lettres, un master de *Quantum Technologies* à l'université Paris-Cité, le programme ARTeQ (année de recherche en technologies quantiques) coporté par l'ENS Paris-Saclay et l'Institut Polytechnique de Paris (IPP).

> *"La demande en ingénieurs quantiques généralistes va croître."*

La place de l'X dans cette offre

À l'IPP, par ailleurs, un parcours « sciences et technologies quantiques » a été mis en place en troisième année du cycle polytechnicien, complétant la formation à la physique quantique prodiguée en première et en deuxième année, ainsi que les cours dispensés dans les autres matières : mathématiques, mathématiques appliquées, informatique, biologie. Dans ce parcours Sciences et Technologies Quantiques, proposé par le département de physique de l'École polytechnique, la formation sur les technologies quantiques associe cours théoriques sur les technologies quantiques actuelles et le formalisme permettant de les modéliser, et étude critique de publications scientifiques sur le sujet. L'accent y est entre autres mis sur la pratique concrète de l'informatique quantique, avec des travaux pratiques de programmation quantique sur *notebooks* Jupyter. D'autres départements de l'École polytechnique contribuent à cette formation, avec des modules de cours dispensés par le département de mathématiques appliquées (contrôle quantique) et d'informatique. Enfin, un PhD Track *Quantum Science & Technologies* permet aux étudiants de poursuivre leur formation par un doctorat – une formation par la recherche essentielle dans un domaine où l'innovation provient en grande partie de la recherche, y compris dans les grandes entreprises telles que Google ou IBM, qui restent très proches des milieux académiques.

Cette offre, que ce soit à l'IPP ou dans d'autres cursus, est appelée à s'étoffer et à gagner en multidisciplinarité. Avec la multiplication des moyens de calcul quantiques et des défis algorithmiques pour les faire fonctionner de façon fiable et viable, la demande en ingénieurs quantiques généralistes, formés à tous ces sous-domaines, va croître.