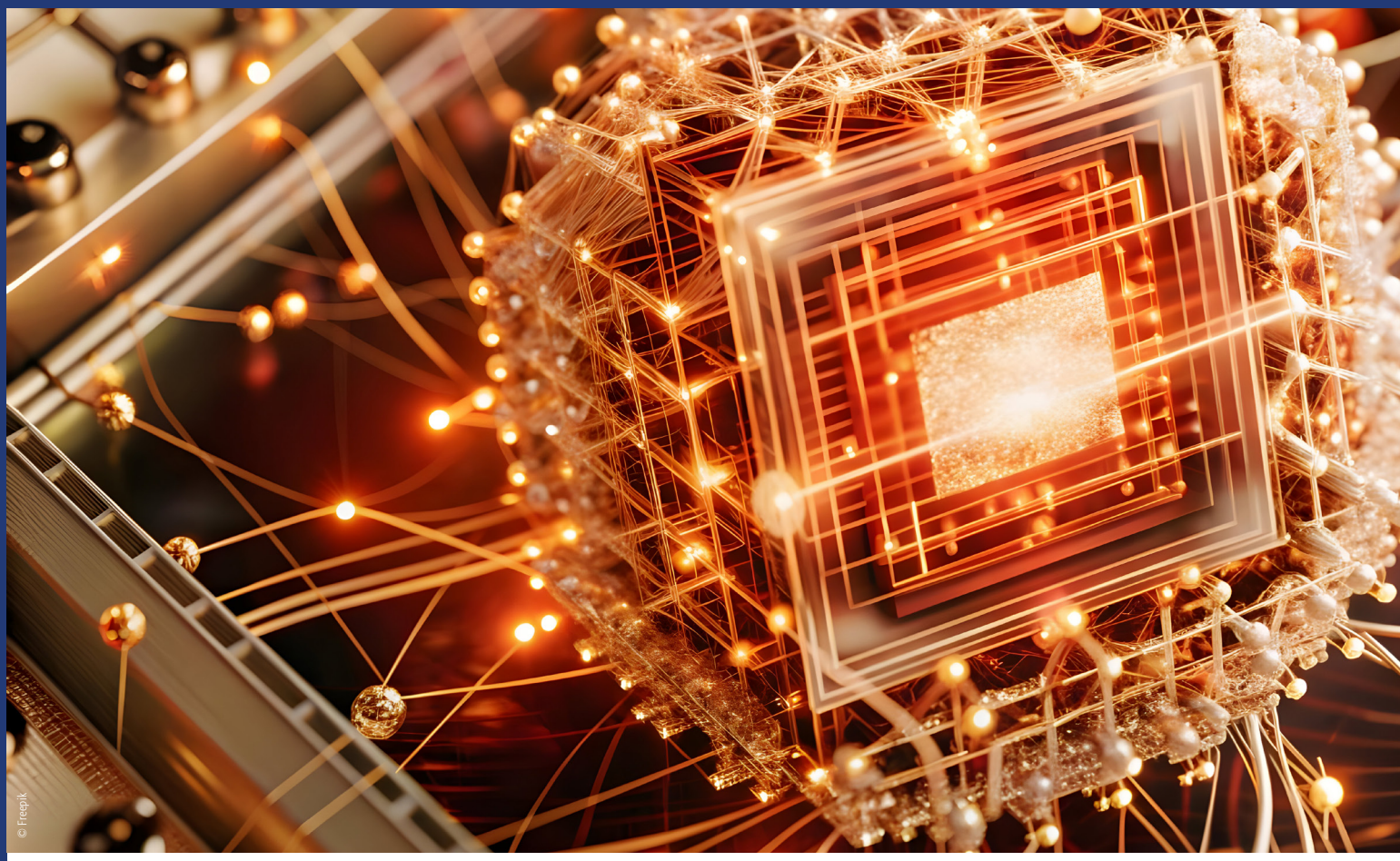


Introduction

Les bits classiques deviennent quantiques. Pourquoi faire ?

Oubliez les bits 0 et 1 : l'ère du bit quantique (le qubit) a sonné. 100 ans après la première révolution quantique, la seconde déverrouille des capacités de calcul inédites, pour certains problèmes complexes. Calculs super-polynomiaux, communications inviolables, détections de signaux plus précises : bienvenue dans le monde fascinant de l'Information quantique !

Fabrice Dupuy
Auteur de l'ouvrage 'Internet Quantique'

Introduction

Information quantique ? Quésaco, aurait-on envie de demander ? L'information quantique (parfois abrégée en QIS pour *Quantum Information Science*) est un domaine interdisciplinaire qui exploite les principes de la théorie quantique pour effectuer des tâches de traitement, de stockage et de transmission d'éléments quantiques d'information ou qubits.

Qubit ? KES ? Explication !

Au lieu d'utiliser des éléments d'information binaires, c'est-à-dire des bits classiques qui peuvent être soit des 0 soit des 1, l'information quantique utilise des éléments binaires quantiques ou qubits, qui seront eux dans l'un des états quantiques de base |0> ou |1>, ou dans une superposition des deux !

Avoir un bit classique d'information (noté c pour classique) sur un système ou un objet, c'est connaître l'état, soit 0, soit 1, dans lequel ce dernier se trouve. La pièce de monnaie est retombée sur *pile* (le bit c prend la valeur 1) ou sur *face* (c = 0); un chat normal est *vivant* (c = 1) ou *mort*

(c = 0). Tout Internet est basé sur ce principe d'encodage des mots, des chiffres, des échantillons de voix ou de vidéo en bits classiques pour leur transport entre expéditeurs et destinataires. Sur les réseaux, ne circulent que des 0 et des 1…

Dans le cadre de cette nouvelle science, avoir un bit quantique d'information (noté q comme quantum bit ou qubit) à propos du même objet, c'est modéliser le fait que l'objet puisse être dans une superposition d'états, jusqu'à ce que l'on effectue la mesure d'une propriété observable de cet objet. Avant la mesure (par exemple l'observation de la pièce retombée sur une surface plate), l'état quantique de la pièce est une superposition complexe des états |pile> = |1> et |face> = |0>. Avant l'ouverture de la boîte imaginée par Erwin Schrödinger, son chat est dans une superposition d'états |mort> = |0> et |vivant> = |1>. Toute l'information sur l'état du système quantique est contenue dans sa fonction d'onde : |Ψ>pièce ou |Ψ>chat.

A quoi ça sert, puisque de toute façon, à notre échelle, la pièce est retombée soit sur son côté pile, soit sur son côté face, et le chat de Schrödinger dans sa boîte est soit vivant, soit mort, mais pas dans une superposition de mort-vivant ?

La science de l'information quantique (QIS) devrait permettre de dépasser les limites des ordinateurs classiques dans la simulation des systèmes quantiques, par exemple. Dans une conférence marquante en 1981 intitulée «*Simulating Physics with Computers*», Richard Feynman soulignait ces limitations intrinsèques ; il fit valoir que la complexité du calcul nécessaire pour simuler un système quantique croît exponentiellement avec la taille du système, rendant la simulation classique impossible pour des systèmes même modestes. L'idée lui vint de la simulation quantique : construire un ordinateur qui fonctionne lui-même selon les principes de la physique quantique. Un tel simulateur quantique serait intrinsèquement capable de manipuler les états quantiques et d'imiter le comportement des systèmes quantiques avec une efficacité bien supérieure à celle des ordinateurs classiques.

Par exemple, l'ordinateur quantique pourra simuler le comportement des électrons dans les matériaux pour comprendre les mécanismes de la supraconductivité à haute température, ce qui pourrait révolutionner le transport d'énergie sans perte ; il pourra nous aider à comprendre les processus d'absorption de la lumière et de transport d'énergie dans les matériaux pour développer des cellules solaires plus performantes. La simulation quantique concernera aussi les interactions entre des molécules d'un médicament potentiel et des cibles biologiques (comme des protéines) afin de prédire leur efficacité et leurs effets secondaires, accélérant ainsi le processus de découverte de médicaments.

A l'échelle des atomes, des molécules, notre univers est probablement un gigantesque processeur d'informations quantiques. Dans ce cadre, l'information quantique peut être considérée comme le concept physique qui capture le mieux la nature de l'univers, à savoir ses changements, les traitements qui y ont lieu, les relations ou corrélations entre ses sous-systèmes. L'information quantique fournira une bien meilleure vision relationnelle des entités, des systèmes, des phénomènes et des événements (du moins à l'échelle de l'infiniment petit).

Un large éventail de domaines applicatifs

Ainsi la science de l'information quantique (QIS) englobe un large éventail de domaines de recherche et de développement, notamment :

• **le calcul quantique (Quantum Computing) ou l'informatique quantique** consistant à développer des ordinateurs quantiques capables de résoudre certains problèmes beaucoup plus rapidement que les ordinateurs classiques, en exploitant la superposition et l'intrication ; les applications potentielles incluent la découverte de médicaments, la science des matériaux, l'optimisation complexe et l'intelligence artificielle ;

• **les communications quantiques (Quantum Communications)** ou l'utilisation des propriétés quantiques pour transmettre des informations de manière sécurisée ; la **cryptographie quantique** promet des systèmes de communication théoriquement inviolables ; la **téléportation quantique** permet de transférer l'état quantique d'un qubit à un autre ;

• **la détection quantique (Quantum Sensing)** ou le développement de capteurs ultra-sensibles basés sur les principes quantiques pour des mesures de haute précision dans des domaines tels que la physique, la biologie et la médecine ;

• **la simulation quantique (Quantum Simulation)** utilisant des systèmes quantiques contrôlables pour simuler d'autres systèmes quantiques complexes, ce qui est bien plus difficile avec les ordinateurs classiques ; l'apport est crucial pour la recherche en chimie, en science des matériaux et en physique fondamentale.

> **" Les ordinateurs quantiques à petite échelle (de 50 à 1 000 qubits), déjà disponibles dans des 'clouds' permettent de réaliser des expériences et de tester des algorithmes, mais ils restent bruyants et ne surpassent pas encore les machines classiques dans les applications réelles."**

Au sein de cette science, le calcul quantique (ou l'informatique quantique) consistera donc à coder l'information quantique en qubits sur lesquels les ordinateurs quantiques pourront effectuer des opérations de calcul : par exemple l'algorithme quantique conçu par Peter Shor en 1994, qui factorise un entier naturel N (non premier) de façon polynomiale et non plus sub-exponentielle. Quant à la cryptographie quantique, elle consistera à encoder les n bits d'une clé secrète en qubits et à les distribuer de façon plus sécurisée. Enfin, les capteurs quantiques seront des appareils utilisant les principes de la physique quantique pour mesurer des grandeurs physiques (durée, valeur d'un champ magnétique, masse, etc.) avec une précision bien supérieure à celle des capteurs classiques ; ces capteurs exploiteront des phénomènes comme la superposition et l'intrication quantique pour améliorer la sensibilité et la précision des mesures. On les utilisera notamment en médecine, en navigation, en géophysique et en détection de matières.

Pour bien préciser les choses : si la physique quantique consistait à obtenir de l'information sur les états et le comportement de tel ou tel système physique, tel ou tel objet d'une expérimentation, la science de l'information quantique consiste à faire porter de l'information quantique et sa surprenante logique algorithmique sur de tels systèmes physiques (des capteurs, des ordinateurs quantiques). L'objectif étant de simuler l'infiniment petit (les électrons d'un matériau supraconducteur, les molécules d'un nouveau médicament, les liquides de spin quantique, les condensats de Bose-Einstein) ou de bénéficier d'une algorithmie non classique.

Dans ce dossier

Les technologies quantiques suscitent donc un intérêt considérable, mais parfois encore excessif. Entre promesses audacieuses et réel progrès technologique, il est important d'essayer d'y voir clair. Ce qui est réel aujourd'hui, en octobre 2025, ce sont les ordinateurs quantiques à petite échelle (de 50 à 1 000 qubits), déjà disponibles dans des 'clouds' ; ils permettent de réaliser des expériences et de tester des algorithmes, mais ils restent bruyants et ne surpassent pas encore les machines classiques dans les applications réelles. L'article suivant questionnera ce que pourrait être une suprématie quantique.

Ce qui est réel aussi est la distribution quantique de clés (QKD), avec des projets pilotes dans les réseaux de télécommunications et via les satellites, utilisant l'intrication de photons pour échanger des clés de chiffrement avec une sécurité basée sur la physique. **Yannick Gautier** et **Sylvain Chenard** aborderont la cybersécurité et l'apport du quantique dans l'article 'Du risque quantique à l'atout défensif : le réseau au cœur de la cybersécurité'.

Ce qui est réel concerne les capteurs quantiques déjà en laboratoire et en phase de tests industriels préliminaires. Ils permettront des imageries par résonance magnétique ultra-précises, détecteront les structures souterraines par gravimétrie et prendront en charge la navigation sans GPS, grâce à des interféromètres atomiques. Dans ce qui suit, **Myriam Nouvel** poursuit avec un point d'avancement sur le développement des capteurs quantiques, 'lorsque la technologie est au service de notre quotidien'.

Dans une synthèse du rapport de l'académie des technologies, **Olivier Ezratty** présente 'les défis de la création d'ordinateurs tolérants aux fautes', avec leurs millions de qubits et leurs codes de correction d'erreurs.

Enfin, vu l'hétérogénéité matérielle (hardware) des ordinateurs quantiques, **Frédéric Barbaresco**, **Félicien Schopfer** et **Emmanuelle Vergnaud** présentent l'objectif d'un projet visant l'obtention d'un classement mondial des performances des calculateurs quantiques agnostiques aux technologies matérielles : le projet BACQ (Benchmarks Applicatifs des Calculateurs Quantiques) du programme national du Laboratoire national d'essais (LNE).

Bonne lecture, bonne découverte ! ■

Les articles

Le calcul quantique et sa suprématie tant attendue p.35
Du risque quantique à l'atout défensif p.39
Les capteurs quantiques p.47
Les défis de la création d'ordinateurs tolérants aux fautes p.55
Vers un classement mondial des performances des calculateurs quantiques agnostiques aux technologies matérielles p.61

Le calcul quantique et sa suprématie tant attendue

Fabrice Dupuy

Orange

Avec les ordinateurs quantiques bruyants à échelle intermédiaire (NISQ) d'aujourd'hui, et les ordinateurs quantiques tolérants aux pannes (FTQC) de demain, quels types de calcul quantique seront possibles ? Démontrent-ils déjà l'existence d'une suprématie quantique ?

Introduction

Dans son cours au Collège de France, Serge Haroche expliquait qu' « *un calcul quantique est un dispositif idéal qui permet de réaliser des opérations unitaires agissant sur les qubits suivant les lois quantiques. Le caractère unitaire des opérations assure leur réversibilité.* »

Effectuer un calcul quantique sur des qubits signifie appliquer une succession d'opérations fidèles aux lois quantiques. Il s'agit d'être capable de simuler la nature et donc ses opérateurs hamiltoniens. Ainsi, effectuer un calcul quantique, c'est appliquer, sur un 1 ou plusieurs qubits, une série d'opérations d'algèbre linéaire devant respecter quelques règles de transformation linéaire.

La section suivante abordera la façon dont un tel calcul se programme : le modèle des algorithmes quantiques s'appuyant sur des portes universelles, ou le modèle adiabatique. Puis nous présenterons les avancées concrètes de 2025, dans le domaine. Enfin nous nous poserons la question de la suprématie quantique, souvent annoncée, tant attendue.

Les modèles de calcul quantique

Les opérations effectuées par le calcul quantique répondent à au moins trois grands paradigmes de calcul.

• Soit elles correspondent à des opérations logiques sur les qubits et seront alors implémentées par des portes quantiques, des opérations unitaires qui modifient l'état des qubits de manière réversible. Des exemples de portes quantiques sont la porte Hadamard (H), la porte Pauli-X (équivalent du NOT) ou la porte CNOT (contrôle ●●●

conditionnel) ; l'ensemble des portes implémentées forme un circuit quantique.

• Soit les opérations de l'algorithme implémentent une évolution lente du système quantique à travers un Hamiltonien qui encode le problème ; c'est le modèle adiabatique utilisé par des machines comme celles de D-Wave, surtout pour résoudre des problèmes d'optimisation combinatoire.

• Soit elles ne sont définies que par leurs entrées/sorties ; la fonction de calcul encodée est alors un oracle ; un oracle est un moyen d'estimer une fonction finie, sans exposer sa logique. C'est comme une boîte noire permettant l'estimation d'une fonction quantique non exposée. Un exemple est l'oracle de Grover.

Il est dit parfois que le calcul quantique adiabatique est un calcul analogique, et que le calcul quantique à base de portes quantiques est un calcul digital.

Comment procède le concepteur d'un calcul quantique pour choisir parmi ces modèles ?

• Soit il cherche à concevoir et simuler un Hamiltonien, il basera alors davantage sa programmation sur un modèle adiabatique (un *quantum annealer* comme D-Wave) ou sur un processeur quantique universel variationnel (VQE, QAOA) ;

• soit son objectif est de simuler un système physique (comme des molécules ou des matériaux) en concevant son algorithme à base de circuits quantiques déjà documentés et d'oracles ;

• soit il cherche, comme l'ont fait Shor et Grover, à exploiter les propriétés quantiques de la superposition, de l'interférence, et de l'intrication pour tenter de résoudre un problème (celui de la factorisation d'un grand nombre entier dans le cas de Shor, ou celui de la recherche d'un élément répondant à un critère donné parmi des éléments non classés dans le cas de Grover).

" Tous ces modèles de calcul quantique universel (calcul adiabatique, circuit quantique, modèle topologique) sont équivalents à la machine de Turing quantique (MTQ) introduite par David Deutsch en 1985."

À première vue, l'algorithme quantique pour le problème de recherche d'un élément dans une base (l'algorithme de Grover), celui de la factorisation (c'est-à-dire l'algorithme de l'estimation de phase selon Shor) et la simulation hamiltonienne adiabatique ne semblent partager aucune structure commune. Et pourtant ils pourraient tous être dérivés d'une seule primitive algorithmique, et obtenus par un simple changement de paramètres ; c'est la théorie qu'ont démontrée des chercheurs [1] en 2021. Tous ces modèles de calcul quantique (calcul adiabatique, circuit quantique, modèle topologique) sont équivalents à la machine de Turing quantique (MTQ) [2] introduite par David Deutsch en 1985.

En pratique, la machine quantique universelle possédant suffisamment de ressources n'existant pas encore, le concepteur doit faire un choix entre l'un des modèles de calcul : quel calculateur quantique semble le plus simple à utiliser pour le problème posé ? De combien de qubits logiques a-t-il besoin et quel code de correction d'erreurs quantiques est à sa disposition ?

Quelles avancées en 2025 grâce au calcul quantique ?

Nous assistons en 2025 à des améliorations technologiques importantes pour le calcul quantique, celle permettant par exemple de rendre les codes correcteurs quantiques (ici les codes LDPC [3]) plus viables dans la pratique, ou celle permettant de mieux [4] gérer les erreurs conduisant à la perte de qubits logiques.

Par ailleurs le calcul quantique connaît, toujours en 2025, des avancées notables dans la résolution de problèmes d'optimisation, notamment grâce à des approches hybrides combinant algorithmes quantiques et méthodes classiques (pour des applications dans divers domaines comme la logistique, la finance et la gestion de projets).

Néanmoins, c'est dans les domaines applicatifs comme la recherche médicale, la chimie ou l'astrophysique que nous allons ici explorer ses percées.

Dans le domaine de la chimie, des chercheurs ont introduit de nouvelles techniques, telles que la 'factorisation tensorielle améliorée' et la 'compilation en volume actif', permettant une accélération significative des simulations de structures électroniques de molécules complexes. Ces méthodes ont été appliquées avec succès à des systèmes tels que le cytochrome P450, réduisant les temps de calcul de plusieurs ordres de grandeur.

En chimie encore, des chercheurs de Qubit Pharmaceuticals et de la Sorbonne (Jean-Philip Piquemal) ont développé des algorithmes quantiques basés sur des 'marches' quantiques (*quantum walks*) pour analyser des chaînes de Markov non réversibles. Ces méthodes permettent

1 John M. Martyn, Zane M. Rossi, Andrew K. Tan and Isaac L. Chuang, 'Grand Unification of Quantum Algorithms', Center for Theoretical Physics, Massachusetts Institute of Technology, 2021.

2 Généralisation de la machine de Turing universelle classique.

3 Contrôle de Parité de Faible Densité

4 A l'aide de nouvelles techniques de décodage et d'optimisations de circuits.

une accélération exponentielle, surpassant les gains quadratiques observés pour les chaînes réversibles, et ainsi rendent le calcul quantique plus accessible pour des applications pharmaceutiques concrètes, avec les technologies actuelles.

En conception de médicaments anticancéreux, une équipe internationale de chercheurs a développé un modèle hybride quantique-classique pour concevoir deux petites molécules ciblant la protéine KRAS [5], impliquée dans divers cancers. En combinant circuits quantiques et apprentissage automatique classique, ils ont pu filtrer des millions de composés, aboutissant à deux candidats prometteurs validés en laboratoire.

Concernant la simulation de systèmes biologiques, des chercheurs australiens ont remporté le prix Gordon Bell pour avoir réalisé la première simulation quantique précise de systèmes biologiques. Cette avancée permet de modéliser le comportement chimique et les propriétés physiques des atomes au fil du temps, offrant une précision comparable aux expériences physiques et promettant d'accélérer la découverte de médicaments.

Enfin, des physiciens de Caltech ont réussi à créer un état d'hyperintrication en manipulant simultanément les états électroniques et les mouvements de deux atomes à l'aide de pinces optiques. Cette avancée pourrait améliorer la capacité de stockage d'information quantique par atome et ouvrir de nouvelles perspectives en simulation quantique et en métrologie (pour la cosmologie par exemple).

Sont-ce là des exemples de la suprématie quantique tant commentée ? Mais existe-t-elle vraiment ?

La suprématie quantique existera-t-elle vraiment ? Quels défis reste-t-il ?

John Preskill a introduit l'expression « suprématie quantique » en 2012 pour désigner « *le moment où un ordinateur quantique pourra accomplir un calcul qu'un ordinateur classique ne peut pas réaliser en un temps raisonnable.* »

Si avérée, une suprématie quantique signifierait que même les meilleurs superordinateurs classiques ne pourront pas simuler ou reproduire le résultat donné par l'ordinateur quantique en un temps raisonnable. Même si la tâche à reproduire n'est pas nécessairement utile (elle peut être purement académique ou aléatoire), elle serait alors irréalisable classiquement à grande échelle. Par exemple, en 2019 le processeur Sycamore de Google a réalisé une tâche dite d'échantillonnage de circuits quantiques aléatoires ou RCS (*Random Circuit Sampling*), en quelques 200 secondes, alors qu'il est estimé que le meilleur supercalculateur aurait mis des milliers d'années.

Si avérée, l'accélération obtenue par l'ordinateur quantique serait alors super-polynomiale ; un algorithme quantique accélère '*super-polynomialement*' une tâche s'il résout un problème en un temps qui est une fonction polynomiale de n ($a_1 n^1 + a_2 n^2 + a_3 n^3 + \ldots$) alors que le temps d'un ordinateur classique sera de type exponentiel de n ou $n^k \log(n)^l$.

Il semble néanmoins que des accélérations super-polynomiales ne soient possibles que pour des problèmes ayant une structure spéciale bien adaptée au modèle de calcul quantique. John Preskill précise : « *Nous ne nous attendons pas à des accélérations super-polynomiales pour les pires instances des problèmes de la classe NP, tels que SAT ou le problème du voyageur de commerce. Pour ces problèmes sans structure évidente, nous ne pourrons peut-être pas faire mieux qu'une accélération quadratique de la recherche exhaustive d'une solution.* »

Par ailleurs, la supposée «suprématie» quantique pourrait n'être que temporaire, en fonction des progrès des algorithmes classiques. En fait, plutôt que de communiquer sur une éventuelle suprématie, il serait davantage utile d'approfondir deux questions :

1. Quels types de calcul quantique sont réalisables ?

2. Quels types de calcul quantique sont difficiles à simuler de manière classique ?

Il est possible que les ressources exponentielles extravagantes apparemment requises pour la description et la simulation classiques d'états quantiques génériques soient illusoires. Toujours John Preskill : « *Peut-être que les états quantiques réalisés dans la nature admettent réellement des descriptions classiques succinctes, soit parce que les lois de la physique qui régissent les systèmes quantiques complexes sont différentes de ce que nous pensons actuellement […], soit parce qu'il existe des moyens intelligents de simuler d'une manière classique qui nous ont échappé jusqu'à présent.* »

Avons-nous déjà des preuves convaincantes que la nature accomplit des tâches qui vont au-delà de ce qui peut être simulé efficacement par les ordinateurs classiques ? Par exemple, il existe de nombreuses questions mathématiques auxquelles nous ne pouvons pas répondre concernant les ma- ●●●

" Si avérée, une suprématie quantique signifierait que même les meilleurs superordinateurs classiques ne pourront pas simuler ou reproduire le résultat donné par l'ordinateur quantique en un temps raisonnable. "

5 Le gène KRAS produit une protéine qui transmet des messages à la cellule pour lui indiquer quand croître et se multiplier. La protéine agit comme un interrupteur « marche/arrêt » pour le signal.

tériaux fortement corrélés et les molécules complexes, et pourtant la nature fournit des réponses. « *Avons-nous échoué parce que ces problèmes sont intrinsèquement difficiles à résoudre de manière classique ou en raison de notre manque d'ingéniosité jusqu'à présent ?* » se demandait à nouveau John Preskill.

La notion de la suprématie quantique est loin d'être un sujet clos. Avec des algorithmes optimisés et suffisamment de puissance, un supercalculateur haute performance (HPC) pourra peut-être un jour calculer la solution de l'un de ces problèmes en un temps plus court qu'actuellement.

Conclusion

Suprématie avérée ou temporaire, toujours est-il que cette révolution quantique apportera des améliorations notables dans la recherche moléculaire, pharmaceutique et astrophysique. La conception d'un algorithme quantique s'approchera davantage du type de tâches que la nature ou le cosmos accomplissent sans discontinuer.

Pour autant, les défis à relever sont encore importants : grand nombre d'itérations et de longs temps de stabilisation pour les ordinateurs quantiques adiabatiques (ou analogiques) ; réduction exponentielle de la fidélité, codes correcteurs d'erreurs quantiques efficients pour les ordinateurs quantiques à portes universelles (ou discrets, numériques).

Concluons avec les mots de Thomas Ayral [6] : « *La question de savoir si, à court terme, le hardware quantique sans correction d'erreurs offrira un avantage quantique pour des applications de niche, ou si cet avantage ne sera obtenu que grâce à un hardware quantique avec correction d'erreurs et à des algorithmes quantiques plus traditionnels, très consommateurs de portes, reste ouverte. En fait, il est fort possible qu'une combinaison intelligente des deux paradigmes permette d'atteindre les objectifs des ordinateurs quantiques.* » ■

6 Thomas Ayral, 'Quantum computing : promises, achievements and challenges', Photoniques 131 (2025)

L'auteur

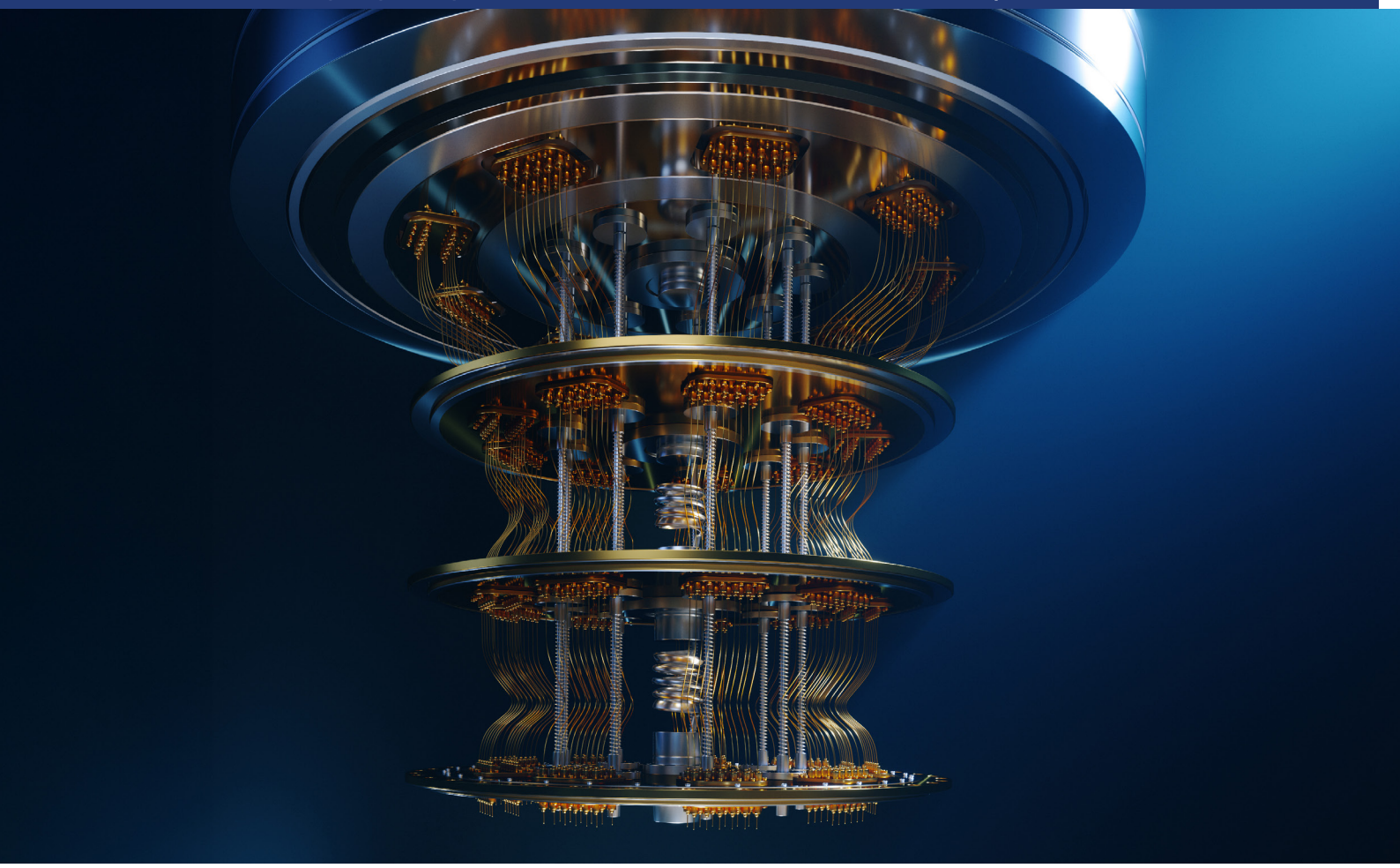
Fabrice Dupuy est polytechnicien, ingénieur du corps des télécoms/mines. Après avoir été directeur des systèmes d'information d'Orange Europe, en République du Congo et d'Orange France, il a conclu sa carrière chez l'opérateur de télécommunications comme doctorant dans le domaine de l'Internet Quantique. Il est aujourd'hui consultant, écrivain et membre du comité de rédaction de la REE.

Résumé

Le calcul quantique repose sur différentes façons de traiter l'information : en programmant des circuits composés de portes quantiques universelles, en utilisant des systèmes physiques évoluant progressivement vers l'état recherché ou des « boîtes noires » appelées oracles. Toutes ces approches visent à tirer parti des lois de la mécanique quantique pour résoudre certains problèmes plus vite qu'avec les ordinateurs classiques. En 2025, on observe des avancées concrètes : de meilleurs outils pour corriger les erreurs, des méthodes hybrides qui combinent quantique et classique, et surtout des résultats prometteurs dans la chimie et la pharmacie. On parvient par exemple à accélérer la simulation de molécules complexes, à explorer de nouvelles pistes pour concevoir des médicaments et à mieux comprendre certains systèmes biologiques. Mais la fameuse « suprématie quantique » reste un objectif encore flou : si des expériences ont montré des gains impressionnants, il est difficile de dire si ces avantages dureront face aux progrès constants des superordinateurs classiques. L'avenir du domaine semble donc se jouer dans la complémentarité : utiliser le calcul quantique là où il apporte vraiment un plus, en particulier dans des domaines comme la santé, la chimie ou la recherche fondamentale. ■

Abstract

Quantum computing relies on different ways of processing information : programming circuits composed of universal quantum gates, using physical systems that gradually evolve toward the desired state, or using "black boxes" called oracles. All these approaches aim to leverage the laws of quantum mechanics to solve certain problems faster than with classical computers. By 2025, we are seeing concrete advances: better tools for correcting errors, hybrid methods that combine quantum and classical computing, and, above all, promising results in chemistry and pharmacy. For example, we can accelerate the simulation of complex molecules, explore new avenues for drug design, and better understand certain biological systems. But the famous "quantum supremacy" remains an unclear goal: while experiments have shown impressive gains, it is difficult to say whether these advantages will last in the face of constant progress in classical supercomputers. The future of the field therefore seems to lie in complementarity: using quantum computing where it really provides a plus, particularly in areas such as health, chemistry or fundamental research. ■



Du risque quantique à l'atout défensif :

le réseau au cœur de la cybersécurité

Menacées par le calcul quantique, nos communications peuvent aujourd'hui compter sur les réseaux d'infrastructure (*Quantum Safe Networks*) pour les protéger et transformer le quantique en un allié d'une cybersécurité moderne.

Yannick Gautier
NOKIA
Sylvain Chenard
NOKIA

Introduction

Cet article traite de la sécurité quantique de réseau et présente une perspective polyvalente, adaptée aux différentes couches OSI. Cette approche repose principalement sur l'usage d'un chiffrement symétrique robuste, d'une distribution symétrique de clés, générées par un générateur d'entropie physique, classique ou quantique, et de son orchestration par une infrastructure certifiée de gestion des clés.

Nous explorons ici les différentes déclinaisons d'une telle solution, incluant la distribution manuelle des clés, la distribution automatique centralisée de clés générées à partir de sources de physique classique, la génération et l'échange de clés basé sur des liens quantiques, ainsi que la distribution de clés via des liaisons satellitaires quantiques. Dans ces modèles, les clés partagées et les politiques associées peuvent être créées et gérées de manière centralisée. Elles sont ensuite distribuées sur demande à des points de terminaison dûment authentifiés et autorisés. Cette approche garantit une administration sécurisée et efficace des clés, tout en offrant une protection renforcée contre les attaques potentielles des ordinateurs quantiques.

Effective key strenght/Security level			
Algorithm	**Key lenght**	**Conventional computing**	**Quantum computaing**
RSA-1024	1013 bits	80 bits	0 bits
RSA-2048	2048 bits	112 bits	0 bits
ECC-256	256 bits	128 bits	0 bits
ECC-384	384 bits	256 bits	0 bits
AES-128	128 bits	128 bits	64 bits
AES-256	256 bits	256 bits	128 bits

Tableau 1 : Résistance des algorithmes aux attaques quantiques.

Ce risque majeur qui fragilise nos communications sensibles

Les avancées en informatique quantique, en recherche fondamentale et dans les technologies industrielles et critiques promettent des possibilités considérables. D'ici peu, de nombreux acteurs auront accès, directement ou en ligne, à des calculateurs quantiques extrêmement puissants. Or, ces dispositifs représentent une menace importante pour la sécurité des communications : ils pourraient compromettre la confidentialité, l'intégrité et la disponibilité des données (CIA).

Un ordinateur quantique dit "pertinent en cryptographie" (CRQC) rendrait rapidement obsolètes les méthodes de chiffrement actuelles, avec des conséquences potentiellement catastrophiques pour les échanges sensibles. Couplée à l'intelligence artificielle, cette puissance de calcul rendra la cryptanalyse (décryptage illégitime des communications sécurisées) beaucoup plus efficace.

Face à cette menace désormais reconnue, entreprises stratégiques, agences de sécurité et pouvoirs publics prennent conscience de l'urgence à renforcer la résilience des communications et la protection des données.

En Europe, la directive NIS2, le Cyber Security Act et le règlement DORA encadrent cette évolution. NIS2 insiste sur l'usage du chiffrement pour une meilleure gestion des risques, tandis que DORA impose au secteur financier des mesures supplémentaires de résilience opérationnelle et de protection avancée, y compris contre le risque quantique. Ces réglementations se traduisent par des obligations concrètes : les entreprises devront s'assurer que leurs prestataires leur fournissent des solutions et services réseau capables d'accompagner cette transformation.

Les modèles de cryptographie et leur exposition au risque quantique

La plupart des algorithmes actuels ne pourront plus prévenir les conséquences d'intrusions lors d'attaques d'informatique quantique. Comme l'illustre le tableau 1, seuls deux d'entre eux pourraient maintenir une certaine protection.

Au-delà de la robustesse des clés, l'algorithme utilisé mais aussi le canal de communication pour la distribution des clés sont très importants.

Un échange sécurisé repose sur l'utilisation d'un algorithme de chiffrement robuste (ex. AES-256) et d'une clé partagée, suffisamment forte et de haute qualité, connue des deux parties pour chiffrer et déchiffrer les messages. Ce procédé, appelé chiffrement symétrique, suppose l'existence d'un mécanisme

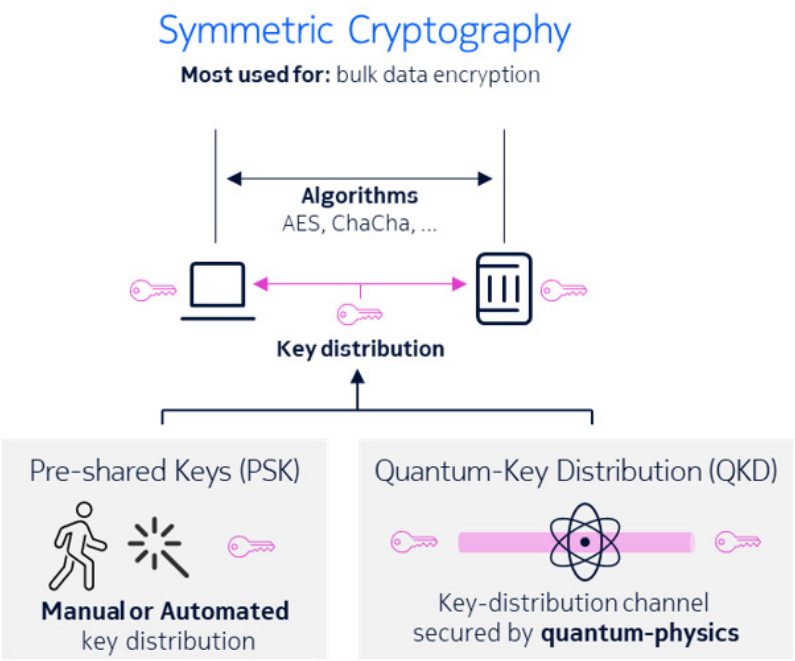


Figure 1 : Cryptographie symétrique.

fiable pour distribuer cette clé aux deux extrémités.

Selon le contexte, cette clé commune peut être obtenue de deux manières principales :

- Clés pré-partagées (*Pre-Shared Key* – PSK) : les clés sont configurées au préalable de manière sécurisée, ou bien distribuées via un mécanisme dédié. Cela peut aller d'une opération manuelle (par ex. un agent militaire installant les clés sur chaque point terminal) à des applications de distribution automatisées qui assurent leur livraison et leur renouvellement. Dans tous les cas, la qualité de la clé dépend de la fiabilité de sa génération : seules des sources d'aléa physique — générateurs de nombres aléatoires véritables (TRNG) ou quantiques (QRNG) — garantissent un niveau de sécurité durable.

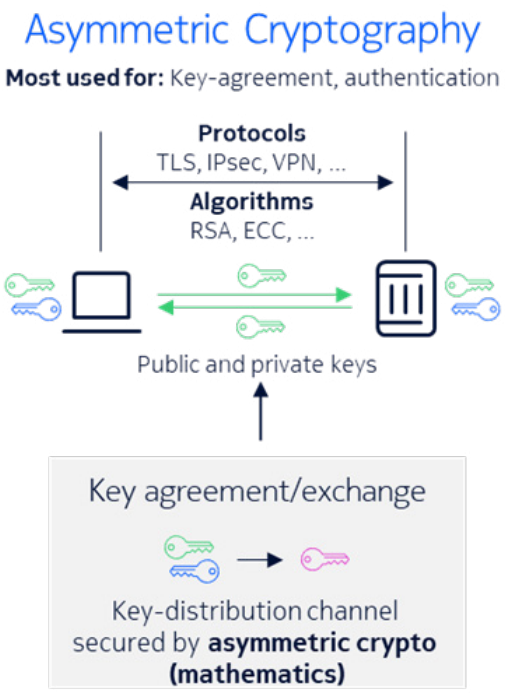


Figure 2 : Cryptographie asymétrique.

- Distribution de clés quantiques (*Quantum Key Distribution* – QKD) : cette approche repose sur l'utilisation de dispositifs quantiques capables d'exécuter des protocoles dédiés (tels que BB84 ou GG02) exploitant les lois fondamentales de la physique quantique. Mesurer un état quantique modifiant celui-ci (par ex. la polarisation d'un photon), toute tentative d'interception peut donc être détectée par les parties légitimes. Cette méthode, réputée extrêmement sécurisée, présente toutefois des contraintes : elle nécessite un canal authentifié préalable, ne tolère pas l'amplification optique classique, et reste limitée en portée faute de relais quantiques. De plus, elle est sensible aux perturbations (vibrations, bruit optique, atténuation), ce qui impose un étalonnage précis, une surveillance constante et souvent l'usage de fibres optiques dédiées.

Contrairement au chiffrement symétrique, c'est la cryptographie à clé publique (asymétrique) qui est aujourd'hui la plus répandue, en particulier au niveau applicatif. Elle constitue le mécanisme privilégié pour négocier une clé cryptographique commune entre plusieurs parties souhaitant échanger.

Ce mode ne nécessite ni accord préalable sur la gestion des clés, ni infrastructure ●●●

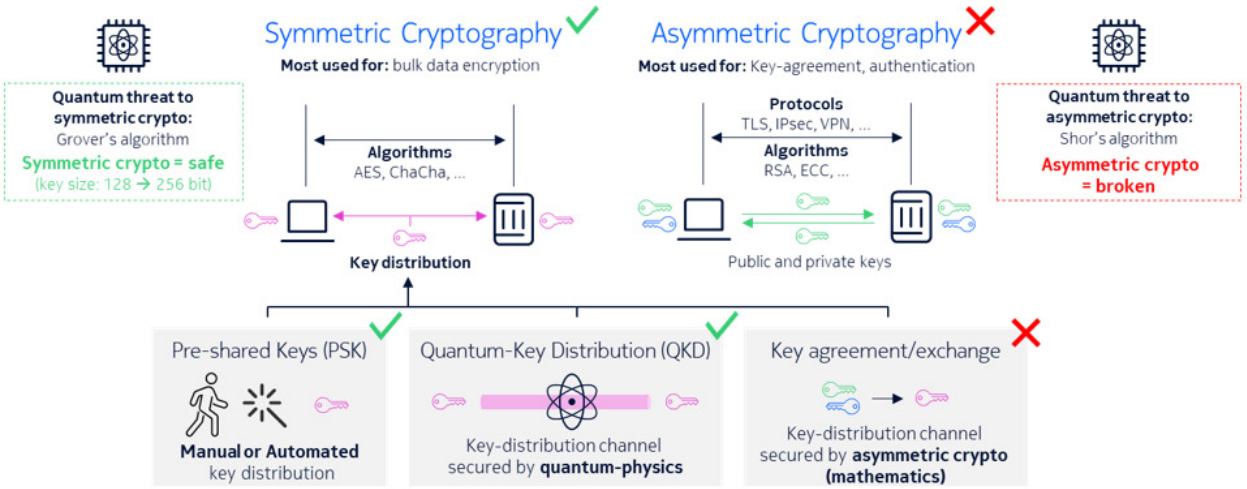


Figure 3 : Comparaison des cryptographies symétrique et asymétrique.

sécurisée de distribution, ce qui le rend particulièrement adapté aux connexions applicatives éphémères et aux échanges impliquant plus de deux participants.

Chaque participant génère alors une paire de clés : une clé publique, partagée avec les autres, et une clé privée, conservée secrète. Sur la base de problèmes mathématiques réputés difficiles (comme la factorisation de grands entiers ou le calcul de logarithmes discrets), les parties parviennent à établir une clé commune, ensuite utilisée pour chiffrer leurs communications.

Parmi les très rares algorithmes aujourd'hui capables de fonctionner sur un ordinateur quantique, deux présentent un impact majeur sur les fondements de notre sécurité numérique :

• L'algorithme de Lov Grover réduit de moitié la sécurité des clés symétriques, ce qui signifie que pour rester en sécurité, nous devrons doubler la taille des clés que beaucoup utilisent aujourd'hui (principalement passer de 128 à 256 bits).

• Plus pénalisant encore, l'algorithme de Peter Shor menace notre cryptographie asymétrique, avec une très forte probabilité de devenir exploitable dans 5 à 7 ans.

Ainsi, si les solutions symétriques restent sûre dans l'ère post-quantique, les solutions asymétriques devront elle être remplacées par une famille différente d'algorithmes dit post-quantiques. Notons que Shor et Grover étaient tous deux affiliés aux Bell Labs au moment où ils ont développé leurs algorithmes.

Quatre attributs majeurs sont en fait indispensables à un système de communication pour pouvoir résister à l'informatique quantique

- Les générateurs d'aléa basés sur des principes physiques - qu'ils soient classiques ou quantiques - produisent un bruit pur qui, par nature, ne converge jamais. Conformément à la deuxième loi de la thermodynamique, l'entropie, définie comme le degré de désordre d'un système, ne peut qu'augmenter ou rester constante. Les clés issues de cette entropie physique constituent ainsi une solution de sécurité fiable face aux menaces quantiques, à la fois présentes et futures.

- Longueur de clé appropriée : une clé de 256 bits est considérée comme sécurisée face à l'informatique quantique (2^256 possibilités) pour contrer les effets de l'algorithme de Grover.

- Distribution symétrique sécurisée : que ce soit par transport (génération centralisée de clés) ou par « téléportation » (QKD), la fourniture sécurisée de la même clé symétrique aux deux extrémités, protégée par un chiffrement symétrique, assure une distribution de clés résistante aux attaques par informatique quantique.

- Algorithme de chiffrement de données robuste : l'utilisation de l'AES256-GMAC (*Galois Message Authentication Code*) ou AES-GCM (*Galois Counter Mode*) est considérée comme sécurisée.

Deux attributs supplémentaires donneront une solution de référence pour la protection long terme de l'information. Ils apparaissent d'ailleurs comme besoins exprimés par les dernières réglementations européennes en matière de sécurité et de résilience numérique :

- Rotation des clés : Plus une clé est utilisée (en temps et en volume de donnée chiffrée), plus elle concentre de risque (compromission, analyses statistique, progrès technologique) et elle doit donc être régulièrement changée.

- Segmentation des fonctions de supervision : Les fonctions d'administration de la sécurité réseau et en particulier du chiffrement (activation/désactivation et gestion des règles associées) doivent pouvoir être séparée des fonctions plus traditionnelle de gestion de réseau (*Network Operations Center* - NOC). Même si ce dernier devait être compromis, le Centre de sécurité (*Security Operations Center* – SOC) doit pouvoir être préservé.

> **" Selon le Forum économique mondial, nous devrons évoluer vers une économie de sécurité quantique. Nous pensons aussi que l'industrie mesurera la nouvelle puissance à la portée des acteurs malveillants et devra, entre autre, y répondre par une offre de réseau et de connectivités à la sécurité physique et quantique. "**

La défense en profondeur et physique du réseau

Selon le Forum économique mondial, nous devrons évoluer vers une économie de sécurité quantique. Nous pensons aussi que l'industrie mesurera la nouvelle puissance à la portée des acteurs malveillants et devra, entre autre, y répondre par une offre de réseau et de connectivités à la sécurité physique et quantique.

Dans les communications actuelles, un chiffrement applicatif de bout en bout est souvent déjà en place (voir figure 4), reposant sur une infrastructure à clé publique (PKI). Il est désormais largement reconnu que ces dispositifs sont vulnérables face à l'informatique quantique.

À court et moyen terme, la cryptographie post-quantique (PQC) devra permettre

l'évolution des infrastructures PKI. L'équation du Dr. Mosca souligne l'urgence de cette transformation afin d'être protégé lorsque les attaquants disposeront de la puissance de calcul quantique nécessaire (« Q day »).

Cette migration vers la PQC prendra du temps mais renforcera la sécurité des communications, en assurant une résistance au déchiffrage quantique jusqu'aux points d'extrémités du réseau. Durant cette transition, un risque subsistera : le contenu des échanges actuels pourrait être intercepté et stocké pour être ultérieurement déchiffré (attaque *Harvest Now, Decrypt Later* – HNDL).

Même si les algorithmes PQC (par exemple ML-KEM) promettent de contrer les menaces des ordinateurs quantiques (CRQC), ils reposent sur des problèmes mathématiques qui finiront par être résolus. La question n'est donc pas de savoir si, mais quand leur sécurité sera compromise.

Pouvoirs publics et industriels reconnaissent ainsi que la sécurité des communications ne pourra pas reposer uniquement sur une protection PQC applicative et bout en bout. Aux États-Unis, la CISA, le NIST et la NSA ont défini des exigences et recommandations sur les algorithmes résistants aux technologies quantiques pour les infrastructures critiques et les systèmes de sécurité nationale. En Europe, les agences nationales telles que l'ANSSI en France et le BSI en Allemagne publient leurs recommandations techniques et accompagnent la mise en conformité des organisations. Toutes recommandent aujourd'hui une approche hybride, superposant plusieurs protections pour faire face aux capacités incertaines mais croissantes des acteurs malveillants.

Les entreprises devront également développer leur agilité cryptographique, c'est-à-dire la capacité d'adapter rapidement leurs mécanismes de protection face à de nouvelles menaces susceptibles de compromettre les algorithmes et d'exposer leurs infrastructures à des vols de données sensibles.

L'approche de défense en profondeur et physique de la solution Nokia *Quantum Safe Networks* (QSN) repose sur un environnement de cryptographie flexible, multicouche et conçu pour s'adapter aux besoins de communications spécifiques aux entreprises et de leurs différents cas d'usage.

Si les opérateurs d'infrastructure comprennent désormais qu'une seule couche cryptographique ne suffit plus pour contenir les risques, la solution QSN n'impose pas non plus le chiffrement à chaque couche OSI.

La cryptographie mathématique à clé publique, utilisée pour le chiffrement de bout en bout, peut ainsi être renforcée sur les principales artères du réseau d'infrastructure grâce à une ou plusieurs couches inférieures (niveaux 1, 2 ou 3 du modèle OSI), offrant des clés de qualité physique supérieure.

Cette protection réseau peut être déployée sous forme de 1+1 ou 1+N, créant ainsi une ou plusieurs couches additionnelles de sécurité. Une telle approche accroît la résistance au déchiffrage algorithmique, renforce la résilience en cas d'écoute clandestine et permet de faire évoluer la sécurité applicative tout en conservant la protection sous-jacente.

Lorsqu'un segment de réseau en fibre optique est traversé, le chiffrement résistant aux menaces quantiques peut être activé directement sur la couche optique (Optical Transport Network – OTN), garantissant une sécurité optimale.

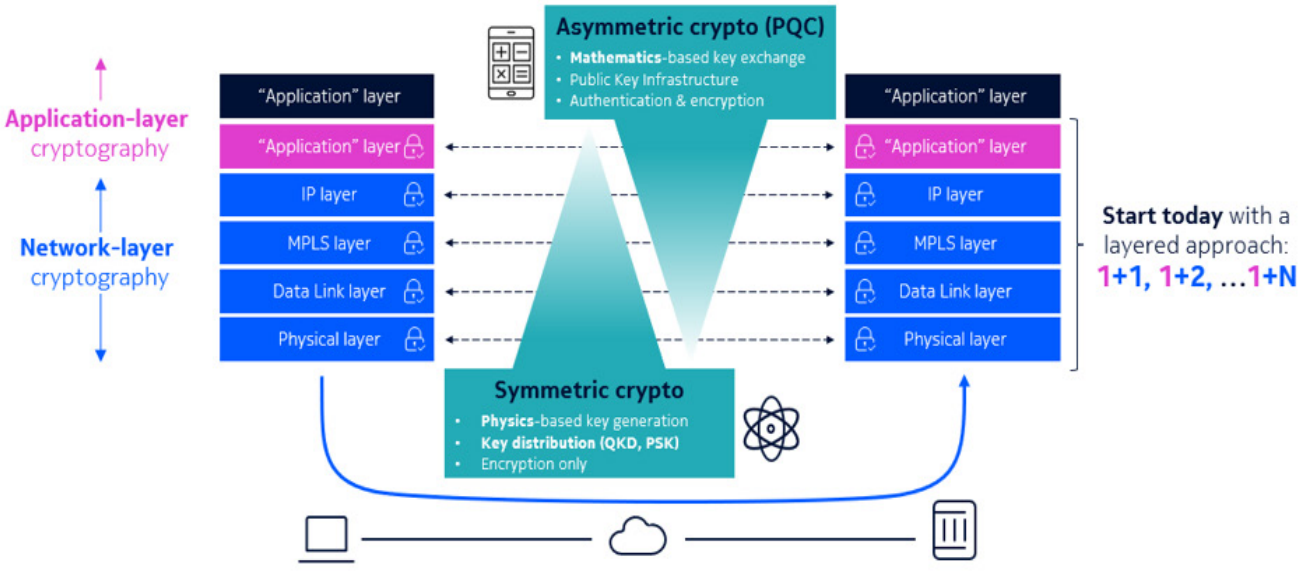


Figure 4 : Solution de cryptographie complète.

La supervision avancée de la fibre permet de détecter et localiser toute intrusion potentielle, et, si nécessaire, d'étendre la protection à davantage de services. Tous les types de trafic, et pas uniquement IP/Ethernet, peuvent ainsi être protégés. Cette activation n'impacte ni la bande passante disponible, ni la latence du service de connectivité.

Au-delà des données échangées, l'ensemble des métadonnées — en particulier les informations d'adressage et de routage des couches supérieures — est également chiffré et rendu opaque, même face à l'informatique quantique. Sans ce chiffrement, ces métadonnées seraient vulnérables à l'écoute clandestine et pourraient être exploitées pour analyser les flux et la topologie du réseau, facilitant des attaques telles que les *Distributed Denial of Service* (DDoS).

Le 1830 SMS moteur de la solution Nokia Quantum-Safe-Networks

Avec sa solution *Quantum-Safe Networks* (QSN), Nokia offre dès aujourd'hui plusieurs options de protection réseau contre les menaces quantiques.

Dans un mode manuel sécurisé, des clés robustes peuvent être créées puis remises « en main propre » aux points d'extrémité d'un service de connectivité chiffrée. Cependant, ce processus peut être long et fastidieux.

La solution QSN apporte surtout une automatisation complète : génération, orchestration et distribution des clés résistantes aux risques quantiques. Elle permet d'activer rapidement de nombreux services chiffrés et de renouveler les clés plus fréquemment, tout en éliminant les erreurs liées aux processus manuels.

Cette automatisation repose sur une gestion centralisée des clés, capable de les générer à partir d'une entropie physique, de les distribuer en toute sécurité et de surveiller l'état des services chiffrés depuis le SOC.

L'élément central, le Nokia 1830 SMS (conçu en France), constitue une plateforme intégrant un HSM certifié ANSSI, AIS31, FIPS 140-2 et CC EAL4+, garantissant une génération de nombres aléatoires fiables. Elle permet de générer et distribuer des clés de 256 bits de façon sécurisée, de gérer centralement les politiques de cryptographie, d'assurer la surveillance et

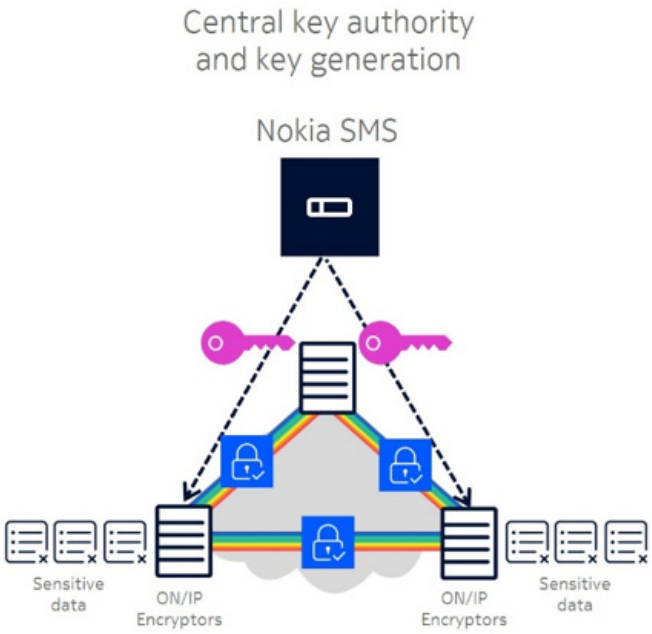


Figure 5 : Nokia 1830 SMS configuré en distribution symétrique centralisée.

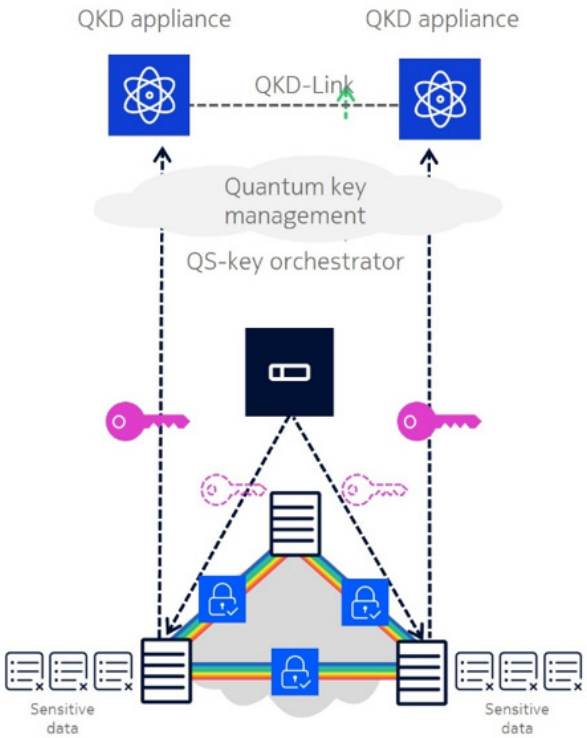


Figure 6 : Nokia 1830 SMS configuré en distribution symétrique QKD-Hybride terrestre.

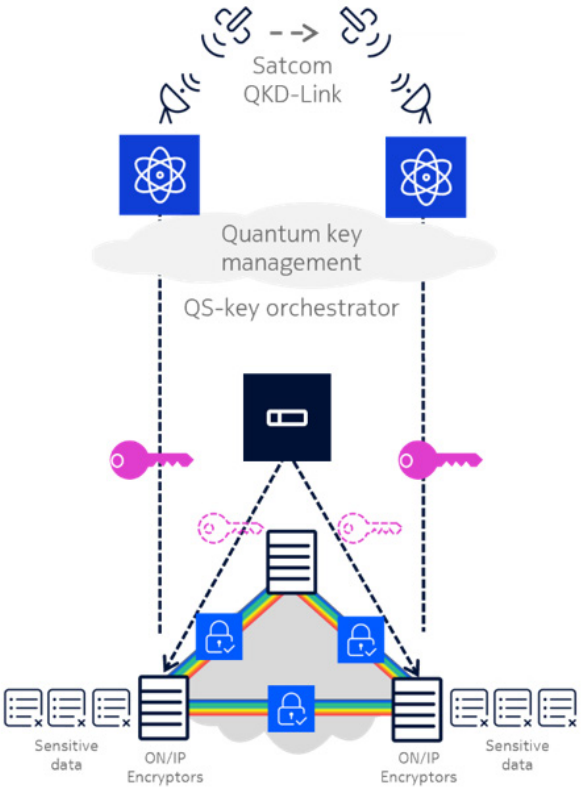


Figure 7 : Nokia 1830 SMS configuré en distribution symétrique QKD - Hybride par satellite.

la résilience du chiffrement, et de garantir automatisation, haute disponibilité et cloisonnement des accès (figure 5).

Grâce à son écosystème partenaire, QSN permet également de déléguer la génération et distribution des clés à des infrastructures quantiques (QKD). Le 1830 SMS communique à la fois avec les chiffreurs du réseau et avec les Q-KMS via l'interface standardisée ETSI GS QKD 014 (figure 6) . À la demande du 1830 SMS, les deux extrémités d'un service reçoivent une clé inviolable issue du réseau quantique. En cas de perturbation ou d'attaque sur le réseau quantique, le 1830 SMS peut basculer vers une génération locale classique afin de garantir la continuité du service.

D'autres architectures QSN, comme la distribution de clés quantiques par satellites (figure 7), sont actuellement en validation, offrant ainsi une protection sans contrainte de distance.

Conclusion

L'ordinateur quantique constitue aujourd'hui une menace majeure pour la confidentialité de nos communications, menace qui s'accentuera avec le développement de l'intelligence artificielle. La cybersécurité doit s'adapter pour y répondre, en multipliant les lignes de défense. Si le réseau représente une part essentielle de la surface d'attaque, il dispose également de puissants leviers pour renforcer la sécurité applicative.

La protection des communications ne se limite pas aux données transmises : elle inclut aussi la sécurisation des connexions elles-mêmes. Une sécurité efficace nécessite aussi une surveillance fine et continue. Au plus près de l'infrastructure, la couche de transport (optique) offre une protection physique avancée et peut faire du quantique et l'IA aussi de véritables ressources de défense du réseau.

La solution Nokia *Quantum Safe Networks* (QSN), adossée à l'environnement modulable de contrôle 1830 SMS, offre les outils essentiels pour accéder à la sécurité quantique. Déjà déployée au sein de nombreux réseaux commerciaux et stratégiques, et testée dans des architectures innovantes couvrant divers secteurs, elle permet une évolution progressive, résiliente et sécurisée de la protection applicative vers les algorithmes émergents.

Certifiée et éprouvée, cette solution unique constitue un atout stratégique pour les communications des entreprises dans les secteurs critiques, tout en offrant aux fournisseurs d'infrastructures et de services réseau un facteur de différenciation et de croissance. ■

Les auteurs

Fort de plus de trois décennies d'expérience internationale dans les réseaux, Yannick Gautier est un expert des infrastructures communicantes à forte valeur ajoutée. Il a été architecte en chef de solutions innovantes intégrant agrégation mobile, synchronisation ultraprécise et transport optique multiservice. Il est aujourd'hui, au sein de Nokia, responsable de l'offre produits pour les réseaux photoniques sécurisés sur le marché EMEA.

Avec près de trente ans d'expérience dans les télécommunications, Sylvain Chenard est responsable des solutions *Quantum-Safe Networks* au sein de l'activité Network Infrastructure de Nokia. Spécialiste des communications optiques sécurisées, de la cryptographie et de la virtualisation logicielle, il collabore avec Nokia Bell Labs pour développer et industrialiser des technologies de pointe visant à protéger l'infrastructure numérique du futur.

Références

[1] Nokia, "Quantum-safe optical networks," 2024. https://www.nokia.com/industries/quantum-safe-networks/

[2] EAGLE-1 is Europe's first quantum key distribution satellite system: https://www.ses.com/sites/default/files/2023-12/EAGLE-1_SES_Infographic_Quantum_Communications_20231213.pdf

[3] World Economic Forum - Transitioning to a Quantum-Secure Economy 2022: https://www3.weforum.org/docs/WEF_Transitioning%20to_a_Quantum_Secure_Economy_2022.pdf

[4] Field demonstration of a fully managed, L1 encrypted 3-node network with Hybrid Relayed-QKD and centralized Symmetric classical key management - 2024

[5] Quantum-safe networks: How telcos secure their future: https://www.frontier-enterprise.com/quantum-safe-networks-how-telcos-secure-their-future/

[6] Quantum-safe networks: protecting the future against quantum threats: https://biforesight.com/quantum/quantum-safe-networks-protecting-the-future-against-quantum-threats/

[7] Nokia and Proximus demonstrate future of network security with europe's first live hybrid quantum encryption key trial: https://www.nokia.com/about-us/news/releases/2023/06/20/nokia-and-proximus-demonstrate-future-of-network-security-with-europes-first-live-hybrid-quantum-encryption-key-trial/

[8] Quantum Computing Is Coming. Here's What Needs To Happen First. (forbes.com): https://www.forbes.com/sites/nokia-industry-40/2024/08/12/quantum-computing-is-coming-heres-what-needs-to-happen-first/

Résumé

À l'ère des échanges numériques, la sécurité des communications constitue un enjeu majeur. Il s'agit à la fois de maintenir la continuité des connexions et de préserver la confidentialité des informations sensibles.

La montée en puissance des ordinateurs quantiques menace directement les mécanismes actuels d'authentification et de chiffrement. Déjà, certains acteurs malveillants interceptent et stockent du trafic sécurisé pour le déchiffrer demain grâce aux capacités du calcul quantique.

Vulnérable, la cryptographie asymétrique doit évoluer vers des algorithmes plus robustes (PQC). Mais cette avancée ne suffira pas à garantir durablement la sécurité des communications: les agences de cybersécurité préconisent de multiplier les lignes de défense.

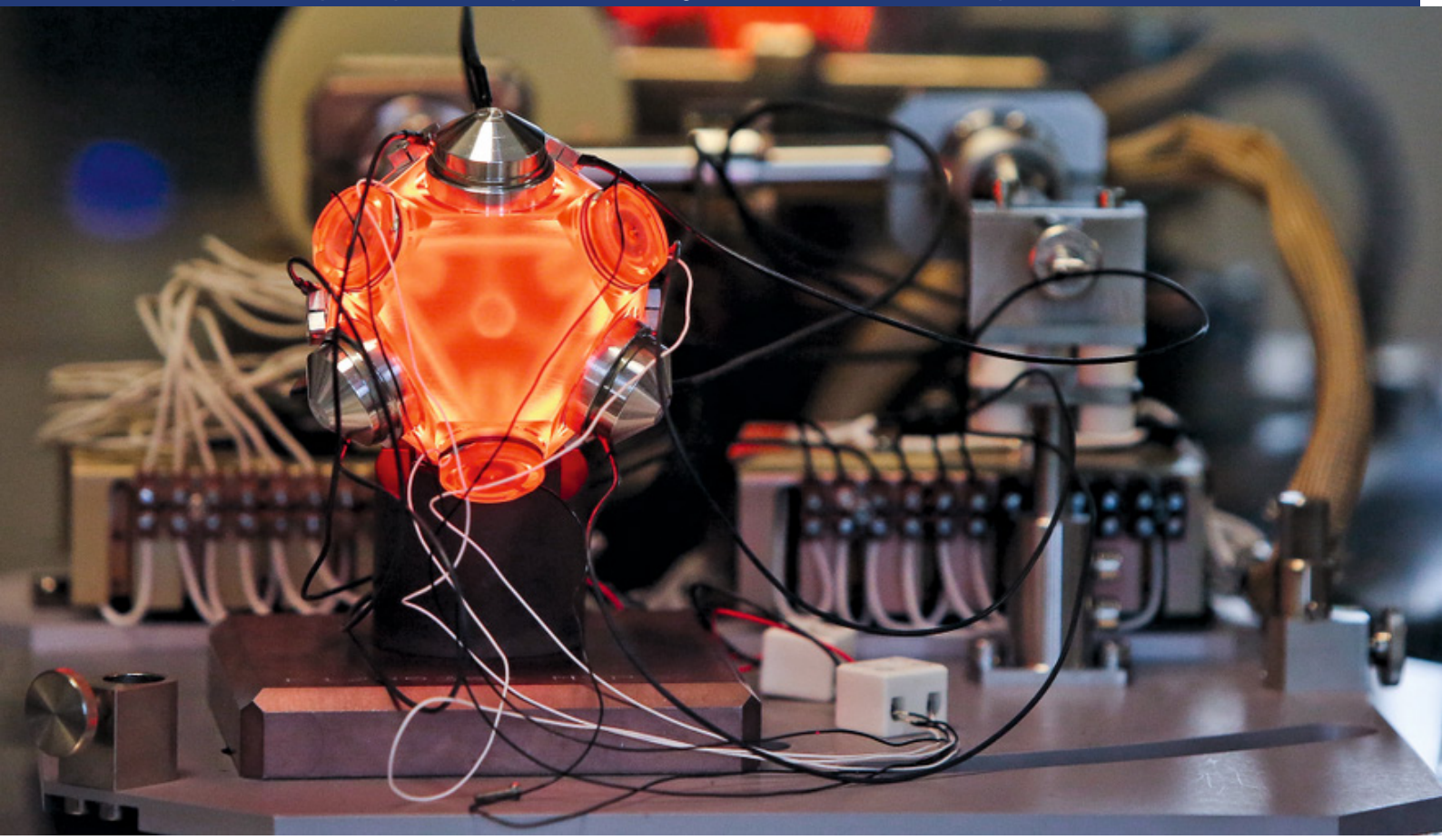
C'est dans ce contexte que s'inscrit *Quantum Safe Networks* (QSN), la solution flexible de Nokia, acteur de référence en sécurité quantique réseau. Elle offre une protection supplémentaire de nature physique, agissant au plus près du risque d'interception et des moyens avancés de surveillance, grâce à un chiffrement haute performance, sans compromis sur les liens optiques. Des clés issues de la physique classique ou quantique, distribuées symétriquement et orchestrées de manière intelligente, assurent ainsi un niveau inédit de robustesse et de résilience. Les adversaires se retrouvent privés de toute possibilité d'intercepter des données exploitables, d'identifier leur destinataire ou même simplement de détecter l'existence d'une communication, sur un réseau dont la topologie leur demeure invisible. ■

Abstract

In the era of digital communication, communications security is a major challenge. It involves both maintaining the continuity of connections and preserving the confidentiality of sensitive information.

The rise of quantum computers poses a direct threat to current authentication and encryption mechanisms. Some malicious actors are already intercepting and storing secure traffic to decrypt it in the future using quantum computing capabilities. Vulnerable, asymmetric cryptography must evolve toward more robust algorithms (PQC). But this advancement will not be enough to guarantee communications security in the long term: cybersecurity agencies recommend multiplying lines of defense.

This is the context in which Quantum Safe Networks (QSN), the flexible solution from Nokia, a leading player in quantum network security, comes into play. It offers additional physical protection, acting as closely as possible to the risk of interception and advanced surveillance methods, thanks to high-performance encryption, without compromising optical links. Keys derived from classical or quantum physics, distributed symmetrically and orchestrated intelligently, thus ensure an unprecedented level of robustness and resilience. Adversaries find themselves deprived of any possibility of intercepting exploitable data, identifying their recipient or even simply detecting the existence of a communication, on a network whose topology remains invisible to them. ■



Une centrale inertielle pour avion de Thales. Source : Thales.

Les capteurs quantiques :
lorsque la technologie est au service de notre quotidien

Si l'informatique quantique occupe le devant de la place publique ces dernières années, les capteurs à base de différentes technologies quantiques permettant de mesurer un large éventail de grandeurs physiques pourraient, à terme, eux aussi révolutionner notre quotidien.

Myriam Nouvel
Thales

Introduction

Ce qui est maintenant communément appelée « la seconde révolution quantique » ou « La nouvelle révolution quantique » [1] a débuté il y a une vingtaine d'années. Une accélération notable s'est produite en 2022, date de l'attribution du Prix Nobel de Physique à Alain Aspect, John F. Clauser et Anton Zeilinger pour leur expérimentation de l'intrication quantique. Depuis, cette révolution est portée, essentiellement, en termes d'investissements financiers mondiaux en recherche et développement, par des investissements dans l'informatique quantique (ordinateurs et calculs). Ainsi les autres pans de cette révolution sont-ils moins connus du grand public, attirant bien moins l'attention médiatique. Ils sont également financés dans une proportion moindre que l'informatique quantique [2]. Ces autres pans de le seconde révolution quantique sont :

- la cryptographie quantique ;
- les communications quantiques ;
- les capteurs quantiques.

Ces derniers en sont, dans une certaine mesure et à ce stade, les « parents pauvres ». Beaucoup de travaux restent donc à accomplir ! [3]

Les capteurs quantiques exploitent les propriétés fondamentales de la mécanique quantique - superposition, intrication et décohérence. Ils manipulent des particules individuelles de la physique, telles que les électrons, les atomes et les photons afin de mesurer des grandeurs physiques (temps, gravité, distance, champ magnétique, température, amplitude du champ électromagnétique) avec une précision et une sensibilité ultime.

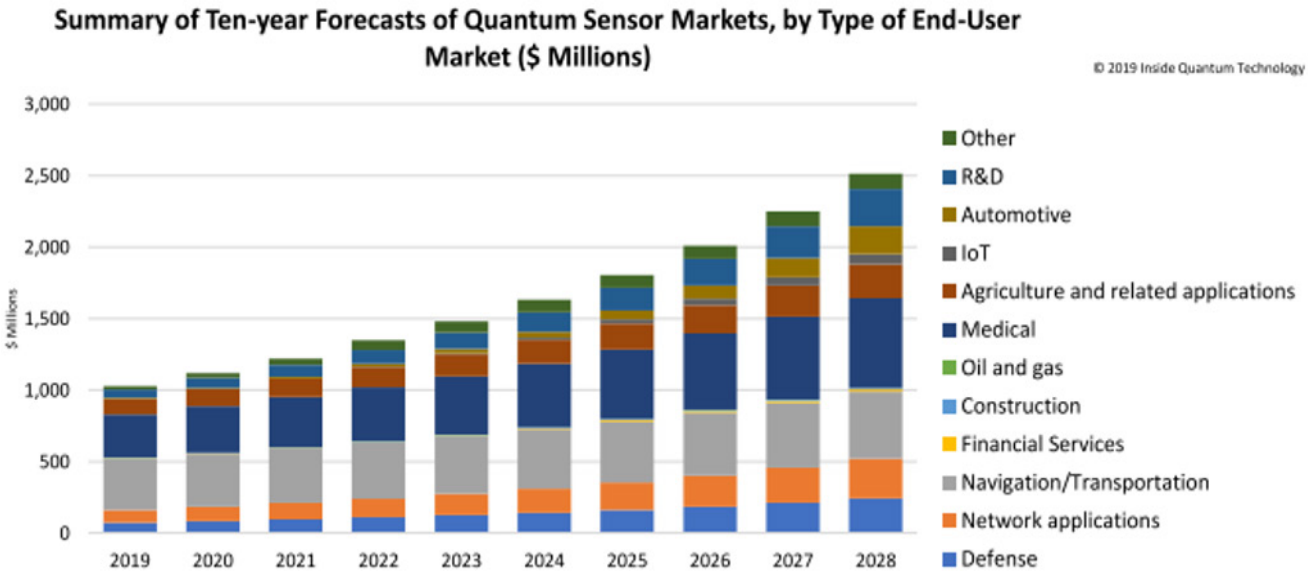


Figure 1 : Projection selon les domaines d'applications du marché des capteurs quantiques.

Dans un cadre classique, la sensibilité des capteurs est bornée par des contraintes physiques et technologiques : bruit thermique, fluctuations électromagnétiques, précision des instruments électroniques. Ces limites imposent un seuil minimal d'incertitude.

La mécanique quantique introduit un bruit de fond inévitable : le bruit quantique issu du principe d'incertitude de Heisenberg. Par exemple, la mesure simultanée de la position et de la vitesse d'une particule est fondamentalement limitée. Mais paradoxalement, les états quantiques peuvent être manipulés pour dépasser les limites classiques de détection.

Ainsi, contrairement aux capteurs classiques, qui sont souvent limités par le bruit thermique et d'autres sources d'erreur, les capteurs quantiques tirent parti de propriétés fondamentales des systèmes quantiques pour dépasser ces limitations. Ils représentent une avancée majeure dans le domaine de la métrologie.

En résumé, « un capteur quantique est un instrument de mesure qui recourt à des phénomènes de nature quantique pour mesurer une grandeur physique. Les capteurs quantiques utilisent des effets quantiques comme la superposition ou les interférences pour atteindre une très haute sensibilité ou stabilité à long terme, dépassant celle des dispositifs classiques ». [4]

Gravimètres, accéléromètres, magnétomètres ou encore horloges atomiques appartiennent déjà à cette catégorie d'outils. Leur impact potentiel couvre des domaines aussi variés que la médecine, la géophysique, la navigation ou la défense. Lawrence Gasman a présenté en 2019 la projection du marché des capteurs quantiques sur 10 ans (figure1).

Dans la deuxième section de cet article, nous présentons les principes physiques majeurs sous-jacents aux capteurs quantiques ainsi que quelques-unes des technologies clés. Dans la troisième section, nous décrivons quelques exemples d'application et explorons l'impact croissant des capteurs quantiques dans plusieurs secteurs clés de notre vie quotidienne : la navigation ou PNT (*Positioning Navigation and Timing*), la médecine, l'environnement et l'industrie et enfin la Défense. Pour chaque application, nous mettons en lumière les applications actuelles et les perspectives d'avenir.

Principes physiques et technologies clés

Fondements de la détection quantique

Les grands principes physiques exploités dans les capteurs quantiques sont :

La superposition quantique et l'interférence : Un atome ou un photon peut exister dans une superposition d'états. Lorsqu'on les fait interférer, la figure obtenue est extrêmement sensible aux perturbations extérieures (champs gravitationnels, magnétiques, accélérations). Cette sensibilité aux perturbations physiques extérieures peut donc être exploitée par les capteurs quantiques.

L'intrication quantique : Des particules intriquées partagent un état commun, même séparées spatialement. En utilisant des corrélations intriquées, il est possible de réduire le bruit de mesure et d'atteindre des précisions surpassant la limite dite *Standard Quantum Limit* (SQL).

Cohérence quantique : la durée pendant laquelle un système quantique garde sa cohérence influe sur la qualité de la mesure.

Ainsi les horloges atomiques constituent le premier succès des capteurs quantiques. En mesurant la fréquence de transition électronique d'atomes refroidis (comme le césium ou le strontium), on obtient une stabilité temporelle de l'ordre de 10^{-18}, ce qui correspond à une dérive d'une seconde sur plusieurs milliards d'années.

Exemples de technologies clés des capteurs quantiques

Le refroidissement et la manipulation des atomes

L'objectif de cette technologie est de ralentir au maximum le mouvement thermique des atomes afin d'observer et de manipuler leurs propriétés quantiques, en particulier leur comportement ondulatoire. On parle communément « d'atomes froids » ou d'atomes piégés, sans que des moyens de cryogénie soient utilisés.

En réduisant l'énergie cinétique moyenne des atomes, leur température est indirectement réduite tendant vers le zéro absolu (quelques microkelvins, voire des nanokelvins).

Le refroidissement repose principalement sur des techniques optiques et magnétiques :

Refroidissement par laser (ou refroidissement Doppler) : un faisceau laser est accordé légèrement en dessous de la fréquence de résonance d'une transition atomique. Quand un atome se déplace vers la source du laser, il perçoit la lumière décalée vers le bleu (effet Doppler) et absorbe un photon, ce qui le ralentit. Après absorption, l'atome réémet un photon dans une direction aléatoire, ce qui a pour effet moyen de réduire la vitesse globale des atomes. En combinant plusieurs faisceaux lasers dans différentes directions, le mouvement des atomes est ralenti dans les trois dimensions, créant un « piège optique » de basse énergie.

Les pièges magnéto-optiques : les faisceaux lasers sont combinés avec un champ magnétique spatialement variant afin de créer un piège qui à la fois refroidit et confine les atomes. Le champ magnétique agit sur les niveaux d'énergie des atomes selon leur position, modulant la fréquence de transition et assurant une force de rappel vers le centre du piège.

A ces basses températures, les atomes perdent pratiquement toute leur énergie thermique, laissant apparaitre des propriétés quantiques macroscopiques qui sont :

Interférométrie atomique : la nature ondulatoire des atomes froids permet de réaliser des expériences d'interférence avec des faisceaux d'atomes, analogues à des interféromètres optiques, mais avec des masses et des interactions différentes, pour des mesures extrêmement précises.

Longue cohérence quantique : les atomes se comportent comme des ondes de matière (principe de de Broglie) et conservent leur état quantique pendant des durées longues, ce qui est crucial pour les mesures précises.

Formation de condensat de Bose-Einstein : lorsque la température est suffisamment basse, un grand nombre d'atomes bosoniques occupent le même état quantique fondamental, formant une « super-particule » macroscopique. Cette propriété permet d'observer des phénomènes quantiques à grande échelle.

Les grandeurs physiques mesurées par la technologie des atomes froids :
- le temps ;
- l'accélération et la rotation ;
- le champ magnétique externe.

Typiquement, l'interféromètre atomique, comparable à l'interférométrie optique, utilise des ondes de matière. Cette technique repose sur la division d'un paquet d'ondes atomiques en deux trajectoires distinctes. ●●●

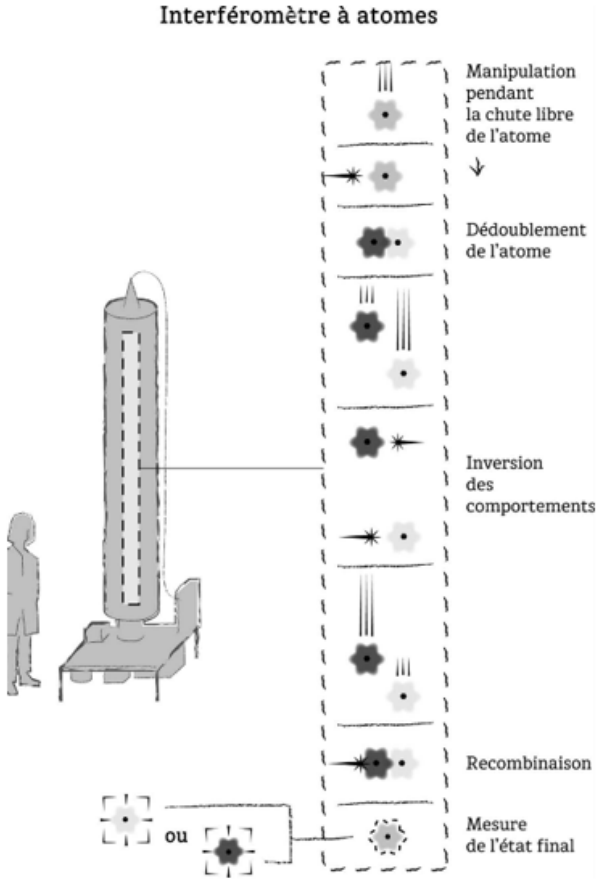


Figure 2 : Exemple d'un interféromètre à atome pour la mesure de la gravité. © Julien Bobroff.

” Le diamant est cinquante fois plus résistant que n’importe quel autre matériau naturel grâce à sa structure atomique très solide. Il comporte néanmoins plus d’une centaine de défauts atomiques. ”

La différence de phase accumulée entre les chemins dépend du champ gravitationnel, de l’accélération ou de la rotation (figure 2).

Les centres lacune-azote (NV : *Nitrogen Vacancy*)

Le diamant est cinquante fois plus résistant que n’importe quel autre matériau naturel grâce à sa structure atomique très solide. Il comporte néanmoins plus d’une centaine de défauts atomiques. Parmi ces défauts se trouvent les centres NV (*Nitrogen-Vacancy*) dans la structure cristalline du diamant, constitués d’un atome d’azote (N) adjacent à une lacune vide (*Vacancy*) dans le réseau de carbone.

La propriété principale des centres NV exploitée astucieusement pour permettre la mesure de grandeurs physiques, à l’échelle de la nanométrie, repose sur le spin électronique.

Le centre NV possède en effet un spin électronique (propriété quantique liée au moment magnétique) qui peut être préparé, manipulé et lu optiquement à température ambiante. En illuminant le cristal avec un laser vert, le centre NV émet une fluorescence dans le domaine du rouge dont l’intensité dépend de son état de spin. Ceci permet une lecture non invasive et très précise de cet état sans destruction.

La fluorescence, reliée au niveau d’énergie du spin du Centre NV, décroît en présence des champs magnétiques ou électriques environnants. Les variations d’énergie du spin du centre NV modulent la fluorescence (effet Zeeman), permettant de mesurer ces grandeurs physiques avec une très grande sensibilité.

Le principe général simplifié de mise en œuvre de la mesure est le suivant (figure 3).

A. Initialisation : le spin est « mis à zéro » par éclairage laser.

B. Manipulation : le spin est manipulé par des micro-ondes en fonction de la grandeur physique à mesurer (champ magnétique, température).

C. Lecture : la fluorescence recueillie permet de déduire l’état du spin, donc d’extraire la valeur de la grandeur physique.

Les centres NV dans le diamant sont utilisés dans des magnétomètres quantiques, des thermomètres à l’échelle nanométrique, ou pour l’imagerie de matériaux magnétiques et biologiques, offrant une résolution spatiale nanométrique et des mesures extrêmement précises, souvent à température ambiante [4] [6].

Les jonctions Josephson et la supraconductivité

Une jonction Josephson est un dispositif constitué de deux matériaux supraconducteurs séparés par une couche très fine d’isolant (quelques nanomètres).

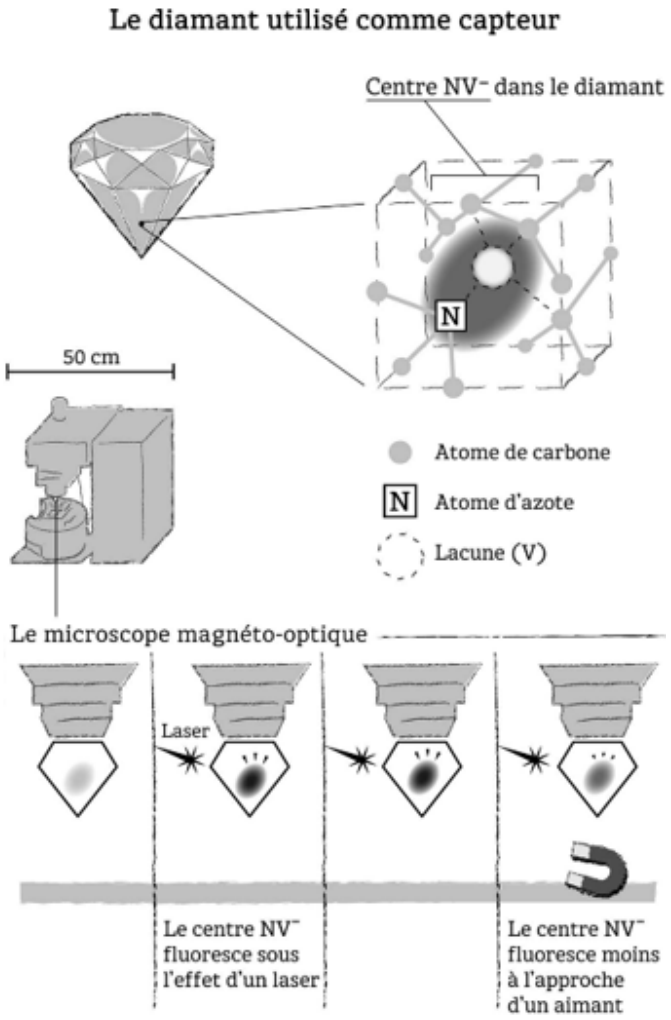
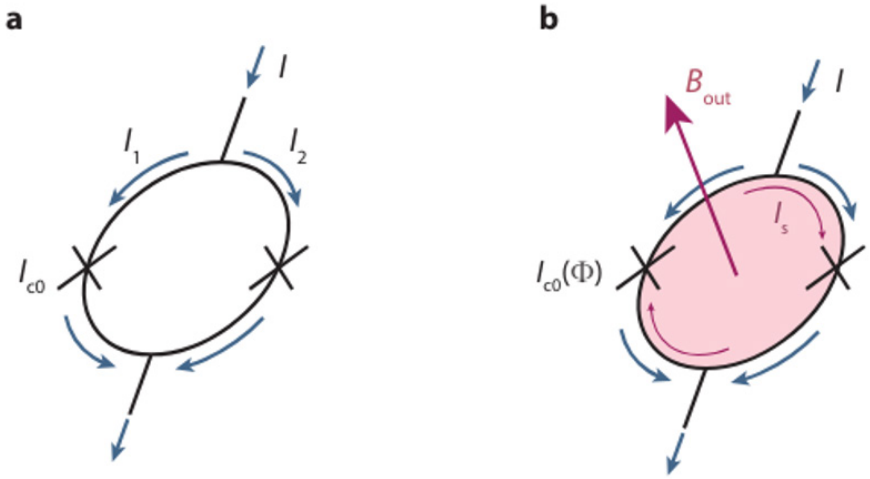


Figure 3 : Le principe du microscope magnéto-optique à centre NV de diamant. © Julien Bobroff.



I Figure 4 : Principe de fonctionnement des SQUIDs avec et sans application de champ magnétique. [6].

Cette configuration permet le passage d'un courant électrique supraconducteur à travers l'isolant sans aucune résistance, via un phénomène quantique appelé « effet Josephson ».

Les principes physiques sont les suivants :

• **Courant Josephson sans tension :** un courant superfluide peut traverser l'isolant sans perte d'énergie.

• **Relation courant-phase :** ce courant dépend de la différence de phase de la fonction d'onde supraconductrice entre les deux électrodes. Cette phase est une grandeur quantique fondamentale.

• *Effet de la tension appliquée :* une tension constante génère une oscillation du courant à une fréquence liée à la tension (effet Josephson AC).

Un *Superconductive Quantum Interference Device* (SQUID) est une boucle supraconductrice contenant deux jonctions Josephson en parallèle (figure 4).

En l'absence de champ magnétique et pour un courant de polarisation donné inférieur au courant critique, le courant traversant le dispositif est donné par la relation courant-phase Josephson :

$$I = I_1 + I_2 = I_{c0}(sin\varphi_1 + sin\varphi_2),$$

Avec $\varphi_{1,2}$ les différences de phase au travers des jonctions 1 et 2 et I_{c0}, le courant critique d'une jonction. Lorsqu'un courant de polarisation inférieur au courant critique est appliqué au dispositif, ce dernier passe en état supraconducteur générant une tension aux bornes du SQUID.

Lorsqu'un champ magnétique est appliqué perpendiculairement au SQUID, celui-ci doit respecter la relation courant-tension Josephson mais également le changement de phase total au voisinage de la boucle SQUID qui doit être un multiple de 2π, afin de garantir que la fonction d'onde au travers de la boucle n'a qu'une valeur. Un courant variable est généré pour compenser la variation de champ magnétique. Ceci induit une baisse du courant critique du SQUID périodique avec le champ tel que :

$$I_c(\Phi) = 2I_{c0}\left|\cos\left(\frac{\pi\Phi}{\Phi_0}\right)\right|.$$

En choisissant un point de fonctionnement juste au-dessus de I_c, une variation de champ magnétique va générer une variation de tension au travers du SQUID.

Les applications

D'après Olivier Ezratty dans [8], d'un point de vue du transfert entre la recherche et les applications, le marché des capteurs quantiques semble plus mature que celui de l'informatique quantique avec des niveaux de TRL[1] plus hauts. Néanmoins ce n'est pas sans compter que beaucoup des capteurs quantiques annoncés ne sont pas encore dans une phase d'industrialisation réelle. La figure 5 démontre bien le foisonnement d'acteurs dans différentes technologies.

Dans cette section, nous tenterons de fournir une description non exhaustive des domaines d'applications possibles et potentiels.

La navigation et PNT : vers une précision extrême et une autonomie renforcée

Aujourd'hui, la navigation repose largement sur les systèmes de positionnement par satellites (GPS, Galileo, GLONASS, Beidou) qui fournissent des données de localisation avec une précision de l'ordre de quelques mètres, voire quelques centimètres dans les meilleures configurations. Ces systèmes utilisent des horloges atomiques embarquées qui fournissent des référentiels temporels extrêmement stables, condition indispensable à la triangulation par temps de propagation radio. Cependant plusieurs limitations subsistent :

• la dépendance au signaux satellites, qui peuvent être brouillés ou compromis par des attaques malveillantes (*spoofing*) ;

• une précision insuffisante dans certains cas pour des applications critiques (drones, conduite autonome) ;

• la difficulté à prolonger la navigation dans l'absence de tout signal externe.

Les avancées en horlogerie atomique numérique miniaturisée, associées au ●●●

1 L'échelle TRL (*Technology readiness level*) évalue le niveau de maturité d'une technologie jusqu'à son intégration dans un système complet

développement des capteurs inertiels quantiques, apportent des solutions prometteuses :

• Les horloges atomiques compactes à base d'atomes froids sont en train d'être miniaturisées pour être embarquées sur des satellites et même dans des dispositifs terrestres. Leur stabilité temporelle accrue permet d'améliorer la précision du positionnement, avec des marges d'erreur réduites à des niveaux inférieurs au centimètre sur le long terme [9].

• Les capteurs inertiels quantiques à base d'atomes froids permettent avec une extrême précision la mesure directe des accélérations et rotations en l'absence de référence (GPS).

• Systèmes de navigation hybrides : le couplage des données issues de capteurs quantiques avec des algorithmes avancés permet de corriger les dérives du positionnement inertiel classique et d'assurer une continuité de la navigation dans des environnements complexes [10].

Les exemples concrets d'application sont prometteurs pour l'aéronautique et les drones qui utilisent déjà des systèmes de navigation inertielle. Les versions quantiques amélioreraient fortement leur autonomie et précision, particulièrement dans les zones urbaines denses ou les espaces soumis à des perturbations électromagnétiques.

Malgré le ralentissement actuel du marché de la voiture autonome, l'intégration de capteurs quantiques compacts (tels que les centres NV par exemple auxquels Bosch s'intéresse fortement) augmenterait la fiabilité des données de localisation.

La médecine

Le corps humain génère de nombreux signaux électriques et magnétiques très faibles (de l'ordre du picotesla ou moins) au départ des neurones, du cœur et d'autres tissus. La détection non invasive par des capteurs quantiques ultrasensibles, notamment aux champs magnétiques et donc biomagnétiques, ouvre la voie à des diagnostics précoces et précis des pathologies.

De plus, même si la miniaturisation de certaines technologiques de capteurs quantiques actuels -à base de centre NV ou de SQUID- n'est pas optimale, ils demeurent moins coûteux en énergie électrique et plus facilement portatifs que des dispositifs de type IRM ((Imagerie à résonance magnétique).).

Des types d'utilisation possibles sont donc :

Magnétoencéphalographie (MEG) quantique : la détection des faibles champs magnétiques du cerveau, par des capteurs quantiques portables, améliore le suivi des activités neuronales. Elle permet de mieux comprendre les fonctions cérébrales, ou de détecter précocement des troubles tels que l'épilepsie, la maladie d'Alzheimer ou la schizophrénie.

IRM portatif : la startup française Chipiron propose ce type de produit permet-

Figure 5 : Représentation du marché des capteurs quantiques et des quelques technologies habilitantes issue de [8].

tant de ne pas déplacer le patient (cas d'urgences par exemple) [11].

Imagerie cardiaque ultra-sensible : les capteurs quantiques peuvent cartographier les variations de champ magnétique liées à l'activité cardiaque avec une précision hors du commun, aidant à diagnostiquer fibrillations, arythmies et autres troubles (*cf.* ce que développe la société Bosch).

Biosenseurs quantiques : la nanométrie quantique permet aussi la détection ultra-sensible de biomolécules spécifiques, avec des capteurs capables d'interagir à l'échelle moléculaire. Ces biosenseurs ouvrent la voie à :

• la détection rapide de pathogènes ou biomarqueurs dans des échantillons biologiques (sang, urine).

• le suivi personnalisé des traitements médicamenteux via la détection en temps réel des concentrations de substances dans le corps.

L'environnement et l'industrie

Si nous nous limitons aux technologies mises en œuvre dans les capteurs quantiques mesurant des informations de température, de gravité, de champ magnétique ou encore d'accélération, les applications dans l'environnement et l'industrie sont de type :

Mesures fines pour la gestion des ressources naturelles : La mesure des variations infimes de pression, température ou humidité locale par capteurs quantiques améliore la modélisation des systèmes climatiques ou hydrologiques.

Détection précoce de défauts mécaniques par contrôle non destructif des pièces produites : les capteurs quantiques d'accélération et de vibration peuvent capter des anomalies invisibles aux capteurs classiques, permettant de prévenir des pannes coûteuses [12].

Suivi des paramètres de processus : température, pression, champ magnétique dans les machines peuvent être suivis avec une très haute résolution, assurant une meilleure qualité des produits et l'optimisation énergétique.

Contrôle de qualité : les capteurs quantiques basés sur la détection photonique ou atomique permettent d'effectuer des mesures ultra-précises de dimensions ou de propriétés mécaniques à l'échelle nanométrique, essentielles dans l'électronique ou la microfabrication.

La Défense

Les applications potentielles ou avérées dans le domaine de la Défense demeurent plus confidentielles tant les enjeux d'avantages stratégiques et de souveraineté sont importants. Il peut néanmoins être cité les applications suivantes :

Localisation précise et la navigation autonome : les capteurs décrits dans la section 3.1 peuvent être utilisés dans des zones contestées et/ou brouillées, dites GNSS denied (*Global Navigation Satellite System*).

Détection magnétique et géophysique, ainsi que la détection électromagnétique large bande : Les magnétomètres quantiques (basés sur les atomes froids, les centres NV ou les SQUID) peuvent détecter des signatures magnétiques faibles, utiles pour la détection de véhicules sous-marins, de munitions enfouies ou d'équipements militaires cachés. Ils permettent aussi la surveillance des champs magnétiques terrestres pour la géolocalisation passive.

Radar quantique : Des recherches sont en cours pour exploiter les propriétés quantiques dans le développement de radars. Néanmoins ces propriétés ne sont pas directement exploitables à l'émission et à la réception d'une onde électromagnétique propres à la détection radar réalisée par une première étape de filtrage adapté. Le terme Radar n'est peut-être pas bien adapté pour désigner ce nouveau type de capteurs qui seraient capables de détection et localisation à longue portée des cibles non coopératives (*cf.* [13]).

L'auteur

Myriam Fiani Nouvel est Ingénieure, diplômée de l'ENSEA (Ecole Nationale Supérieure de l'Electronique et de ses Applications) en 1998 et Docteur en automatisme et traitement du signal (Université Paris-Sud, 2001).
De 2001 à 2022 à la Direction Technique de Thales DMS (Systèmes de Mission de Défense), elle est successivement ingénieure d'études, responsable de projets d'études DGA et d'études européennes dans le domaine Radar aéroporté, puis responsable de service d'études algorithmiques appliquées de guerre et enfin responsable du département Simulation.
De 2008 à 2022, elle est en charge de la réglementation du spectre pour THALES DMS, participant à 4 Conférences des Radiocommunications et à des études de partage pour des sujets en lien avec les Radars et la protection de leurs bandes de fréquences. Elle a également été pendant 4 ans la présidente de la Commission Fréquences du GIFAS.
En 2023, elle rejoint THALES SIX (Systèmes d'Information et Communication Sécurisés) pour prendre en charge le pilotage programmatique et technique d'un projet autour des technologies quantiques pour une durée de deux ans.
Depuis 2025, elle est charge de la réglementation du spectre pour THALES SIX et est également référente simulation pour l'ensemble des produits Radiocommunications, Radioaltimètres, Liaisons de Données et systèmes de connectivité.
Elle est impliquée dans la SEE (Société de l'électricité, de l'électronique et des technologies de l'information et de la communication) depuis près de 20 ans (membre émérite).
Membre senior IEEE.
Présidente générale de la conférence « IEEE International Radar conference 2024 » RADAR 2024.
Membre du comité d'organisation et du comité scientifique de la conférence QUEST-IS (QUantum Engineering Sciences & Technologies for Industry and Services) - From Quantum Engineering to Applications for Citizens.

Conclusion

Dans cet article, nous avons pu dresser un panorama non exhaustif des applications avérées et potentielles dans des domaines très variés tels que la médecine, la navigation ou la Défense des capteurs à base de technologies quantiques. Tous ces capteurs offrent la promesse d'une amélioration notable des performances en termes de précision de mesure, stabilité par rapport à des capteurs classiques, tout en apportant des avantages de miniaturisation des capteurs en eux-mêmes. Des défis restent à relever :

• la chaîne industrielle – très souvent la production des technologies quantiques est encore faite dans des laboratoires de recherche (par exemple les diamants à Centres NV) ;

• la maîtrise, la production et l'intégration dans les capteurs des technologies habilitantes (lasers, cryogénie).

Nous n'avons pas encore fini de découvrir l'apport dans le quotidien des capteurs quantiques tout en nous souvenant que parfois une technologie (quantique ou non) peut en chasser une autre !

Pour preuve les lecteurs et graveurs de CD commercialisés à grande échelle des années 1990 jusqu'aux années 2000-2010 [14], oubliés au profit des contenus digitaux ou des vinyles pour l'écoute de la musique par le grand public. ■

Références

[1] Bienvenue dans la Nouvelle Révolution Quantique de Julien Bobroff, Ed. Flammarion 2022.
[2] Marché de la technologie quantique : les chiffres à connaître - Bpifrance Le Hub : https://lehub.bpifrance.fr/marche-de-la-technologie-quantique-les-chiffres-a-connaitre/#:~:text=Le%20march%C3%A9%20mondial%20des%20technologies,%2C8%20milliard%20d%27euros
[3] Capteurs quantiques – Portail de la stratégie nationale quantique : https://quantique.france2030.gouv.fr/perimetre/capteurs-quantiques/
[4] Quantum Sensing, C. Degen, F. Reinhard et P. Cappellaro, Reviews of modern physics 89 (3), 035002 – 2017.
[5] Quantum Sensing with nitrogen-vacancy colour centers in diamond. Thierry Debuisschert, Photoniques, Numéro 107, Mars-Avril 2021.
[6] Le centre coloré NV du diamant : un capteur quantique multifonctionnel. Vincent Jacques, Aurore Finco, Isabelle Robert-Philipp, Reflets de la Physique Dossier Le Diamant février 2025
[7] I. C. Rodrigues, Coupling harmonic oscillators to superconducting quantum interference cavities, PhD thesis (2021).
[8] Understanding Quantum Technologies Volume 4/5 : Communications and Sensing 7ième édition -2024. O. Ezratty
[9] Atomic Clocks - Quantum Technology | Quantum Flagship : https://qt.eu/quantum-principles/basic-science/atomic-clocks
[10] Q-CTRL wins DARPA awards to develop quantum sensors for navigation, JP Joosting, Technology News, 28 août 2025.
[11] Chipiron High-quality 1 mT MRI, Dimitri Labat, white paper March 10, 2025 chipiron-white_paper_10032025.pdf : https://www.chipiron.co/wp-content/uploads/2025/03/chipiron-white_paper_10032025.pd
[12] High-resolution non-destructive detection of grinding burns with NV diamond quantum magnetometer, Baptiste Vindolet, Benjamin Ducharne, HoaiNam Nguyen ,Xavier Mougenot, Christophe Gallais ,ThomasHingan, NDT & E International, Volume 155, October 2025, 103439
[13] Detecting a target with quantum entanglement, Giacomo Sorelli, Nicolas Treps, Frédéric Grosshans, Fabrice Boust, IEEE Aerospace and Electronic Systems Magazine, Volume: 37,Issue: 5, 01 May 2022
[14] Académie des Sciences et Lettres de Montpellier Bull. Acad. Sc. Lett. Montp., vol. 49 (2018) Séance publique du 3 décembre 2018 Mécanique quantique : un monde étrange et pourtant familier Jean-Pierre NOUGIER

Résumé

Les capteurs quantiques font partie des quatre pans principaux de la seconde révolution. Moins médiatisés que l'informatique quantique et également moins financés (comme par exemple le programme PROQCIMA lancé par le ministère des Armées en 2024), les capteurs quantiques de par leur grande précision et stabilité de mesures des grandeurs physiques, telles que la température, le temps ou encore le champ magnétique trouvent de nombreux champs d'application. De la géolocalisation à la Défense, en passant par la médecine ou le contrôle non destructif en industrie, la montée en maturité des potentiels produits se poursuit à des rythmes différents selon la technologie clé quantique mise en œuvre et la maîtrise des technologies dites habilitantes tels que les lasers ou la cryogénie. Qui sait si la fin de la course à l'informatique quantique confrontée à la maîtrise de l'industrialisation mais surtout la miniaturisation et l'intégration de ces mêmes technologies ne permettra pas de démocratiser ces capteurs « magiques » ! ■

Abstract

Quantum sensors are one of the four main areas of the second revolution. Less publicized than quantum computing and also less funded (such as the PROQCIMA program launched by the Ministry of the Armed Forces in 2024), quantum sensors, due to their high precision and stability in measuring physical quantities, such as temperature, time, or even the magnetic field, find numerous fields of application. From geolocation to Defense, including medicine or non-destructive testing in industry, the rise in maturity of potential products continues at different rates depending on the key quantum technology implemented and the mastery of so-called enabling technologies such as lasers or cryogenics. Who knows if the end of the race for quantum computing, faced with the mastery of industrialization but especially the miniaturization and integration of these same technologies, will not allow these "magical" sensors to be democratized! ■

Les défis de la création d'ordinateurs tolérants aux fautes

La puissance des algorithmes quantiques est lié à l'utilisation de bits quantiques qubits qui peuvent être dans des superpositions d'états. Or cette superposition d'états subit très rapidement des altérations de phase dépendantes de l'environnement. C'est pourquoi très vite des mécanismes de corrections d'erreurs ont été proposés pour résoudre les erreurs de phase mais ont eu pour conséquence de définir des qubits logiques idéaux et des qubits physiques liés au matériel. Le nombre de qubits physiques selon les cas augmente dans des proportions importantes par rapport au qubits logiques qui ne dépendent que de l'algorithme. Le développement de calculateurs quantiques est dépendant de la mise au point de ces systèmes de correction.

Olivier Ezratty

Auteur, enseignant, cofondateur de la Quantum Energy Initiative

En juin 2025, l'Académie des Technologies publiait le rapport « État de l'art de l'ordinateur quantique tolérant aux fautes - Questions et défis ». Commandé par l'Etat (SGPI), l'objectif était d'apporter un regard sur ces défis pour identifier les verrous scientifiques et technologiques les plus importants et ainsi créer ces ordinateurs quantiques qui devraient apporter un avantage certain par rapport aux supercalculateurs.

Ce rapport a été préparé pendant près de deux ans par un groupe de travail comprenant des membres de l'Académie des Technologies et des spécialistes du domaine venant des milieux académiques et industriels. Il résulte de l'audition de plusieurs dizaines de scientifiques, académiques et industriels. Il se focalise sur l'état des lieux des technologies de qubits développées en France et en les mettant en perspective vis-à-vis des technologies développées dans le monde. Il couvre aussi l'état de l'art des démonstrations de corrections d'erreur, de qubits logiques et de tolérance aux fautes ainsi que les approches permettant le passage à l'échelle.

L'objet de cet article est de donner un aperçu des principales conclusions de ce rapport et un éclairage sur la question posée.

La recherche d'avantages quantiques algorithmiques et cas d'usages

Le rapport explique les notions d'algorithme quantique, d'avantage quantique calculatoire, et décrit comment cet avantage varie selon les algorithmes et les cas d'usage.

Des arguments théoriques montrent qu'un ordinateur quantique tolérant aux fautes (FTQC) pourrait résoudre certaines classes de problèmes plus rapidement qu'un ordinateur classique, tels que la factorisation des grands nombres entiers ou la simulation de systèmes quantiques. L'avantage quantique couvre aussi potentiellement la qualité des solutions générées comme la précision chimique d'une simulation.

Le gain de temps théorique par rapport aux meilleurs algorithmes classiques est le plus souvent uniquement polynomial pour d'autres classes de problèmes. Son utilité pratique dépendra de divers effets de seuils et notamment du temps d'exécution des portes quantiques qui est relativement lent et peut compenser négativement les bénéfices du parallélisme quantique. Cela concerne en particulier les algorithmes de résolution de problèmes d'optimisation et de décision, qui sont du domaine de la recherche opérationnelle. Des questionnements équivalents existent au sujet des algorithmes d'apprentissage automatique (*machine learning*) en raison notamment du coût de chargement des données d'entraînement.

Les premières estimations de ressources pour des algorithmes utiles dédiés aux calculateurs FTQC à même de résoudre des problèmes de portée industrielle sont de l'ordre de plusieurs milliers de qubits logiques, avec des milliards d'opérations générant potentiellement des temps de calcul très longs. Cela illustre le besoin d'optimiser la vitesse d'exécution des circuits quantiques et de la correction d'erreurs.

Au vu de l'audition des entreprises utilisatrices comme EDF, Total Energies et Thales, les cas d'usage industriels du FTQC sont, pour l'instant, peu ou mal identifiés en France. Les industriels se sont focalisés sur l'exploration des applications sur les ordinateurs quantiques bruités disponibles actuellement dits NISQ (*Noisy Intermediate Scale Quantum*) ou sur les ordinateurs quantiques analogiques comme ceux de la startup française Pasqal. Leur avantage quantique en vitesse de calcul ou qualité des résultats généré n'est pas encore acquis.

Le rôle de la correction d'erreurs

Vu du développeur, les qubits sont des objets mathématiques permettant de résoudre des problèmes à l'aide de mécanismes relevant de l'algèbre linéaire. ●●●

” Un qubit est un objet analogique fragile qui peut prendre une infinité de valeurs possibles. Stabiliser et/ou corriger un objet analogique est bien plus difficile que pour un objet binaire. ”

Des portes quantiques s'appliquent à un ou plusieurs qubits et réalisent des opérations de multiplication de vecteurs par des matrices carrées de nombres complexes. Cela relève du bon vieux calcul matriciel. De nombreuses conditions sont à réunir pour obtenir une accélération exponentielle dans ce cadre. Elles concernent les portes quantiques utilisées ainsi que la structure du problème à résoudre. Tous les algorithmes quantiques ne sont pas égaux devant l'accélération.

Le substrat physique de ces qubits sont des objets quantiques tels que des atomes, des électrons, des photons individuels, ou des systèmes quantiques composites comme des qubits supraconducteurs, dont on peut contrôler une propriété physique prenant deux valeurs possibles, l'initialiser, créer une superposition des deux états possibles de cet objet, relier entre eux ces objets par le mécanisme de l'intrication et enfin, mesurer l'état à la fin du calcul.

Quels sont ces deux états ? Pour des atomes, il peut s'agir de leur niveau d'énergie correspondant à l'excitation du seul électron de la dernière couche d'électron, mais aussi le spin du noyau de l'atome. Pour les électrons piégés dans des puits de potentiels, dans les qubits dits « silicium » ou « à boites quantiques » (chez Quobly), ou dans des nanotubes de carbone (comme chez la startup française C12), la propriété exploitée est leur *spin* dans une direction donnée. Avec les photons, il s'agit de la polarisation qui est par exemple soit horizontale soit verticale mais également la longueur d'onde ou le moment de l'émission et cela devient d'ailleurs très vite contre-intuitif. On exploite aussi des systèmes quantiques composites, aussi dénommés « atomes artificiels », qui ont deux états quantiques possibles. C'est le cas des qubits supraconducteurs qui sont utilisés par IBM, Google, IQM et plein d'autres acteurs. Ce sont des courants électriques supraconducteurs oscillant à une fréquence de quelques MHz et traversant une barrière de potentiel que l'on appelle une jonction Josephson, le tout à une température très basse, de 10 mK. L'état 0 ou 1 de cet objet correspond à deux fréquences de résonance et phases bien distinctes d'un oscillateur anharmonique.

En informatique classique, les bits sont à zéro ou un et on ne se pose pas trop de question, même si on doit tout de même corriger leur valeur, surtout lorsque les bits sont transmis par des moyens de communication ou emmagasinés dans des systèmes de stockage. Mais la correction est relativement facile car un bit n'a que deux états possibles.

A contrario, un qubit est un objet analogique fragile qui peut prendre une infinité de valeurs possibles. Stabiliser et/ou corriger un objet analogique est bien plus difficile que pour un objet binaire.

Deux principales méthodes sont proposées pour traiter ce problème. La première qui est adaptée aux ordinateurs quantiques de type NISQ est la mitigation d'erreurs. Elle utilise un post-traitement qui corrige les effets des erreurs compte-tenu de la connaissance que l'on a acquise à leur sujet. Cela fait principalement appel à des méthodes d'apprentissage automatique (*machine learning*). Mais cela ne peut pas fonctionner à grande échelle, étant limité à 100 à 200 qubits physiques, et elle coûte cher en calcul classique.

La seconde méthode est la correction d'erreurs. Elle joue un rôle fondamental pour réaliser des ordinateurs quantiques universels et les dernières avancées de ce domaine sont nombreuses autant en provenance d'équipes académiques que des industriels tels que Google, IBM, QuEra et aussi Alice&Bob.

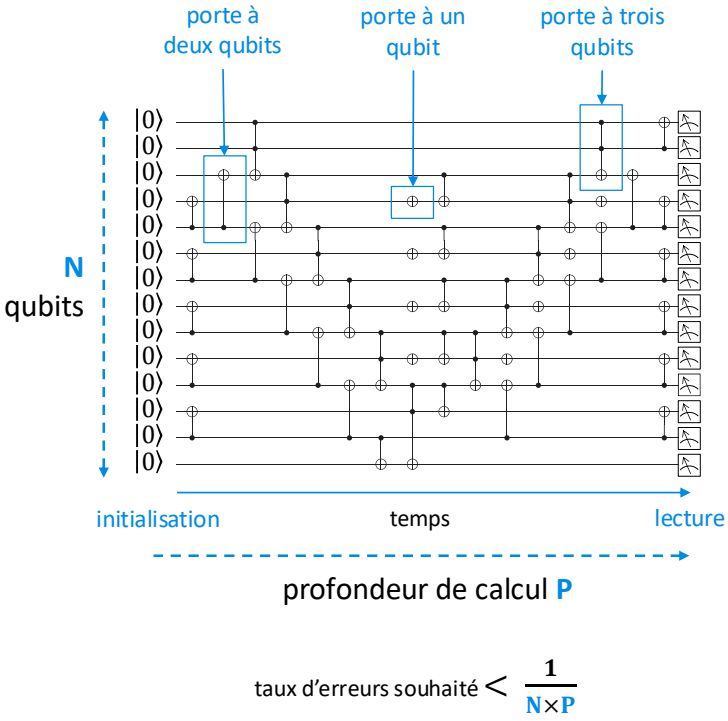
La recherche en correction d'erreurs quantiques a beaucoup progressé au cours des cinq dernières années, avec des avancées théoriques et des démonstrations expérimentales significatives. La plus connue est celle de Google avec son processeur Willow de 105 qubits supraconducteurs qui supporte une mémoire quantique avec un qubit logique qui est corrigé dans la durée et présente une fidélité meilleure que les qubits physiques qui la composent.

Les codes de correction d'erreurs dits qLDPC qui sont inspirés de codes de correction d'erreurs classiques LDPC permettent de réduire le surcoût de la correction d'erreurs d'au moins un ordre de grandeur par rapport au traditionnel code de surface qui était privilégié auparavant. C'est l'approche visée par IBM.

Les développements récents concernant les codes bosoniques correspondent aux qubits dont une partie des erreurs est corrigée nativement au niveau physique. C'est l'approche issue de l'Ecole des Mines et d'Inria avec les travaux de Pierre Rouchon et Mazyar Mirrahimi, qui ont abouti à la création des qubits de chats de la startup Alice&Bob.

D'autres réalisations expérimentales importantes ont été présentées entre 2023 et 2025, notamment avec des atomes froids et des ions piégés. Les premières portes logiques corrigées ont été réalisées tout comme la création des fameux « états magiques ». Il s'agit de la génération d'une porte T [1] à un qubit. Cette

1 La porte T est une porte de phase qui applique un déphasage à l'état du qubit.



I Figure 1 : Un algorithme quantique est représenté par un circuit quantique qui contient des opérations agissant sur les qubits qui sont sérialisées dans le temps. Il y a des portes à un, deux et même trois qubits. La largeur du circuit correspond au nombre de qubits. Sa profondeur correspond au nombre de cycles de portes quantiques. Sachant que l'inaction sur un qubit est assimilable à une opération « identité » qui génère aussi des erreurs. Le taux d'erreur acceptable pour exécuter un tel circuit est l'inverse de sa taille, NxP.

porte quantique est indispensable à la création d'algorithmes générant une accélération exponentielle théorique par rapport aux algorithmes classiques. Mais elle est difficile à créer en mode tolérant aux pannes. La création d'état magique consiste à préparer un qubit logique auquel une transformation de type 'porte T' est appliquée, puis à téléporter cette porte sur un qubit logique distant via une opération tolérante aux pannes, dite transversale, qui n'utilise que des portes « non magiques », peu coûteuses. C'est une logistique assez complexe à mettre en œuvre.

L'estimation des ressources

Un nœud gordien relie les algorithmes quantiques et l'ordinateur quantique : l'estimation des ressources physiques pour le faire tourner convenablement.

Quatre paramètres sont à prendre en compte :

• La dimension de l'algorithme exprimée en taille de circuit, à savoir sa largeur en nombre de qubits multipliée par sa profondeur, c'est-à-dire le nombre de cycles de portes quantiques à réaliser (figure 1). Le taux d'erreurs acceptable des qubits logiques est l'inverse de la taille du circuit, ce qui se comprend assez bien d'un point de vue des probabilités. On ne crée en effet pas de qubits logiques parfaits avec la correction d'erreurs mais des qubits logiques qui ont un certain taux d'erreur compatible avec les besoins algorithmiques. Pour réaliser des simulations chimiques ayant un intérêt industriel, les algorithmes connus contiennent plusieurs milliards de portes quantiques. Cela correspond à des taux d'erreurs « logiques » situés entre 10^{-9} et 10^{-15}.

• L'assemblage des codes de correction d'erreurs utilisés. On en utilise en pratique plusieurs pour corriger différents types d'erreurs, ainsi que pour la création des états magiques déjà décrits.

• La qualité des qubits physiques qui s'exprime en termes de fidélités pour les opérations à un et deux qubits ainsi que pour la mesure. Les mesures des qubits sont utilisées fréquemment par les codes de correction d'erreurs.

• La connectivité physique entre les qubits physiques qui va conditionner l'efficacité des codes de correction d'erreurs. En gros, meilleure est cette connectivité, moins on aura besoin de qubits physiques pour créer des qubits logiques corrigés.

S'y ajoutent divers éléments techniques comme la vitesse des portes quantiques, des mesures quantiques et de la partie classique de la correction d'erreurs, qui doit être réalisée en temps réel. Ces éléments vont conditionner la surcharge temporelle de la correction d'erreur. Elle augmente avec la fidélité des qubits logiques.

On va alors s'intéresser au nombre de qubits physiques nécessaires à la création d'un qubit logique. Il est situé entre une dizaine et plusieurs milliers en fonction de tous ces paramètres. Plus la taille du circuit quantique est grande, plus on aura besoin de qubits physiques par qubit logique.

On le voit ici, la correction d'erreur a un coût significatif. Elle multiple d'un à plusieurs ordres de grandeur la quantité de ressources physiques quantiques et classiques pour la création d'ordinateurs quantiques utiles. Cela peut aussi influencer la consommation d'énergie du processeur quantique.

Le défi de la quantité et de la qualité des qubits

Le rapport dresse donc un état des lieux des technologies de qubits les plus matures et qui sont notamment développées en France. Pour chacune de ces technologies sont alors précisées les avancées dont elles ont fait preuve ainsi que les défis auxquels leur maîtrise est confrontée, leur capacité d'évolution et les feuilles de route qui en résultent. ●●●

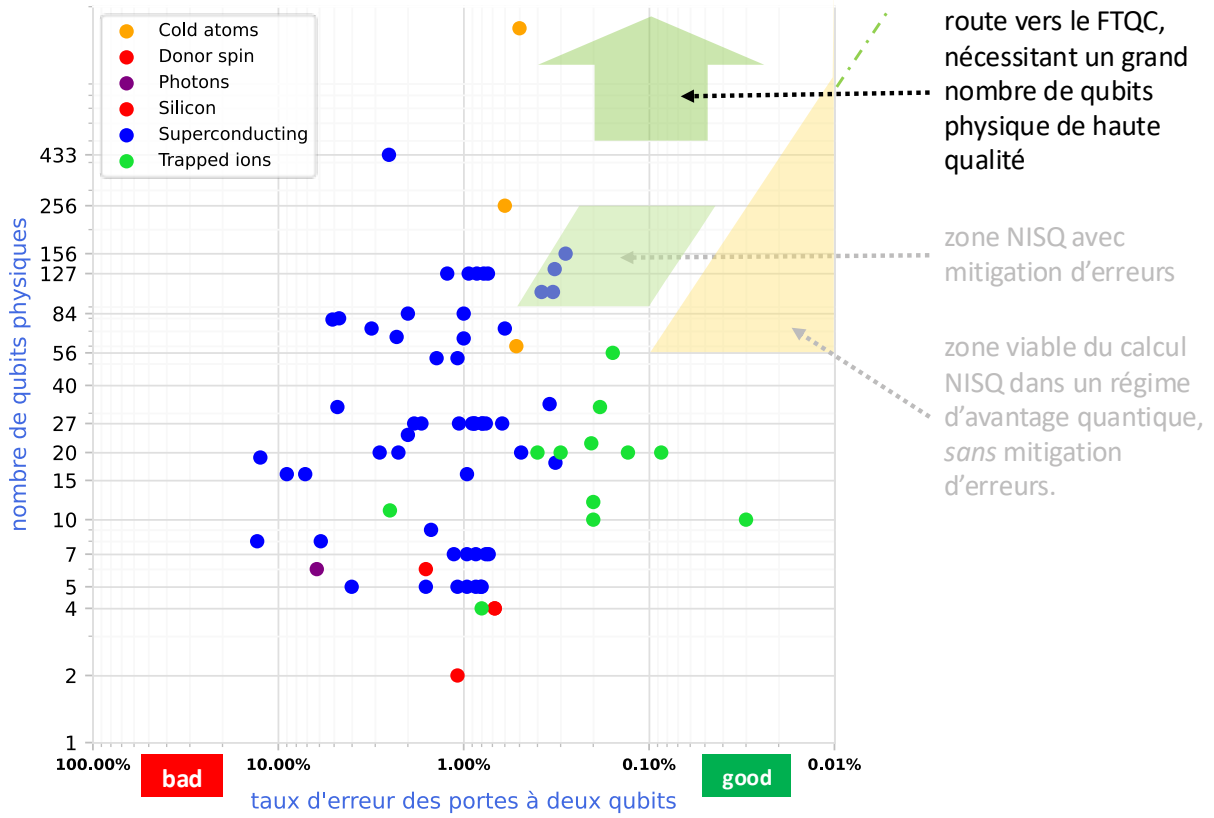


Figure 2 : État des lieux des fidélités des portes à deux qubits physiques actuels par type de qubit sur des processeurs quantiques commerciaux disponibles en général dans le cloud. Les ions piégés ont les meilleures fidélités mais il est pour l'instant difficile d'en contrôler plus d'une cinquantaine. Trois zones importantes y figurent : celle du régime NISQ utile en avantage quantique, où il n'y a pour l'instant personne. Celle du NISQ avec de la mitigation d'erreurs où on trouve notamment IBM. Puis le chemin vers le haut pour atteindre la tolérance aux fautes, qui nécessite un très grand nombre de qubits physiques de haute qualité. © Olivier Ezratty, Août 2025.

Cinq technologies de qubits concurrentes ont été analysées en détail sachant qu'elles ont toutes de nombreuses variantes, qui ont des points forts et des points faibles différents concernant la fabrication et le passage à l'échelle. L'état actuel des connaissances ne permet pas d'en distinguer une comme étant clairement plus avantageuse. Le débat reste ouvert.

"Les défis s'amoncellent en termes de montée à l'échelle. Il faut pouvoir créer des processeurs quantiques avec des milliers de qubits et maintenir leur qualité à un très haut niveau avec des taux d'erreurs de l'ordre de 0,1 %."

Les défis s'amoncellent en termes de montée à l'échelle. Il faut pouvoir créer des processeurs quantiques avec des milliers de qubits et maintenir leur qualité à un très haut niveau avec des taux d'erreurs de l'ordre de 0,1 % (voir figure 2). Or les sources de bruit ont tendance à s'accumuler avec l'augmentation du nombre de qubits et elles sont très variées. Elles détruisent à petit feu la cohérence des registres de qubits, à savoir la superposition et l'intrication qui permettent la puissance du calcul. On a beau refroidir à très basse température les qubits eux-mêmes, comme pour les qubits supraconducteurs et silicium, ou les dispositifs avoisinants comme pour les photons, les atomes froids ou les ions piégés, les sources de bruit sont omniprésentes. Elles peuvent par exemple provenir des imperfections des signaux de contrôle classiques permettant de contrôler et mesurer les qubits comme les bruits de phase ou de fréquence de la génération de signaux électroniques et lasers ou bien des défauts de fabrication des circuits contenant les qubits.

Il est aussi nécessaire de faire monter en échelle toute la logistique du contrôle des qubits : la génération des signaux de pilotage et de lecture des qubits, le câblage et la cryogénie dont on a besoin dans toutes les technologies de qubits, avec des températures allant de 10 mK à 4K. C'est du ressort de ce que l'on appelle les technologies habilitantes et qui sont stratégiques.

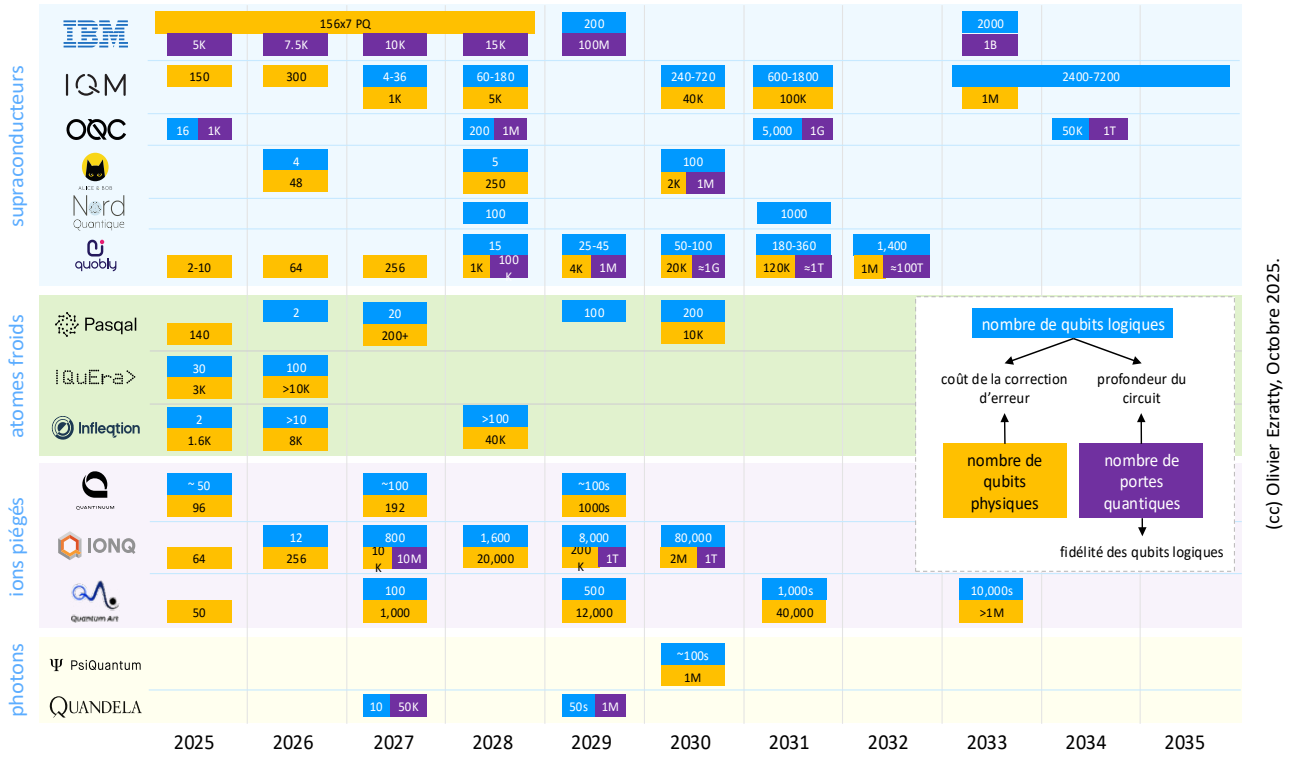


Figure 3 : Consolidation des feuilles de route des principaux constructeurs d'ordinateurs quantique. Les indications portent sur le nombre de qubits logiques (bleu), le nombre de portes quantiques supportées (en violet) et/ou le nombre de qubits physiques associés (orange). Ces trois valeurs permettent d'en déduire la profondeur des circuits quantiques supportés, le coût de la correction d'erreur et la fidélité des qubits logiques. On remarquera que ces trois informations ne sont pas systématiquement publiées. © Olivier Ezratty, Août 2025.

L'interconnexion d'ordinateurs quantiques

Le rapport traite d'un point clé du passage à l'échelle des ordinateurs quantiques à tolérance aux fautes. Pour de nombreuses raisons techniques, on atteindra des limites sur le nombre de qubits qui peuvent être intégrés dans un processeur quantique. Avec les qubits à base de puces microélectroniques comme les qubits supraconducteurs ou en silicium, la variabilité de la qualité des qubits augmente sensiblement avec leur nombre.

La solution envisagée consiste à interconnecter ces processeurs quantiques dans une approche modulaire, à l'aide de liaisons quantiques. Cette interconnexion repose sur la création d'intrication entre qubits distants.

Pour les qubits supraconducteurs, l'interconnexion démarrera avec des liaisons directes entre puces placées sur un même *chiplet* [2] ou sur des câbles flexibles micro-ondes. Les signaux micro-ondes permettent en effet de relier les qubits entre eux.

> **"La solution envisagée consiste à interconnecter ces processeurs quantiques dans une approche modulaire, à l'aide de liaisons quantiques."**

L'autre solution consiste à utiliser des liaisons avec des photons optiques. Elle est particulièrement adaptée aux types de qubits déjà pilotés avec des fréquences optiques comme les atomes, les ions piégés et bien évidemment, les qubits photons eux-mêmes. Pour les autres qubits, il faudra passer de la transduction de signaux entre fréquences microondes et optiques.

Et pour synchroniser tout cela, il faut des mémoires quantiques comme celles de la startup française Welinq. La fidélité de toutes ces opérations est un sujet de préoccupation.

Comme les connexions seront limitées en nombre de qubits reliés entre eux, les compilateurs devront être capables de partitionner les circuits quantiques entre processeurs en tenant compte de cette connectivité limitée. C'est une affaire d'optimisation de graphes.

Le rôle clé du benchmarking

Le rapport de l'Académie des Technologies évoque aussi le rôle du benchmarking. Il est ●●●

2 Plusieurs circuits intégrés soudés sur un même substrat contenant la connectique entre les différents circuits

rendu difficile par la diversité des systèmes, leur maturité encore faible, ainsi que par l'évolution rapide des technologies. L'évaluation des performances pratiques du FTQC pourra exploiter des benchmarks proches d'applications réelles et qui ont du sens pour les utilisateurs finaux industriels [3] sachant que ceux-ci devront aussi intégrer toutes les composantes classiques de la solution.

Le calcul quantique n'est évidemment pas destiné à remplacer le calcul classique, mais à le compléter. Les avantages quantiques seront à rechercher du côté des applications intensives en calcul plutôt que des applications intensives en données. Les technologies FTQC devront aussi se positionner par rapport aux technologies classiques qui ne cessent de progresser, que ce soit au niveau du silicium (3D) ou des algorithmes classiques (par exemple, à base de réseaux de tenseurs).

Enfin, la compréhension des conditions de couplage entre le calcul haute performance (HPC) et le FTQC et les adéquations entre technologies et applications, ainsi que la question d'un éventuel avantage énergétique du FTQC, notamment pour les applications ou FTQC et HPC pourraient être en concurrence.

En conclusion, les défis de la création d'ordinateurs quantiques à tolérance aux fautes sont immenses. Ils mettent en œuvre un très grand nombre de disciplines : de la physique quantique fondamentale, de l'électronique de contrôle, de la photonique micro-ondes ou optique, de la cryogénie, et beaucoup de mathématiques. C'est un mélange de science fondamentale, d'ingénierie d'intégration de systèmes complexes, et de développement technologique. Et surtout, un grand concours de patience et de ténacité. Cela rend le sujet passionnant pour les chercheurs et ingénieurs curieux ! ■

I L'Académie des Technologies a publié en juin 2025 un rapport de 224 pages sur l'état de l'art de l'ordinateur quantique tolérant aux fautes. Il détaille de nombreux points évoqués dans cet article. https://www.academie-technologies.fr/publications/etat-de-lart-de-lordinateur-quantique-tolerant-aux-fautes/

3 Voir l'article à ce sujet dans ce même numéro.

L'auteur

Olivier Ezratty est auteur, enseignant et formateur spécialisé dans les technologies quantiques. Il est notamment l'auteur de l'ouvrage Understanding Quantum Technologies (Septembre 2025, huitième édition) et animateur de deux podcasts sur les technologies quantiques avec Fanny Bouton d'OVHcloud. Il enseigne à l'EPITA, l'ENS Paris-Saclay, CentraleSupelec et divers autres établissements d'enseignement supérieurs. Il est expert auprès de Bpifrance, de l'Agence Nationale de Recherche, de l'Académie des Technologies et de la Commission Européenne. Il est aussi cofondateur de la Quantum Energy Initiative.

Résumé

Cet article synthétise les conclusions d'un rapport de l'Académie des Technologies publié en juin 2025 sur les ordinateurs quantiques tolérants aux fautes (FTQC). Il explore les verrous scientifiques et technologiques à surmonter pour atteindre un avantage quantique pratique dans l'industrie. L'article détaille les cas d'usage industriels les défis à surmonter au niveau des algorithmes quantiques. Il met en lumière les progrès en correction d'erreurs, notamment les codes qui nécessitent moins de qubits physiques, ainsi que les défis liés à la montée en échelle. La qualité et la quantité des qubits physiques sont des facteurs critiques, tout comme leur interconnexion via des liaisons quantiques. Le benchmarking reste complexe mais essentiel pour évaluer les performances réelles. Enfin, le couplage entre calcul classique et quantique, ainsi que les enjeux énergétiques, sont abordés. L'ensemble révèle une discipline multidisciplinaire exigeante, mêlant physique, ingénierie et mathématiques. ■

Abstract

This article summarizes the findings of a report by the French Academy of Technologies published in June 2025 on fault-tolerant quantum computers (FTQC). It explores the scientific and technological challenges that must be overcome to achieve a practical quantum advantage in industry. The article details industrial use cases and the challenges to be overcome in quantum algorithms. It highlights progress in error correction, including codes that require fewer physical qubits, as well as the challenges related to scaling up. The quality and quantity of physical qubits are critical factors, as is their interconnection via quantum links. Benchmarking remains complex but essential to assess real-world performance. Finally, the coupling between classical and quantum computing, as well as energy issues, are addressed. The overall picture reveals a demanding multidisciplinary discipline, combining physics, engineering, and mathematics. ■

Vers un classement mondial des performances des calculateurs quantiques agnostiques aux technologies matérielles

Le projet BACQ (Benchmarks Applicatifs des Calculateurs Quantiques) du programme national MetriQS du LNE

L'étude des performances des calculateurs quantiques s'est dès le début confrontée au fait qu'il n'existait pas de calculateurs quantiques sur lesquels les algorithme les plus puissants comme l'algorithme de Shor pouvaient être testés. La performance était uniquement déterminée théoriquement à partir des caractéristiques de l'Algorithme. Aujourd'hui la puissance des calculateurs permet d'établir des méthodes pour comparer les performances des algorithmes quantiques. Le projet BACQ a pour objectif d'établir des principes de mesures de performances indépendante des calculateurs.

Frédéric Barbaresco
Leader du segment « Algorithmes et calculs quantiques » (THALES)

Félicien Schopfer
Responsable du programme MetriQs (LNE)

Emmanuelle Vergnaud
Responsable TQCI (TERATEC)

Introduction

L'informatique quantique promet de révolutionner de nombreux domaines techniques et secteurs d'activité, de l'optimisation dans la logistique à la simulation pour la recherche en physique ou en chimie, en ingénierie ou dans l'industrie, en passant par la cryptographie. Mesurer les progrès vers l'avantage quantique et la réalisation de ces promesses, avec objectivité et fiabilité, est d'un grand intérêt pour les utilisateurs finaux potentiels et crucial pour le développement futur du domaine, aujourd'hui sujet à un battage médiatique et à une forte concurrence. Les défis, notamment pour parvenir à des mesures comparables, proviennent de la diversité des plateformes matérielles, de leurs spécificités en termes de caractéristiques physiques et d'applications, de leur maturité qui peut encore être faible et de l'évolution potentielle rapide des technologies.

Plusieurs initiatives existent pour comparer les performances des ordinateurs quantiques. On peut citer par exemple Quantum VOLUME et CLOPS d'IBM, SupermarQ de Super-Tech ou Quantum LINPACK de Berkeley Lab. Les métriques utilisées dans les approches précédentes sont très techniques et nécessitent une familiarité avec la technologie. Elles ne permettent donc pas de dériver des indicateurs opérationnels des performances des différentes familles d'algorithmes exécutés sur les différents ordinateurs quantiques existants. Dédié à la mise en place de l'ensemble de la chaîne de valeur depuis le développement du matériel quantique jusqu'aux cas d'utilisation industrielle, le projet de benchmarks BACQ est complémentaire des initiatives de benchmarking, se concentrant uniquement sur les critères physiques du matériel de bas niveau. La suite de benchmarks envisagée sera basée sur la résolution de plusieurs classes de problèmes couvrant des domaines d'application importants de l'informatique quantique qui ont du sens pour les utilisateurs industriels (voir figure 1) : simulation de modèles de physique quantique, optimisation, résolution de systèmes linéaires et factorisation en nombres premiers. L'apprentissage automatique pourrait être inclus dans le domaine d'application de l'optimisation.

Ces problèmes sont génériques et pourraient être pertinents pour différentes branches d'industries et de services (chimie, aéronautique, électronique et énergie par exemple). Des critères seront définis pour la résolution de chaque problème, certains étant agnostiques au matériel et d'autres dépendants du matériel (bas niveau) : temps de calcul, latence, taille du problème, taux d'approximation, probabilité de résolution, précision, fidélité… Il est important de noter que le projet prend également en compte des critères énergétiques pour l'évaluation des performances énergétiques des machines.

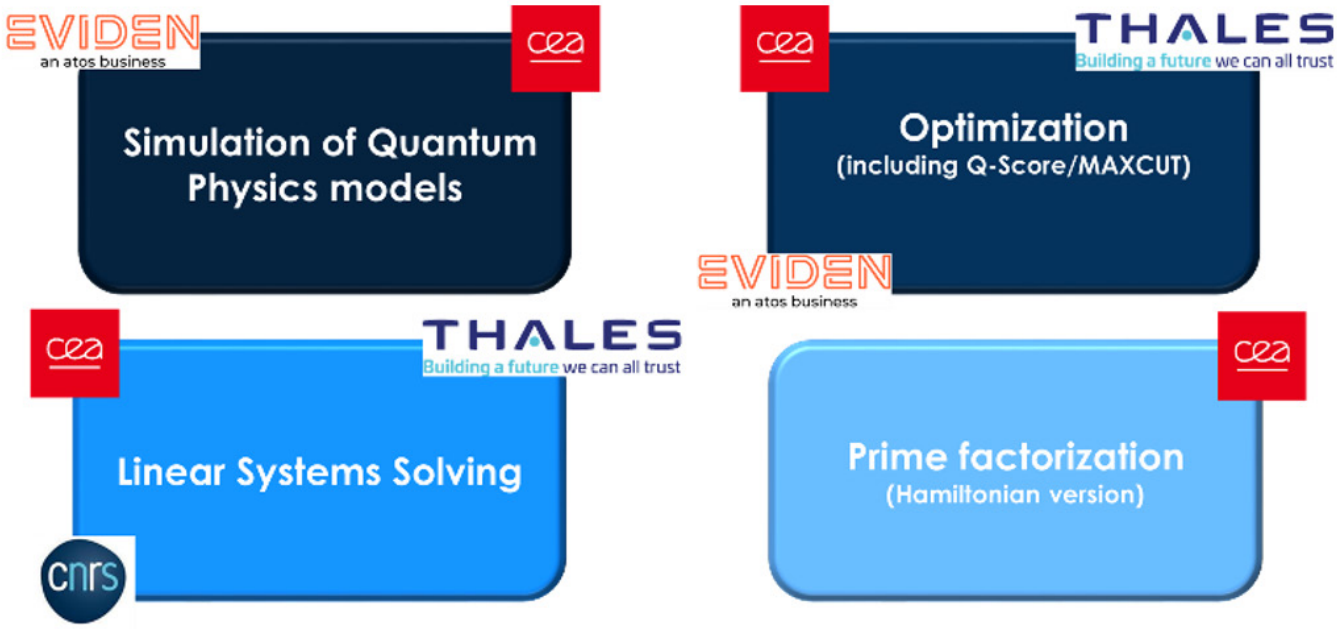


Figure 1 : Familles de problèmes utilisés pour le benchmark QPUs.

La méthodologie proposée consiste en l'agrégation de mesures techniques de bas niveau et une analyse multicritère via l'outil MYRIAD-Q afin de fournir des indicateurs de performance opérationnelle des différentes solutions de calcul quantique et de souligner les qualités de service intéressantes pour les utilisateurs finaux. L'agrégation des critères et l'analyse multicritère permettent des notations entièrement explicables et transparentes, des comparaisons entre différentes machines quantiques et avec des ordinateurs classiques, ainsi que l'identification des avantages pratiques de chaque machine quantique par rapport à des applications spécifiques. Le projet portera à la fois sur les machines analogiques (simulateurs et recuits quantiques) et les machines à portes, le *Noisy Intermediate Scale Quantum* (NISQ) et le *Fault Tolerant Quantum Computing* (FTQC). L'approche pratique suivie consiste à disposer d'une série de benchmarks, adaptatifs dans une certaine mesure, appropriés aux capacités des machines disponibles et capables de démontrer leurs avantages respectifs, y compris, à plus long terme, l'accélération exponentielle d'algorithmes spécifiques sur les machines FTQC.

Dans le cadre du projet, une première action a déjà été lancée concernant Q-Score, où Eviden a développé le problème d'optimisation MAXCUT, pour tester et valider le benchmark sur différents types de machines quantiques.

Au début du projet, les machines dont l'accès est visé seront principalement le « Très Grand Centre de Calcul du CEA » (TGCC est une infrastructure de calcul scientifique de haute performance. Nous explorerons également toutes les opportunités d'accès aux machines via des accords entre GENCI/CEA et EuroHPC et les entités d'hébergement QC ou des organisations internationales, ou directement avec les fournisseurs de QPU. L'entreprise commune EuroHPC a signé des accords d'hébergement avec dix sites à travers l'Europe pour héberger et exploiter les ordinateurs quantiques EuroHPC. Ces ordinateurs quantiques permettront aux utilisateurs européens d'explorer une variété de technologies quantiques couplées à des supercalculateurs de pointe.

Objectifs du Programme MetriQs-France

MetriQs-France est le programme national de mesure, d'évaluation et de normalisation des technologies quantiques. L'objectif de MetriQs-France est de développer, d'exploiter et de promouvoir des capacités de mesure de référence, validées et harmonisées, pour la caractérisation et l'évaluation des performances des technologies quantiques avec fiabilité, impartialité et comparabilité : la métrologie, les tests et l'évaluation, la normalisation internationale sont au cœur du programme. MetriQs-France est coordonné par le LNE, le laboratoire national de métrologie et d'essais, établissement public sous tutelle du ministère de l'Économie et des Finances, en charge de l'industrie.

Objectifs du Projet BACQ

En regardant vers l'avenir, il est essentiel de mesurer les progrès vers la réalisation des promesses de l'informatique quantique. Des benchmarks orientés vers les applications, permettant d'évaluer les performances réelles de l'informatique quantique du point de vue de l'utilisateur, semblent utiles dans cette perspective. Le défi vient de la diversité des plateformes matérielles, de leurs spécificités en termes de caractéristiques physiques et d'applications, de leur maturité et de l'évolution rapide potentielle de la technologie. Développer un instrument de mesure objectif, pérenne et largement partagé, pour servir de référence commune.

L'évaluation des performances pratiques de l'informatique quantique sera réalisée à travers des benchmarks proches des applications réelles, utiles aux utilisateurs finaux industriels (et académiques). L'objectif principal est de mesurer les progrès vers un avantage quantique pratique. À cet égard, le consortium prévoit d'effectuer des comparaisons entre les différentes solutions de calcul quantique ainsi que de les comparer aux ordinateurs classiques actuels. Cette initiative de benchmarking mettra à terme les atouts de chaque solution de calcul quantique compte tenu des applications spécifiques.

La suite de benchmarks résultant de ce projet sera maintenue par le LNE, un tiers indépendant et de confiance. Grâce à leur interaction avec la communauté des utilisateurs finaux, cet outil sera exploité afin d'analyser les résultats obtenus par les machines testées avec les différents benchmarks en utilisant l'outil d'agrégation explicable. Le LNE établira une liste de performances, la maintiendra dans le temps et mettra à jour la définition des tests. De plus, l'adoption de cette initiative par des partenaires français, européens et éventuellement internationaux sera encouragée grâce au développement d'outils de communication sur la démarche suivie et de représentations visuelles de l'agrégation des résultats obtenus par les machines des différents benchmarks. Les dialogues et collaborations internationaux sur le sujet du benchmarking des ordinateurs quantiques seront favorisés afin que l'approche, soutenue par MetriQs-France, soit et reste une référence internationale. Ce projet BACQ favorise le développement d'une normalisation internationale concernant les méthodes utilisées pour évaluer les spécifications des machines quantiques.

Description du projet BACQ

L'objectif de cette section est de présenter les travaux prévus au cours du projet. Le projet est organisé autour de six tâches.

" En regardant vers l'avenir, il est essentiel de mesurer les progrès vers la réalisation des promesses de l'informatique quantique. Des benchmarks orientés vers les applications, permettant d'évaluer les performances réelles de l'informatique quantique du point de vue de l'utilisateur, semblent utiles dans cette perspective. "

Définition des tests de référence

En s'appuyant sur l'état de l'art sur les différents benchmarks, l'objectif de cette tâche est d'identifier les différents critères et les approches algorithmiques associées. Pour cela, les partenaires contribueront à identifier les critères et à les répartir en différentes classes (critères liés au problème abordé par un benchmark, critères liés à la méthode ou aux différentes méthodes de calcul et critères liés aux ordinateurs). Enfin, la tâche identifie l'approche multicritère générique permettant la construction d'un score agrégé.

Comme indiqué dans l'introduction, l'ensemble des benchmarks est divisé en quatre catégories : problèmes d'optimisation, résolution de systèmes linéaires, simulations de physique quantique et factorisation en nombres premiers.

Les sections suivantes décrivent chacune des quatre familles de référence.

Optimisation

L'optimisation est un domaine pour lequel l'informatique quantique est considérée comme la plus adaptée pour des applications industrielles à court et moyen terme. Néanmoins, on pense également que l'ensemble des problèmes résolubles en temps polynomial sur un ordinateur quantique (BPQ) est différent de la classe des problèmes dits NP, il ne faut donc pas avoir d'attentes irréalistes concernant les approches de l'informatique quantique. Cependant, il s'agit d'un domaine d'application de l'informatique quantique de la plus haute importance, car il peut améliorer le temps de résolution, ou la qualité de la solution approximative, ou, plus important encore, l'énergie nécessaire pour atteindre un niveau de qualité donné pour une solution.

La famille de problèmes et de programmes d'optimisation s'articulera autour de 3 à 4 séries de problèmes :

MaxCut (dans le cadre du QScore d'Eviden), comme exemple de modèle binaire quadratique NP-dur sans contrainte,

Correspondance de cardinalité maximale, comme exemple de problème de contrainte polynomiale qui est réputé difficile pour les approches de recuit,

Problèmes d'optimisation binaire d'ordre supérieur (HOBO), qui ne sont pas nécessairement NP-difficiles, mais qui sondent le cas de problèmes non quadratiques qui peuvent être importants dans le cas général, par exemple,

En option, quelques problèmes contraints NP-difficiles.

Systèmes linéaires

L'algèbre linéaire en général fournit un ensemble de problèmes qui sont aussi importants que les problèmes d'optimisation en termes d'applications, et est un domaine où le calcul quantique idéal a une accélération exponentielle connue. Bien qu'il soit clair qu'aucun avantage de calcul exponentiel à court terme ne peut être attendu, il reste un domaine important à étudier.

●●● À cet effet, deux séries d'applications se distinguent :

Résolution de systèmes linéaires, qui est l'ensemble pour lequel HHL sera l'algorithme le plus pertinent pour les QPU basés sur des portes.

Valeurs propres – vecteurs propres d'une matrice donnée, car il s'agit d'une famille d'applications dans laquelle certains algorithmes hybrides comme l'algorithme résolveur variationnel VQE pourraient être appliqués.

Pour le moment, VQE est déjà connu comme une famille d'algorithmes qui peuvent être une application potentielle à court terme de l'informatique quantique.

Simulations de physique quantique

Les problèmes de physique quantique se posent dans de nombreux domaines scientifiques. Par exemple, en physique du solide, la compréhension de nouveaux phénomènes quantiques et la conception de nouveaux matériaux avec des applications potentielles nécessitent souvent de simuler des problèmes quantiques avec de nombreux électrons. La physique quantique avec de nombreux électrons joue également un rôle central en chimie. Ce sont également des problèmes centraux dans d'autres domaines de la recherche fondamentale, comme en physique des particules ou en physique nucléaire ou encore en théorie de l'information quantique. Parmi les hamiltoniens à plusieurs corps simples mais non triviaux définis sur des réseaux, on peut citer les modèles quantiques à spin 1/2 (interactions de Heisenberg, modèle d'Ising en champ transverse, …) les modèles à fermions sans spin, les modèles à fermions à spin 1/2 (modèle de Hubbard) ou les modèles à bosons (ex : Bose-Hubbard). La simulation de ces systèmes quantiques à plusieurs corps est notoirement difficile sur un ordinateur classique, pour la même raison qu'un ordinateur quantique est plus puissant qu'un ordinateur classique, à savoir que la dimension de l'espace de Hilbert d'un système quantique croît exponentiellement avec le nombre de particules. Cependant, avec un simulateur quantique analogique ou avec un ordinateur quantique numérique (à portes), on pourrait en principe étudier des systèmes à plusieurs corps qui sont intraitables sur une machine classique.

" En physique du solide, la compréhension de nouveaux phénomènes quantiques et la conception de nouveaux matériaux avec des applications potentielles nécessitent souvent de simuler des problèmes quantiques avec de nombreux électrons."

Dans ce contexte, on peut mentionner deux tâches distinctes : 1) à partir d'un hamiltonien donné H, déterminer les valeurs attendues de certaines observables (y compris de H lui-même) dans l'état fondamental de H ; 2) étant donné un état initial simple (produit) $|\psi_0\rangle$, déterminer les valeurs attendues de certaines observables dans l'état évolué dans le temps $|\psi_t\rangle = \exp(-iHt/\hbar)|\psi_0\rangle$.

Factorisation en nombres premiers

La découverte de l'algorithme de Shor pour la factorisation en nombres premiers est l'un des résultats qui a suscité d'immenses attentes de la part de l'informatique quantique. Bien qu'il soit clairement irréaliste de s'attendre à ce que cet algorithme particulier puisse être appliqué sans avoir au préalable développé des ordinateurs quantiques tolérants aux pannes, il existe d'autres approches possibles. L'une d'elles consiste à utiliser des approches basées sur l'Hamiltonien. Le principe de base est assez simple car il nécessite simplement la minimisation de la fonction de coût suivante :

$$C(p_1,p_2)=(N-p_1\,p_2)^2$$

Où p_1 et p_2 sont 2 nombres premiers possibles qui doivent être trouvés et N est l'entier qui fait l'objet de la factorisation première.

Les approches qui ne sont pas basées sur l'algorithme de Shor ne devraient pas fournir un quelconque avantage informatique, mais il n'est pas exclu pour le moment qu'elles puissent fournir un quelconque avantage du côté énergétique.

Critère énergétique par estimation des ressources pour la résolution d'algorithmes simples sur des ordinateurs à portes

Pour une tâche donnée, l'efficacité énergétique peut être définie de manière paramétrique comme la mesure choisie pour quantifier la performance de la tâche, divisée par son coût énergétique. L'efficacité dépend donc étroitement du choix de la mesure, ainsi que de la liste des coûts énergétiques.

L'objectif de la tâche est de proposer et d'étudier le comportement de telles efficacités énergétiques pour certains des algorithmes utiles étudiés dans ce projet. En principe, toutes les machines peuvent donner lieu à de telles figures de mérite. Notre approche s'appuiera sur la méthodologie MNR introduite, qui consiste à trouver des relations entre le bruit, la métrique de performance et le coût des ressources, puis à exploiter ces relations pour minimiser le coût des ressources sous la contrainte d'une performance donnée.

Dans l'esprit du projet BACQ, nous veillerons à rester aussi agnostiques que possible en termes de matériel pour proposer

Les auteurs

Frédéric Barbaresco, responsable du segment « Algorithmes et Calculs Quantiques » au sein de la Direction Technique. Il est chargé de coordonner les activités de recherche et technologie (R&T) dans le domaine des algorithmes quantiques à travers les lignes de métier et les laboratoires cortAIx, ainsi que de favoriser les partenariats avec des start-ups DeepTech et des laboratoires académiques dans ce domaine. Il gère les collaborations avec les start-ups du programme PROQCIMA, ainsi que les études avancées en France (AID, Pack IdF, MoD, ...) et en Europe (ESA, SESAR, ...). Il est le représentant français au sein du groupe SET-IST-339 de l'OTAN sur « L'étude des applications militaires des algorithmes quantiques ». Il coordonne le projet BACQ (Benchmarks appliqués pour le calcul quantique) au sein du programme national MetriQs du LNE. Il est le représentant français du EQCBC (Comité Européen de Coordination du Benchmarking pour l'Informatique Quantique). Il a été coordinateur du sous-groupe GIFAS sur le « Calcul Quantique », qui a remis son rapport en 2024, et il a contribué au rapport de l'« Académie des Technologies » sur le calcul quantique tolérant aux fautes (FTQC). Il occupe le poste de General Chair de la conférence SEE QUEST-IS (Quantum Engineering for Science and Technology – Industry & Services), qui se tiendra à Paris en 2025. Il a été récompensé par le prix Aymée Poirson 2014 de l'Académie des Sciences pour l'application de la science à l'industrie.

Félicien Schopfer a obtenu le diplôme d'ingénieur de l'École Nationale Supérieure de Physique—Grenoble INP, Grenoble, France, en 2001, ainsi que le master en physique de la matière condensée de l'Université de Grenoble, Grenoble, en 2001. Il a également obtenu le doctorat en physique de l'Université de Grenoble, Grenoble, en 2005, pour ses travaux expérimentaux sur le transport électronique quantique dans des nanostructures réalisés au CNRS, Grenoble, France. Il a été nommé au Laboratoire National de Métrologie et d'Essais (LNE), Trappes, France, en 2005, afin de faire progresser la recherche en métrologie électrique quantique. Ses recherches se sont principalement concentrées sur l'effet Hall quantique (EHQ) pour des applications en métrologie fondamentale. Il a travaillé sur des réseaux Hall quantiques dans des structures GaAs/AlGaAs, a coécrit des tests de reproductibilité et d'universalité de l'effet Hall quantique avec des incertitudes records, et il est fortement impliqué dans la recherche sur le graphène, notamment avec des résultats importants pour le développement de la norme de résistance Hall quantique fonctionnant dans des conditions expérimentales assouplies. Il est responsable au LNE du programme MetriQs de benchmark des technologies quantiques.

Emmanuel Vergnaud Direction des Opérations à TERATEC. Emmanuelle Vergnaud coordonne les séminaires TQCI (Teratec Quantum Computing Initiative) dédiés à l'échange autour des différentes initiatives de benchmarking des calculateurs quantiques et plus particulièrement celles dédiées aux applications (https://teratec.eu/activites_quantiques/seminaires_TQCI.html). Elle coordonne le WP1 du projet BACQ dédié aux interactions et communications vers l'écosystème quantiques, en particuliers les échanges avec les strat-ups du programme PROQCIMA.

des outils numériques utiles et flexibles aux utilisateurs finaux et aux industriels. L'accent sera ainsi mis sur les ressources algorithmiques, le lien avec les coûts énergétiques étant traité via des modèles efficaces. En lien étroit avec le projet HQI de la stratégie quantique française, nous construirons une interface conviviale accessible à tout fournisseur de matériel pour estimer l'efficacité énergétique du processeur quantique en jeu.

> **" Le projet BACQ utilise une approche de décision multicritères afin d'agréger les métriques élémentaires en qualité de service de plus haut niveau, facilement interprétable par un utilisateur final des calculateurs quantiques, sans compétence spécifiques du domaine."**

MYRIAD-Q : Outil d'agrégation des métriques et de décision multicritère

Le projet BACQ utilise une approche de décision multicritères afin d'agréger les métriques élémentaires en qualité de service de plus haut niveau, facilement interprétable par un utilisateur final des calculateurs quantiques, sans compétence spécifiques du domaine.

Concepts de base

On nous donne un ensemble $N=\{1,...,n\}$ de métriques représentées $X_1,\ldots,X_n$ respectivement par des espaces. Les solutions quantiques que nous considérons sont caractérisées par une valeur sur chaque métrique, et sont donc considérées comme un élément de $X=X_1\times\cdots\times X_n$. Le but de l'Aide à la Décision Multicritère (AMDC) est de déterminer comment l'élément de Xdoit être comparé, formalisé par une relation dite de préférence $\succcurlyeq$ sur X. Pour deux alternatives $x,y\in X$, « $x\succcurlyeq y$» signifie que « x est au moins aussi préféré que y ». Il est important de définir une telle relation binaire $\succcurlyeq$ pour nécessairement intégrer les préférences de certains experts ou décideurs. La comparaison des options dépend clairement des métriques les plus importantes, de l'intérêt d'améliorer la valeur d'une métrique d'une unité, etc. ●●●

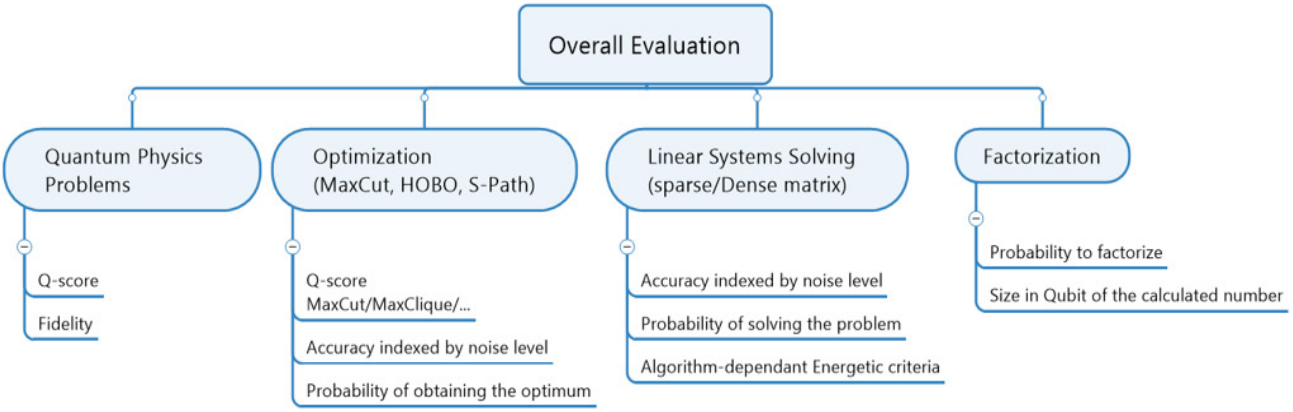


Figure 2 : Esquisse d'une hiérarchie de critères.

L'AMDC vise donc à capturer les préférences des DM (décideurs).

Nous cherchons une représentation numérique $u:X\to S$ de la préférence avec $S\subseteq R$ une échelle telle que $x\succcurlyeq y$ si et seulement si $u(x)\geq u(y)$. La construction de unécessite deux opérations différentes, à savoir normaliser les métriques car elles sont données dans des unités différentes (par exemple un temps en secondes contre une consommation en Watt) et agréger les différentes métriques pour aboutir à un score unique. Ces deux opérations sont ensuite effectuées séparément dans le modèle dit décomposable : pour $x=(x_1,\dots,x_n)$, nous écrivons $u(x)=F(u_1(x_1),\dots,u_n(x_n))$, où $u_i:X_i\to S$ est la fonction d'utilité marginale sur la métrique i, et $F:S^n\to S$ est une *fonction d'agrégation*. On appelle critère la fonction d'utilité u_i attachée à une métrique.

Le nombre de métriques étant généralement important ($\gg 2$), les sorties des critères sont agrégées via une hiérarchie. L'idée est d'introduire plusieurs fonctions d'agrégation imbriquées. Chaque nœud d'agrégation intermédiaire introduit un score intermédiaire, qui a une signification pertinente pour l'utilisateur et facilite la phase d'élicitation. La figure 2 montre une organisation possible des critères. Au premier niveau, on retrouve les différents problèmes que l'on évalue puis la liste des métriques pour chaque problème.

L'échelle S est généralement choisie pour être limitée – ce $S=[0,1]$ qui signifie généralement qu'il existe une valeur de la métrique au-dessus de laquelle (en dessous de laquelle respectivement) les critères sont parfaitement (ou presque parfaitement) satisfaisants (pas du tout, respectivement). Cependant, l'objectif de MYRIAD-Q n'est pas seulement d'évaluer les technologies quantiques actuelles, mais de proposer un module d'évaluation qui sera utilisé pour plusieurs années. Cependant, nous ne pouvons pas prévoir aujourd'hui les niveaux qui seront atteints dans plusieurs années. L'utilisation d'une échelle bornée ne permet pas d'utiliser le même modèle sur plusieurs années. Nous proposons donc d'utiliser l'échelle unipolaire $S=[0,+\infty)$pour laquelle il existe une borne inférieure mais pas de borne supérieure a priori sur la performance.

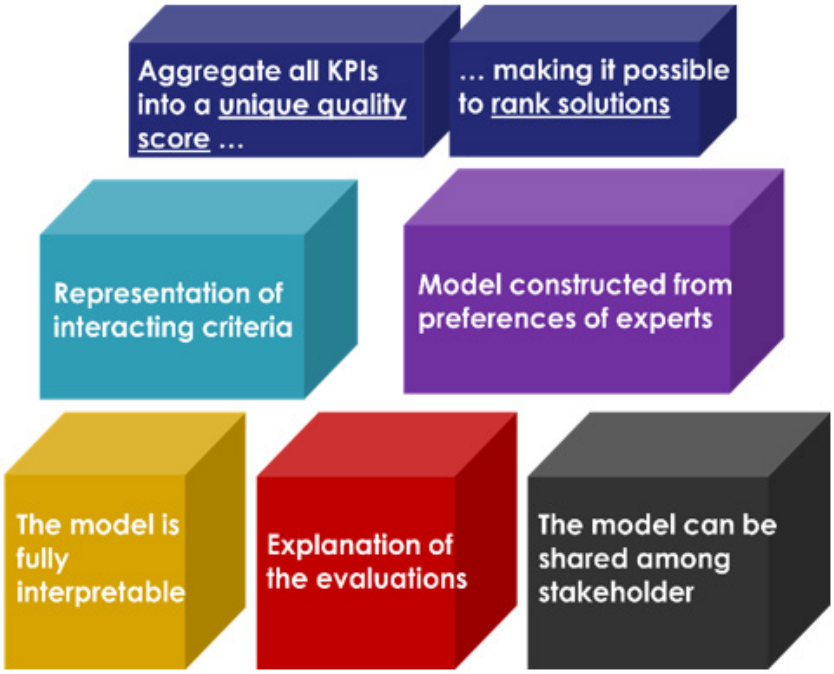


Figure 3 : Principaux avantages du MYRIAD-Q pour les utilisateurs finaux du QPU.

Les principaux avantages de l'approche multicritère MYRIAD-Q sont illustrés dans la figure 3.

Perspectives européennes

Le Comité européen de coordination de l'évaluation comparative de l'informatique quantique (EQCBC) a publié un document offrant un aperçu complet de l'état actuel et des recommandations pour une évaluation comparative systématique des ordinateurs quantiques. Ce document aborde les évaluations comparatives aux niveaux composant, système, logiciel, HPC et application. Les recommandations pour les étapes futures soulignent la nécessité de développer des routines d'évaluation standardisées et d'intégrer les évaluations comparatives aux activités plus larges liées aux technologies quantiques. L'EQCBC a publié un « *white paper* » sur le sujet. ■

Remerciements

Nous remercions les contributions de l'ensemble des partenaires : Alexia Auffèves (CNRS), Baptiste Anselmemartin (EVIDEN), Cyril Allouche (EVIDEN), Damien Nicolazic (EVIDEN), Gregoire Misguich (CEA), Harshit Verma (CNRS), Marie-Pierre Jaffrezic (LNE), Kkyrylo Snizhko (CEA), Christophe Labreuche (THALES), Michel Nowak (THALES), Olivier Hess (EVIDEN) Olivier Noé (THALES), Laurent Rioux (THALES), Robert Wang (EVIDEN), Robert Whitney (CNRS), Stephane Louise (CEA), Harold Erbin (CEA) et Dalbert Benoit (CEA).

Résumé

Initié en septembre 2023, le projet BACQ constitue la première entreprise de recherche et développement issue du programme METRIQs-France, lequel s'inscrit dans le cadre de la Stratégie nationale quantique, placée sous l'égide du LNE et spécifiquement consacrée aux missions de métrologie, d'évaluation et de normalisation des technologies quantiques. Rassemblant autour de lui Eviden, le CEA, le CNRS, Teratec, le LNE, ainsi que Thales, à qui incombe la direction opérationnelle, ce projet a pour finalité l'établissement de référentiels de comparaison (*benchmarks*) destinés à mesurer les performances des calculateurs quantiques en les confrontant à des applications concrètes, porteuses de sens pour les utilisateurs finaux. La difficulté majeure réside dans la très grande hétérogénéité des plateformes matérielles : chacune présente en effet des spécificités propres, qu'il s'agisse de leurs caractéristiques physiques, de leurs champs d'applications, de leur degré de maturité ou encore de l'évolution technologique, rapide et potentiellement disruptive, qui les affecte.

Afin de dégager des indicateurs opérationnels de haut niveau, susceptibles d'attribuer une véritable valeur comparative aux performances des ordinateurs quantiques, le projet s'attache à agréger un ensemble de métriques tant calculatoires qu'énergétiques, toutes relatives à la résolution de problèmes concrets, couvrant un large éventail de domaines : optimisation, résolution de systèmes linéaires, simulation en physique et factorisation. Parmi ces métriques figure notamment le Q-score, conçu par Eviden pour l'évaluation de la résolution du problème d'optimisation MaxCut. Dans une perspective d'ouverture et de diffusion la plus large possible, BACQ nourrit l'ambition de proposer, à terme, un corpus de benchmarks accessible librement et susceptible d'être implémenté sur toute catégorie de calculateurs quantiques. ■

Abstract

Initiated in September 2023, the BACQ project is the first research and development initiative resulting from the METRIQs-France program, which is part of the National Quantum Strategy, under the aegis of the LNE and specifically dedicated to the metrology, evaluation, and standardization of quantum technologies. Bringing together Eviden, the CEA, the CNRS, Teratec, the LNE, and Thales, which is responsible for operational management, this project aims to establish benchmarks to measure the performance of quantum computers by comparing them to concrete applications that are meaningful to end users. The major challenge lies in the extreme heterogeneity of hardware platforms: each has its own specificities, whether in terms of their physical characteristics, their fields of application, their degree of maturity, or the rapid and potentially disruptive technological developments affecting them.

In order to identify high-level operational indicators capable of providing a truly comparative value to the performance of quantum computers, the project aims to aggregate a set of computational and energy metrics, all related to the solving of concrete problems, covering a wide range of fields: optimization, linear system resolution, physics simulation, and factorization. These metrics notably include the Q-score, designed by Eviden to evaluate the resolution of the MaxCut optimization problem. With a view to openness and the widest possible dissemination, BACQ aims to eventually offer a body of benchmarks that is freely accessible and can be implemented on any category of quantum computers. ■