

État de l'art de l'ordinateur quantique tolérant aux fautes

Questions et défis

Rapport de l'Académie



Académie des technologies
Le Ponant — Bâtiment A
19, rue Leblanc
75015 PARIS

+33(0)1 53 85 44 44

secretariat@academie-technologies.fr
www.academie-technologies.fr

© Académie des technologies
ISBN : 979-10-97579-63-0

Couverture : EnigmaEasel - Adobe stock

ÉTAT DE L'ART DE L'ORDINATEUR QUANTIQUE TOLÉRANT AUX FAUTES

QUESTIONS ET DÉFIS

Rapport de l'Académie

Ce rapport a été rédigé sous la direction de Catherine LAMBERT, Thierry BONHOMME et Gérard ROUCAIROL.

Il est le produit d'un groupe de travail dont la composition complète est précisée en annexe. Il répond à un processus rigoureux au sein de l'Académie des technologies garantissant son indépendance et son objectivité; il a été approuvé et voté lors de l'Assemblée générale des académiciens.

SOMMAIRE

| | |
|---|----|
| Contexte | 6 |
| Résumé exécutif | 7 |
| Executive Summary | 12 |
| Introduction | 16 |
| Chapitre 1 | |
| La réalité de l'avantage quantique et ses besoins | 21 |
| 1.1. Algorithme quantique | 21 |
| 1.2. Ordinateur universel | 23 |
| 1.3. Calcul tolérant aux fautes | 24 |
| 1.4. Complexité théorique | 26 |
| 1.5. Accélération quantique | 28 |
| 1.6. Heuristiques et approches empiriques | 31 |
| 1.7. Cas d'usage | 32 |
| Chapitre 2 | |
| Les codes correcteurs d'erreurs | 44 |
| 2.1. La tolérance aux fautes, seule voie vers des algorithmes quantiques profonds | 44 |
| 2.2. Correction d'erreurs et tolérance aux fautes | 46 |
| 2.3. Le principe de la correction d'erreur quantique | 48 |
| 2.4. L'Âge d'or du code de surface | 49 |
| 2.5. De nouvelles approches moins gourmandes en <i>hardware</i> | 54 |
| 2.6. Les défis à venir | 63 |

| | |
|--|-----|
| Chapitre 3 | |
| Les technologies de qubits : défis et feuilles de route | 65 |
| 3.1. Atomes neutres | 73 |
| 3.2. Qubits supraconducteurs | 86 |
| 3.3. Photons | 101 |
| 3.4. Spins dans le silicium | 117 |
| 3.5. Ions piégés | 133 |
| Chapitre 4 | |
| Le passage à l'échelle des calculateurs quantiques | 146 |
| 4.1. La <i>scalabilité</i> par la modularité | 147 |
| 4.2. Interconnexion photonique | 154 |
| 4.3. <i>Scalabilité</i> et connectivité des qubits supraconducteurs | 167 |
| Chapitre 5 | |
| Éléments complémentaires | 178 |
| 5.1. Introduction | 178 |
| 5.2. Analyse technico-économique de l'écosystème - Comparaisons historiques | 178 |
| 5.3. Quelques questions | 181 |
| 5.4. Développement des technologies concurrentes à l'horizon des premiers FTQC ? | 184 |
| 5.5. <i>Benchmarks</i> orientés applications | 187 |
| 5.6. Liens avec le calcul haute performance | 193 |
| 5.7. Capital humain | 199 |
| 5.8. Stratégies de financement | 200 |
| Conclusion | 202 |
| Annexes | 203 |
| A. Glossaire | 204 |
| B. Membres du groupe de travail | 220 |
| C. Personnes auditionnées | 222 |

Contexte

Ce rapport est rédigé par un comité créé par l'Académie des technologies avec pour objectif de produire un document de référence, complété et mis à jour annuellement, évaluant la faisabilité et l'impact du calcul quantique tolérant aux fautes (*Fault Tolerant Quantum Computing - FTQC*). En particulier, il vise à identifier les verrous scientifiques, technologiques et économiques, à préciser les cas d'usage, le potentiel de création de valeurs, les liens avec le calcul haute performance (HPC : *High Performance Computing*) et les horizons de temps.

Ce premier rapport se concentre sur l'état des lieux des technologies de qubits développées en France, sur l'état de l'art des démonstrations de corrections d'erreur, ainsi que sur les approches permettant le passage à l'échelle des technologies de calcul quantique tolérant aux fautes. À ce titre il fait suite à une étude réalisée pour le Secrétariat général pour l'Investissement par l'Académie des technologies. Il ne traite pas la question de l'intérêt stratégique et économique potentiel que représenterait la construction d'un tel ordinateur, sujet qui sera abordé dans un futur rapport.

En 2019 aux États-Unis, les « *National Academies of Sciences, Engineering, and Medicine* » publiaient un rapport¹ sur l'état de l'art des calculateurs quantiques. À l'image du rapport américain, ce rapport de l'Académie des technologies de France correspond à une initiative rare au niveau mondial pour proposer un tour complet d'horizon sur ce sujet difficile qu'est l'utilisation de la mécanique quantique pour le calcul quantique tolérant aux fautes.

1 « Quantum Computing: Progress and Prospects (2019) » - <https://nap.nationalacademies.org/catalog/25196/quantum-computing-progress-and-prospects>

Résumé exécutif

Ce rapport présente les résultats d'une étude collective menée par un Groupe de Travail créé en juin 2023 par l'Académie des technologies pour évaluer la faisabilité et l'impact du calcul quantique tolérant aux fautes (*Fault Tolerant Quantum Computing - FTQC*). Il fait suite à une étude réalisée pour le Secrétariat général pour l'Investissement (SGPI).

Le rapport revient d'abord sur les notions d'algorithme quantique, d'avantage quantique calculatoire, et décrit comment cet avantage varie selon les algorithmes et les cas d'usage. Il met en exergue les enjeux et défis concernant les applications du calcul quantique tolérant aux fautes.

- Il existe des arguments théoriques solides montrant qu'un processeur quantique tolérant aux fautes (FTQC) résoudrait certaines classes de problèmes drastiquement plus rapidement qu'un ordinateur classique, tels que la factorisation des grands nombres et la simulation de systèmes quantiques.
- Pour d'autres classes de problèmes, il existe un gain de temps théorique par rapport aux meilleurs algorithmes classiques, mais il est moins drastique. L'utilité en pratique dépendra alors des détails d'implémentation (notamment le temps d'exécution des portes quantiques).
- Les premières estimations de ressources pour des algorithmes dédiés aux calculateurs FTQC à même de résoudre des problèmes de portée industrielle sont de l'ordre de plusieurs milliers de qubits logiques, avec souvent un très long temps de calcul. Cela illustre le besoin d'optimiser la vitesse d'exécution des circuits quantiques et de la correction d'erreurs.
- Les cas d'usage industriels du FTQC sont, pour l'instant, peu ou mal identifiés en France, probablement car les industriels se sont concentrés

sur l'exploration des applications des petits processeurs quantiques bruités disponibles actuellement ou à court terme (dits NISQ) ou d'ordinateurs quantiques analogiques.

Le rapport souligne ensuite le rôle fondamental que joue la mise en œuvre de codes correcteurs d'erreurs quantiques pour réaliser des ordinateurs quantiques universels et exacts (c'est-à-dire tolérants aux fautes), et décrit les dernières avancées de ce domaine.

- 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.
- Les développements récents concernant les codes bosoniques et les codes dits LDPC non locaux 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.
- Plusieurs réalisations expérimentales importantes ont été annoncées en 2023 et 2024. Il s'agit de preuves de concept qui démontrent la faisabilité expérimentale de la correction d'erreur, par la réalisation de qubits logiques plus fiables que les qubits physiques qui les composent.
- Malgré les progrès réalisés en matière de codes correcteurs d'erreur quantique, le passage à des applications qui mettent en évidence un avantage quantique de manière irréfutable nécessite d'assembler un nombre de qubits logiques de plusieurs ordres de grandeur supérieur à ce qui est possible actuellement.

Puis le rapport dresse l'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 la feuille de route qui en résulte.

- Il existe au moins cinq technologies de qubits concurrentes, avec 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.

- Les feuilles de route technologiques des grands fabricants de technologies de calcul quantique ont dans l'ensemble été bien respectées jusqu'à présent.

Le rapport revient alors sur le passage à l'échelle des solutions existantes, enjeu scientifique et technique mondial majeur pour pouvoir bénéficier concrètement des avantages quantiques calculatoires dans de nombreuses applications, et étudie la capacité à assurer ce passage à l'échelle de façon modulaire par l'interconnexion appropriée de divers composants.

- L'intégration monolithique de qubits dans un seul système physique a des limites, notamment en raison du bruit et des erreurs engendrées par l'augmentation du nombre de qubits sur une même puce et des connexions requises pour adresser chaque qubit.
- Le passage à l'échelle nécessitera une approche modulaire et de l'interconnectivité par des liens de communication quantique, avec des photons micro-ondes et/ou optiques.
- La fidélité des opérations de calcul réparties sur plusieurs processeurs est encore peu étudiée.

Enfin, le rapport examine la question des comparaisons, avec d'autres programmes technologiques de grande envergure développés au cours des dernières décennies, entre le FTQC et des technologies plus classiques (IA, HPC) ainsi que le *benchmarking* d'ordinateurs quantiques et de leurs applications. Il est difficile d'évaluer l'impact économique du FTQC *a priori*, et des comparaisons avec d'autres grands programmes, comme la recherche spatiale, peuvent être éclairantes.

- Pour comparer les avancées et évaluer les progrès avec objectivité et fiabilité, il sera indispensable de développer des *benchmarks* spécifiques pour le FTQC communs à toutes les plateformes. Cela est rendu difficile par leur diversité, leurs spécificités en matière de caractéristiques

physiques et d'applications, leur maturité basse, ainsi que par l'évolution rapide des technologies.

- L'évaluation des performances pratiques du FTQC doit être envisagée à travers des *benchmarks* proches d'applications réelles et qui ont du sens pour les utilisateurs finaux industriels.
- Le calcul quantique n'est pas voué à remplacer le calcul classique, mais à le compléter; les avantages quantiques sont à rechercher du côté des applications intensives en calcul plutôt que des applications intensives en données; dans le futur les technologies FTQC auront à se positionner par rapport à celles fondées sur du Silicium 3D.
- L'architecture système d'un processeur FTQC est un sujet peu abordé en France et mériterait le développement d'expertise et de projets spécifiques. Ces projets devraient inclure 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. À cet égard, partager et analyser conjointement les retours d'expérience d'exploitation de démonstrateurs de processeurs quantiques précoces sera utile.

Après ce rapport d'étape, trois axes devront être explorés plus en profondeur pour compléter l'étude. Du point de vue technologique, l'état d'avancement des algorithmes et des applications, ainsi que des environnements de compilation, et la question des technologies habilitantes, restent à examiner. L'analyse des perspectives économiques nécessitera d'étudier les coûts de fonctionnement des technologies décrites ici et le potentiel de création de valeur associés aux cas d'usage. Enfin, il conviendra d'évaluer la formation et les besoins en compétences du secteur. En outre, il sera important de placer les résultats de cette étude dans le contexte européen et international.

Le rapport conclut que des progrès scientifiques et techniques sont encore nécessaires pour fonder des stratégies industrielles réalistes. Il recommande de poursuivre la réflexion collective pour compléter et mettre à jour régulièrement les informations collectées, afin de garantir une compréhension complète et actualisée des enjeux liés au FTQC.

Executive Summary

This report presents the results of a collective study carried out by a Working Group set up in June 2023 by the National Academy of Technologies of France (NATF) to assess the feasibility and impact of Fault Tolerant Quantum Computing (FTQC). It follows on from a study carried out for the "Secrétariat général pour l'investissement" (SGPI).

The report begins by a review of the concepts of quantum algorithms and quantum computational advantage, and describes how this advantage varies according to algorithms and use cases. It highlights the issues and challenges involved in fault-tolerant quantum computing applications.

- There are strong theoretical arguments showing that a fault-tolerant quantum processor would solve certain classes of problems drastically faster than a classical computer, such as factoring large numbers and simulating quantum systems.
- For other problem classes, there is a theoretical time saving compared with the best classical algorithms, but it is less drastic. Practical usefulness will then depend on implementation details, notably the execution time of quantum gates.
- Initial resource estimates for algorithms dedicated to FTQC computers capable of solving industrial-scale problems are of the order of several thousand logic qubits, often with very long computation times. This illustrates the need to optimize the execution speed of quantum circuits and error correction.
- Industrial use cases for FTQC are, as for now, little or poorly identified in France, probably because industrialists have concentrated on exploring

applications for the small noisy quantum processors currently available or in the near future (known as NISQs) or analog quantum computers.

The report then highlights the fundamental role played by the implementation of quantum error-correcting codes in the realization of universal (i.e. fault tolerant) quantum computers and describes the latest advances in this field.

- Research into quantum error correction has progressed significantly over the last five years, with important theoretical advances and experimental demonstrations.
- Recent developments in bosonic codes and nonlocal LDPC codes have reduced the cost of error correction by at least an order of magnitude compared with the traditional surface code previously favoured.
- Several major experimental projects were announced in 2023 and 2024. These were proofs of concept that demonstrate the experimental feasibility of error correction, through the realization of logic qubits that are more reliable than the physical qubits of which they are composed.
- Despite the progresses made in quantum error-correcting codes, the transition to applications that irrefutably demonstrate a quantum advantage requires the assembly of a number of logic qubits several orders of magnitude greater than is currently possible.

The report then reviews the most mature qubit technologies being developed in France. For each of these technologies, we describe the advances they have made, the challenges they face, their capacity to evolve and the resulting roadmap.

- There are five main groups of competing qubit technologies, with many variants, which have different strengths and weaknesses with regard to manufacturing and scaling. The current state of knowledge does not allow any of them to be singled out as clearly more advantageous.
- The technological roadmaps of the major manufacturers of quantum computing technologies have, on the whole, been well respected to date.

The report then returns to the issue of scaling up existing solutions - a major global scientific and technical challenge if we are to reap the concrete benefits of quantum computing in a wide range of applications - and examines the ability to ensure this scaling up in a modular way through the appropriate interconnection of various components.

- Monolithic integration of qubits into a single physical system has its limits, notably because of the noise and errors generated by increasing the number of qubits on a single chip and the connections required to address each qubit.
- Scaling up will require a modular approach and interconnectivity via quantum communication links, with microwave and/or optical photons.
- The fidelity of distributed computational operations across multiple processors is still largely unexplored.

Finally, the report examines the question of comparisons, with other large-scale technological programs developed over the last few decades, between FTQC and more conventional technologies (AI, HPC), as well as benchmarking quantum computers and their applications. It is difficult to assess the economic impact of FTQC a priori, and comparisons with other major programs, such as space research, can be enlightening.

- To compare advances and assess progress objectively and reliably, it will be essential to develop FTQC-specific benchmarks common to all platforms. This is made difficult by their diversity, their specific physical characteristics and applications, their low level of maturity, and the rapid evolution of technologies.
- Evaluation of FTQC's practical performance should be based on benchmarks that are close to real-life applications and that make sense for industrial end users.
- Quantum computing is not intended to replace classical computing, but to complement it; quantum advantages are to be sought in computationally intensive rather than data-intensive applications.

- The system architecture of a FTQC processor is a subject that has received little attention in France, and would benefit from the development of specific expertise and projects. These projects should include an understanding of the conditions for coupling high-performance computing (HPC) and FTQC, and the fit between technologies and applications, as well as the question of a possible energy advantage for FTQC, particularly for applications where FTQC and HPC could be in competition. In this respect, sharing and jointly analysing feedback from the operation of early quantum processor demonstrators will be useful.

After this interim report, three areas need to be explored in greater depth to complete the study. From a technological point of view, the state of advancement of algorithms and applications, as well as compilation environments, and the question of enabling technologies, remain to be examined. Analysis of the economic outlook will involve studying the operating costs of the technologies described here, and the potential for value creation associated with the use cases. Finally, it will be necessary to assess the sector's training and skill requirements. In addition, it will be important to place the results of this study in a European and international context.

The report concludes that further scientific and technical progress is still needed to establish realistic industrial strategies. It recommends continued collective reflection to complete and regularly update the information gathered, in order to ensure a complete and up-to-date understanding of FTQC-related issues.

Introduction

On attribue au physicien américain Richard Feynman l'idée, énoncée en 1981, de créer des ordinateurs quantiques pour étudier les phénomènes quantiques en les simulant. Par la suite, de nombreux chercheurs ont démontré que si on disposait d'ordinateurs dont les principes de calcul étaient fondés sur certaines propriétés caractéristiques de la mécanique quantique, alors il était possible de concevoir des algorithmes qui présentaient des accélérations significatives, notamment exponentielles, par rapport à leurs équivalents classiques (Bernstein-Vazirani, Deutsch-Jozsa, Shor...). Cela a conduit de nombreuses organisations, qu'elles soient publiques ou privées, grandes ou petites, à se lancer dans l'élaboration effective d'un ordinateur quantique et ceci dans la plupart des pays industrialisés.

L'objectif de ce rapport est de faire le point sur de tels développements. Il s'appuie sur l'expertise internationale des membres du groupe de travail mis en place par l'Académie des technologies ainsi que sur l'analyse détaillée de divers programmes de recherche et expériences menés en France et présentés par leurs responsables. Toutefois, l'emploi des principes de la mécanique quantique au sein du domaine des technologies de l'information ne se limite pas à accélérer des calculs, mais peut aussi concerner l'élaboration de capteurs fournissant de nouveaux types de données, et la transmission sécurisée de l'information au sein des réseaux de télécommunication. Ces autres volets ne sont pas abordés ici.

Deux grandes voies ont été suivies jusqu'à présent pour construire un ordinateur quantique. Une voie dite analogique qui propose des dispositifs physiques peu ou pas programmables adaptés à la simulation de phénomènes quantiques voire à certaines heuristiques d'optimisation. Une voie dite « discrète », ou « digital » en anglais, qui propose de construire des ordinateurs quantiques universels programmables par une séquence d'opérations à l'image de la façon dont on utilise un ordinateur classique.

Dans ce cas toutefois, l'unité d'information traitée n'est plus le « bit », mais le bit quantique appelé « qubit », pour « quantum bit ». Les propriétés de superposition d'états et d'intrication qui caractérisent la mécanique quantique rendent alors possibles des opérations sur un registre de plusieurs qubits qui n'ont pas d'équivalent classique en exhibant notamment diverses formes de simultanéité. C'est cela qui contribue au gain potentiel de performance d'un ordinateur quantique et fournit les éléments de ce qu'il convient d'appeler l'avantage quantique calculatoire. Toutefois, obtenir un avantage quantique pour résoudre un problème donné est difficile, et c'est l'objet de la recherche en algorithmique quantique. En outre, l'exécution d'un algorithme quantique rencontre un obstacle redoutable qu'aucune des expériences en cours dans le monde n'a réussi à surmonter en totalité pour l'instant. Il s'agit des erreurs qui s'accumulent lors de toute opération sur les qubits : leur initialisation, les portes quantiques qui agissent dessus, et enfin la mesure des qubits. Un des effets de ces erreurs est de générer la décohérence qui met fin aux effets quantiques d'intrication et de superposition, ce qui fausse aussi bien les opérations sur les qubits que leur mesure. Les sources d'erreurs sont multiples. Elles proviennent notamment des interactions des qubits avec leur environnement extérieur ainsi que des imperfections des outils de contrôle des qubits avec des signaux électroniques ou lasers.

Pour tenir compte de ce qu'il convient alors d'appeler du bruit quantique et bénéficier tout de même d'un avantage quantique malgré ce bruit, une première génération de solutions est apparue. Appelée génération NISQ (*Noisy Intermediate Scale Quantum*), elle s'applique à la plupart des développements en cours dans le monde. Elle consiste à exploiter un nombre relativement faible de qubits situé entre 50 et 150 et par des algorithmes de taille réduite et qui tolèrent une quantité limitée de bruit. Les applications envisagées concernent par exemple la simulation de molécules pour la chimie (*Variational Quantum Eigensolver*) ou l'optimisation combinatoire (*Quantum Approximate Optimization Algorithm*). Toutefois, le faible nombre de qubits considéré limite considérablement de potentielles applications concrètes. La génération NISQ exploite maintenant la technique dite de mitigation d'erreurs qui fait appel à un post-traitement des résultats du calcul quantique et réduit les erreurs générées grâce à des méthodes statistiques.

Récemment, une nouvelle génération a émergé. Bien que théorisée depuis longtemps, elle est restée hors d'atteinte en laboratoire pendant

de nombreuses années, car elle nécessite un contrôle très avancé des systèmes quantiques. Cette génération vise à corriger activement le bruit quantique pendant le calcul: c'est la génération FTQC (*Fault Tolerant Quantum Computing ou Calcul quantique tolérant aux fautes*), qui fait l'objet de ce rapport. Dans un ordinateur FTQC, des qubits physiques de base sont assemblés pour constituer des qubits logiques, moins nombreux que les qubits physiques, et qui présentent des taux d'erreurs plus faibles. Les qubits physiques redondants sont exploités avec des codes de correction d'erreurs pour détecter l'impact du bruit et pour le corriger au fil de l'eau pendant les calculs. Des découvertes récentes portant sur des techniques de codes correcteurs d'erreurs, plus efficaces en quantité de qubits physiques nécessaires, ont ouvert de nouvelles perspectives. Elles rendent plus réaliste la construction d'ordinateurs quantiques fiables, applicables à de nombreux usages.

Le rapport est structuré comme suit.

Au premier chapitre sont introduits les concepts de base du calcul quantique et la réalité pratique de l'avantage quantique. Cet avantage quantique n'est pas uniforme. Il dépend de la nature des algorithmes à mettre en œuvre et a donc un impact différencié selon les domaines d'usages. De plus, lorsque cet avantage existe en théorie, son exploitation concrète dépend de la quantité et de la qualité des qubits logiques dont dispose l'ordinateur censé exécuter l'algorithme concerné. Ce chapitre se conclut en comparant l'état de l'art en matière de réalisation physique de qubits logiques, aux besoins d'algorithmes caractéristiques de plusieurs cas d'applications. Cette comparaison permet d'estimer l'importance des passages à l'échelle qui restent à accomplir.

Le mécanisme de réduction des erreurs quantiques par l'emploi de codes correcteurs d'erreurs constitue actuellement le seul dispositif permettant d'envisager l'existence d'ordinateurs quantiques tolérants aux fautes. C'est l'objet du deuxième chapitre. Jusqu'à récemment, le code correcteur principalement étudié a été le code dit « code de surface ». Selon les diverses implémentations physiques des qubits, la redondance nécessaire à ce type de code conduit à envisager de l'ordre de 100 à 10 000 qubits physiques pour constituer un qubit logique dans le cadre, par exemple, de l'algorithme de factorisation de nombres entiers de Peter Shor. Cependant, des découvertes récentes permettent soit de construire des qubits intrinsèquement protégés

contre certains types d'erreurs (*bit-flip*), soit de remettre en question la connectivité locale des qubits limitée jusqu'à présent à deux dimensions. On aboutit alors à des réductions importantes du nombre de qubits physiques par qubit logique. Ces approches ouvrent donc un vaste champ d'explorations de nouvelles solutions, moins gourmandes en matériel et très utiles pour la réalisation concrète d'ordinateurs quantiques.

Les technologies physiques qui sont étudiées et expérimentées dans le monde pour mettre en œuvre des qubits physiques et les opérations qui leur sont associées sont nombreuses. Au troisième chapitre celles qui présentent le niveau de technologie le plus élevé du marché sont passées en revue : atomes neutres, qubits supraconducteurs, photons, spins dans le silicium, puis ions piégés. 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 la feuille de route qui en résulte.

Le passage à l'échelle du nombre de qubits physiques avec lequel on peut élaborer un ordinateur quantique est donc le premier enjeu majeur qu'il convient de surmonter. Après avoir constaté les limites de l'intégration monolithique de qubits, le quatrième chapitre se concentre sur l'augmentation du nombre de qubits physiques via l'interconnexion de plusieurs modules quantiques et aborde les différents problèmes liés à cette interconnexion. Sont notamment explorés l'interconnexion photonique, et le couplage de processeurs quantiques par des qubits distants. Le passage à l'échelle et la connectivité des qubits supraconducteurs font l'objet d'une analyse plus approfondie.

Le cinquième chapitre esquisse les premiers éléments d'une analyse technico-financière de l'établissement d'une filière industrielle des ordinateurs quantiques. L'étude de cet aspect sera poursuivie et complétée dans un second rapport de l'Académie. Les trois points abordés dans ce chapitre sont les suivants :

- la hauteur des espoirs suscités par l'existence d'ordinateurs quantiques et l'ampleur des financements publics et privés, qui leur sont consacrés dans le monde, conduisent à comparer la recherche sur les ordinateurs quantiques avec d'autres programmes mondiaux comme la fusion nucléaire, la recherche spatiale, le séquençage du génome humain,

l'accélérateur de particules LHC (*Large Hadron Collider*) du CERN. De ce point de vue, la recherche sur le FTQC paraît plus proche de la recherche spatiale du point de vue géostratégique ;

- la technologie FTQC est, de fait, sur le plan de la performance, en concurrence à court et moyen terme avec d'autres technologies qui peuvent réduire pendant ce laps de temps, la taille de son marché. La technologie 3D des circuits sur silicium et la spécialisation de microprocesseurs dédiés au calcul matriciel (GPU: *Graphics Processing Unit*) amènent à envisager une coexistence des processeurs quantiques avec des processeurs classiques au sein des architectures de supercalculateur et non à leur remplacement. En matière d'Intelligence artificielle (IA) et d'apprentissage, outre l'usage de GPU, la performance des applications est conditionnée par la vitesse d'une très grande quantité d'entrées/sorties portant sur des volumes très importants de données. Dans ce cas, l'accélération quantique est sérieusement handicapée ;
- pouvoir comparer des architectures selon leurs performances requiert des méthodes de *benchmarking* adaptées. Disposer de personnels compétents, pouvoir compter sur des industries habilitantes indispensables (cryogénie, lasers, semi-conducteurs, logiciel quantique...) et renforcer les formations sont autant de questions ébauchées ici, qui seront complétées dans le rapport suivant.

Chapitre 1

LA RÉALITÉ DE L'AVANTAGE QUANTIQUE ET SES BESOINS

1.1. ALGORITHME QUANTIQUE

Un algorithme quantique est un algorithme au sens usuel qui dispose en plus d'une mémoire dans un état quantique. Il peut appliquer une série d'opérations sur cette mémoire, en mesurer une partie, ou bien alterner les deux. Cette séquence est décrite par l'algorithme. Le résultat des mesures peut servir à contrôler la suite des opérations à effectuer. En soi, la description d'un algorithme est donc complètement déterministe. D'ailleurs, des outils de programmation quantique ont émergé depuis longtemps, et certains sont très aboutis, avec langages et environnements de programmation riches de bibliothèques variées. Souvent, le modèle des circuits quantiques est utilisé pour décrire ces algorithmes. Dans ce cas, des portes quantiques agissent sur la mémoire, y préparent l'information initiale, y font des opérations, puis des mesures pour obtenir des résultats intermédiaires (conditionnant la suite des opérations) ou finaux.

À l'aide de cette mémoire, un algorithme quantique peut ainsi, par exemple, simuler l'évolution d'un système quantique en décomposant l'évolution en une suite d'opérations élémentaires qu'il peut ensuite réaliser sur sa mémoire. Il s'agit d'une forme d'émulation, en ce sens que la mémoire quantique est alors dans un état physique approximant l'état du système quantique étudié.

La principale différence avec une mémoire classique, c'est-à-dire régie par la physique classique, réside dans l'existence de phénomènes, ou paradoxes, de la physique quantique qui ne sont ni explicables ni réalisables par la physique classique. Il est bien entendu possible de les décrire, et donc de les simuler numériquement sur un ordinateur classique, mais, comme nous le verrons, la puissance calculatoire d'un ordinateur quantique capable de compiler et d'exécuter un algorithme quantique est théoriquement sans

commune mesure avec celle de nos ordinateurs classiques, ou à venir, car elle est jusqu'à exponentiellement plus grande. Empressons-nous de le dire : cette supériorité calculatoire ne concerne que certaines tâches précises, que la communauté scientifique cerne et cartographie depuis une trentaine d'années.

Un bit quantique ou un système quantique à deux niveaux que l'on représente sous la forme $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$, où α et β sont deux nombres complexes, appelés amplitudes. $|0\rangle$ et $|1\rangle$ correspondent aux états de base du qubit, comme pour un bit classique, mais un qubit peut se trouver dans toute superposition quantique de ces états. Notons qu'il ne s'agit pas d'un mélange statistique des deux états de base : un mélange statistique décrit la situation où il y a incertitude sur l'état considéré, alors qu'une superposition décrit une combinaison cohérente des états $|0\rangle$ et $|1\rangle$, et permet de réaliser des interférences².

La corrélation probabiliste de plusieurs observations, et donc de plusieurs états, est un phénomène connu en physique classique. Il en est de même en physique quantique, et on parle alors d'intrication. Ainsi, il est possible d'intriquer deux objets quantiques, comme deux atomes ou deux spins d'électrons, de sorte que le résultat de l'observation de l'un (par une mesure physique) est corrélé à celle de l'autre. En revanche, en physique quantique, l'expérience montre que le résultat d'une mesure d'un des deux objets quantiques n'est fixé que lors de sa réalisation, un peu comme si un dé n'arrêtait pas de tourner avant qu'il ne soit regardé. C'est alors qu'un phénomène contre-intuitif se produit, car ce résultat aléatoire est corrélé à celui qui est obtenu par la mesure de l'autre particule liée, même si elle est si éloignée qu'aucune information n'a le temps d'être transmise entre les deux objets. Cela peut sembler paradoxal, mais c'est la corrélation entre les deux particules qui est préservée, plutôt qu'une transmission d'informations de l'une à l'autre. L'intrication quantique intervient aussi, et surtout, pendant les calculs eux-mêmes et avant toute mesure, grâce en particulier aux portes quantiques à deux qubits qui génèrent ces corrélations entre qubits et que l'on peut observer plus tard par la mesure. Elle permet de générer

2 Il est en fait aussi possible de considérer des mélanges statistiques de superpositions, appelés états mixtes et représentés par des matrices densité.

des phénomènes d'interférences entre plusieurs qubits puis d'amplifier certaines amplitudes, par exemple celle de l'état quantique correspondant au résultat de l'algorithme, pour que celui-ci soit révélé lors de la mesure finale. Ces phénomènes d'interférences sont parfois désignés par le terme de parallélisme quantique.

Ce genre de phénomène est maintenant vérifié expérimentalement sur de grandes distances, y compris par satellite. Il est désormais admis que la physique quantique ne peut être simulée efficacement, en toute généralité, par un ordinateur, même à l'aide de techniques probabilistes. En revanche, c'est tout un art d'identifier cette frange de problèmes où l'ordinateur quantique fournirait un avantage calculatoire incomparable.

1.2. ORDINATEUR UNIVERSEL

Nos ordinateurs actuels, non quantiques, sont universels, c'est-à-dire non spécialisés, ils peuvent exécuter à la demande tout ce qui est calculable par un autre ordinateur, si on laisse de côté les contraintes de temps et mémoire. Ce caractère universel est en fait lié au concept mathématique de machine de Turing. D'une part toute machine peut être décrite par un « code » ou programme, d'autre part, il existe une machine « universelle » qui peut simuler toute autre machine en lisant son code. En informatique quantique, il existe aussi une variante quantique de cette universalité. On peut définir une machine de Turing qui modélise formellement le calcul quantique. Certaines de ces machines quantiques sont également universelles, on peut donc y programmer n'importe quelle autre machine quantique. Ce point est moins intuitif qu'en informatique classique, car ici, ce sont des transformations physiques - des opérations sur des états quantiques - qui sont configurées selon la tâche à accomplir. Pourtant, ces opérations sont elles aussi universelles, car elles peuvent être décrites par des matrices unitaires à coefficients réels ou complexes, et non plus par des portes logiques à base de 0 et 1.

Des outils de programmation quantique sont déjà développés. Ils sont prêts pour la machine qui saura contrôler une mémoire quantique suffisamment grande. Ces langages de programmation décrivent en fait le plus souvent des circuits quantiques, qui sont ensuite réalisés concrètement sur des plateformes manipulant des particules quantiques. Comme les circuits

logiques, quelques types de portes suffisent seules à réaliser tous les circuits possibles: les portes agissant sur un qubit, augmentées d'une porte d'un type unique agissant sur deux qubits (le *control-not*, par exemple). Il s'agit là aussi d'une notion d'universalité. Un jeu de portes quantiques est universel s'il permet de réaliser par combinaison n'importe quelle transformation unitaire. Il en existe aussi des jeux finis, au prix d'une universalité approchée, mais suffisante pour le calcul. Par exemple, un jeu de portes universel peut être constitué avec les portes Hadamard et T agissant sur un seul qubit complétées par la porte *control-not* agissant sur deux qubits.

Un ordinateur quantique, quantique étant un système plus complexe qu'un ordinateur classique, on peut penser qu'il sera réservé à certaines tâches, et qu'il est donc inutile de chercher à exécuter tous les algorithmes classiques sur des machines quantiques. Il n'en demeure pas moins que des routines de logique classique, telle que l'arithmétique, devront être réalisables sur des états quantiques également. Les transformations sur les états quantiques devant être réversibles, on pourrait penser que cela poserait problème lorsqu'il s'agit d'exécuter une opération logique non réversible, par exemple l'addition de deux bits ou qubits³. Heureusement, il était connu avant même le début de l'informatique quantique que tout calcul classique peut être rendu réversible avec un surcoût en mémoire et en temps de calcul. En outre, il se trouve qu'un calcul classique réversible est un cas particulier d'une transformation unitaire, il peut donc ensuite, en principe, être directement converti en circuit quantique sans surcoût. Bien entendu, sur de petits calculateurs de quelques milliers de bits, voire plus, le surcoût (maîtrisé) du passage au calcul réversible (puis quantique) sera sans aucun doute un obstacle au début.

1.3. CALCUL TOLÉRANT AUX FAUTES

En revanche, contrairement aux ordinateurs actuels, le taux d'erreur des processeurs quantiques, ou même seulement de la mémoire quantique, reste élevé, et ne peut donc être ignoré. Ce paradigme a été étudié un temps lors de la réalisation des premiers ordinateurs (classiques). Il s'agit du problème du calcul tolérant aux fautes, pour laquelle des solutions existent dans

3 Cette opération est non réversible puisqu'il est impossible de retrouver l'état de deux bits a et b à partir de leur seule somme $a+b$.

l'informatique classique. Ces dernières ont été exportées au quantique, et validées théoriquement. De premières démonstrations expérimentales ont d'ailleurs été réalisées (voir chapitre 2).

Les fautes qui se produisent pendant un calcul quantique sont différentes de celles qui interviennent en calcul classique. Dans ce dernier, il peut y avoir, dans un bit classique, une substitution d'un 0 par un 1, ou le contraire. Dans un bit quantique, il peut y avoir tout un continuum de modifications, car l'état d'un bit quantique est représenté par deux nombres complexes (ses coordonnées) qui peuvent subir une transformation non discrète, dite continue. Ces erreurs continues proviennent de différentes sources de bruit qui affectent les objets physiques qui supportent les qubits. Elles résultent des imperfections des systèmes physiques qui agissent sur les qubits pour générer des portes quantiques ainsi que par l'environnement.

De façon surprenante, il est cependant possible de corriger ces erreurs continues avec des codes correcteurs quantiques. La grande découverte a été de se rendre compte qu'il suffit de prendre en compte deux types d'erreur (inversion de bit et inversion de phase) pour corriger toutes les erreurs, grâce à la linéarité des transformations quantiques. Inspirés des codes correcteurs classiques, mais mathématiquement beaucoup plus ardues à construire, les codes correcteurs quantiques permettent de protéger la mémoire quantique contre les sources de bruit. Ils peuvent aussi protéger le calcul, lorsque le taux d'erreur est suffisamment bas. Bien entendu, cela a un surcoût en nombre de qubits nécessaires et en temps de calcul. D'un point de vue théorique, ce surcoût est considéré comme étant raisonnable. D'un point de vue pratique, où, en 2025, le millier de qubits physiques est à peine atteint, il s'agit d'une autre histoire.

Notons que les codes correcteurs (classiques) sont utilisés tous les jours dans les télécommunications par exemple. Il y a donc un très grand savoir-faire qui a permis entre autres la découverte de codes correcteurs quantiques très adaptés au calcul quantique. Ne minimisons pas ici la puissance théorique de ces codes correcteurs quantiques, qui, en détectant une erreur discrète, peuvent corriger une erreur *a priori* continue. Dans les années 1990, l'existence même de tels codes avait été mise en question.

Ces codes correcteurs induisent deux niveaux de mesure du nombre de qubits utilisés: les qubits logiques et les qubits physiques. Les qubits physiques correspondent aux systèmes quantiques effectivement réalisés sur le processeur. Ils sont bruités par construction, mais peuvent être utilisés pour réaliser un qubit logique dont le bruit «logique» est amoindri. Un qubit logique devient alors une abstraction utilisée par l'algorithmique, qui nécessite une erreur suffisamment basse pour qu'elle ne perturbe pas la réponse de l'algorithme (ou alors de façon négligeable).

Le nombre de qubits physiques pour réaliser un qubit logique dépend du taux d'erreur physique, des contraintes matérielles (par exemple sur la connectivité) qui influent sur le choix d'un code correcteur quantique adapté, et du taux d'erreur «logique» en fonction de l'utilisation envisagée. Le lien entre ces deux notions de qubits est développé dans le chapitre 2.

1.4. COMPLEXITÉ THÉORIQUE

Il n'est pas rare de voir, même actuellement sans ordinateur quantique, des algorithmes quantiques rapides découverts, puis, quelques mois après, des algorithmes classiques quasiment aussi bons. Il y a en effet une véritable émulation entre les communautés, un peu comme en cryptographie quand une application de chiffrement, signature ou autre est développée, standardisée, puis attaquée, avant d'être mise à niveau de façon cyclique jusqu'à la prochaine attaque dévoilée. Il est en effet quasiment impossible de prouver qu'un problème est difficile. La théorie de la complexité nous permet de faire la part des choses, et donc de mieux cerner le potentiel du calcul quantique.

Cette théorie classe les problèmes selon leur difficulté prouvée, ou conjecturée. Les plus difficiles sont les problèmes indécidables. Autant passer son chemin ici, car ils sont prouvés mathématiquement insolubles, même avec tout le temps nécessaire. Les problèmes calculatoires ne sont pas forcément solvables facilement (c'est-à-dire en temps polynomial), mais dont la solution est facilement vérifiable sont dits NP. La classe des problèmes NP-complets regroupe tous les problèmes aussi difficiles à résoudre que les autres problèmes de NP. Ils sont en, un sens, universels. si on trouvait un algorithme efficace pour un problème NP-complet, on pourrait résoudre efficacement tous les problèmes de NP. Aujourd'hui, il est conjecturé que les

problèmes de NP ne peuvent pas tous être résolus efficacement (il s'agit du fameux problème « $P=NP?$ »), et résoudre un problème NP-complet est un défi qui nécessite, à l'heure actuelle, un temps exponentiel en fonction de la taille du problème. La théorie de la complexité, une branche de l'informatique, a développé une théorie solide sur leur difficulté présumée. Cette théorie est assez stable, et il y a peu de chance que ces problèmes admettent un jour une solution algorithmique rapide. En revanche, pour certaines instances, utilisées tous les jours dans le monde industriel, il existe des heuristiques qui fournissent des solutions acceptables. C'est l'un des axes de recherche très stratégique de la recherche opérationnelle.

Il existe d'autres problèmes intermédiaires, pour lesquels il est difficile de construire une théorie convaincante de leurs difficultés. Pourtant, aucun algorithme efficace n'est connu. Citons pour exemple le problème de la factorisation. Il s'agit d'exprimer un nombre (non premier) en produit de nombres premiers. La vérification d'une solution est facile, il s'agit d'une simple multiplication. Ce problème est donc NP, mais des arguments laissent penser qu'il ne peut pas être NP-complet. La factorisation, et ses variantes, se trouve être à la base de la cryptographie contemporaine, dite à clé publique, standardisée et développée dans la plupart des transactions et opérations sécurisées. C'est pourtant un des problèmes qu'un ordinateur quantique pourrait résoudre rapidement (c'est-à-dire en temps polynomial lié au nombre de chiffres du nombre à factoriser).

Nous venons donc de voir qu'il existe des problèmes indécidables, NP-complets, NP, mais non complets. Les problèmes résolubles efficacement sont dits dans P, pour solution en temps polynomial (linéaire, quadratique...). On peut considérer aussi la classe BPP (*Bounded-error Probabilistic Polynomial*), des problèmes résolubles par un algorithme probabiliste en temps polynomial avec une erreur probabiliste (négligeable). L'équivalent quantique de cette classe est BQP. Cette dernière est donc *a priori* plus large que BPP et P (*polynomial*). Mais, hélas, il n'est pas raisonnable de penser que BQP contienne un problème NP-complet, en tout cas pas plus que ne le ferait BPP ou.. Cependant, des arguments théoriques laissent penser qu'il y aurait toute une série de problèmes difficiles (pour les ordinateurs classiques) dans BQP, mais qu'aucun d'eux ne serait complet. Il faut donc les rechercher un à un ! Par exemple, la factorisation est un problème NP *a priori* non complet qui n'est *a priori* pas dans BPP, mais dans BQP, car l'algorithme de factorisation

de Peter Shor l'effectue en temps polynomial. L'intérêt d'avoir un tel problème NP est que la solution est facilement vérifiable. En outre, certains problèmes, comme l'échantillonnage de bosons, utilisé en photonique, sont dans BQP, mais pas dans NP, car ils ne sont pas facilement vérifiables.

Notons ici qu'un ordinateur quantique ne permet pas de calculer ce qui est indécidable. Il est aussi prouvé que tout problème résolu par un ordinateur quantique (par exemple dans BQP) peut aussi être résolu par un ordinateur classique, avec une mémoire polynomiale, mais avec un temps potentiellement exponentiel (classe PSPACE). D'un point de vue informatique, l'avantage à rechercher est donc du côté du temps de calcul (aux côtés d'autres avantages potentiels, non liés à la complexité algorithmique, comme le coût énergétique ou la confidentialité des données), et non du côté de la calculabilité. En d'autres termes, le calcul quantique ne remet pas en cause la thèse de Church-Turing, mais remet bien en cause sa version étendue.

1.5. ACCÉLÉRATION QUANTIQUE

Quel ordinateur quantique pour quel usage ? La question se pose aujourd'hui dans un environnement où les premiers calculateurs sont de taille modeste à l'échelle de l'informatique contemporaine. Nous parlons de quelques centaines de bits dans un état quantique, donc de qubits physiques, contre plusieurs giga-octets sur nos smartphones. Pire, ces qubits sont actuellement bruités, c'est-à-dire avec un taux d'erreur trop grand pour mener à bien un calcul. Pourtant il suffirait d'une mémoire quantique fiable de quelques milliers de bits quantiques pour déjà avoir une puissance de calcul quantique qui ne pourrait pas être égalée par les plus puissants des ordinateurs classiques.

Il existe une source *a priori* riche de problèmes pour lesquels un ordinateur quantique apporterait un avantage exponentiel dans le temps de calcul. La factorisation est un de ces problèmes, ainsi que la simulation (ou émulation) d'un système quantique (chimie quantique par exemple). Il est aussi possible de traiter des problèmes d'algèbre linéaire, comme la résolution de systèmes linéaires, intraitables lorsque leur nombre de variables est trop grand. Ces derniers sont d'ailleurs universels pour le calcul quantique.

Il existe aussi toute une série d'algorithmes dont le gain n'est pas exponentiel, mais tout de même significatif. Une accélération quadratique est même quasi

systematique sur toute une série d'algorithmes quantiques d'optimisation, notamment en recherche opérationnelle.

Une dernière catégorie a aussi vu le jour, entre exponentiel et quadratique, autour de l'apprentissage machine, de la résolution d'équations aux dérivées partielles, où finalement de grands systèmes linéaires sont à inverser. Pendant un moment, un gain exponentiel était espéré, mais il n'est finalement que polynomial.

Concernant les accélérations quantiques, on en distingue trois types :

- accélérations exponentielles, par exemple l'algorithme de Shor pour la factorisation des grands nombres ou la simulation de systèmes quantiques ;
- accélérations polynomiales, incluant des algorithmes utilisant HHL (*Harrov-Hassidim-Lloyd*) pour par exemple l'inversion approchée de matrice, ainsi que l'algorithme de recommandation - il convient de noter que, de façon générale, même une accélération polynomiale peut apporter des gains significatifs dans l'industrie ;
- accélérations quadratiques (cas particulier du cas précédent), telles que l'algorithme de Grover pour la recherche dans une base de données non ordonnées, et l'estimation d'amplitude (utile pour des applications type simulation de Monte-Carlo) - même si un facteur quadratique est important en industrie, cette accélération sera sans doute moins évidente en pratique, puisque, compte tenu de la vitesse d'un processeur quantique, son avantage asymptotique ne se manifesterà que sur des temps de calcul démesurés.

Ces accélérations ont été toutes prouvées mathématiquement, puisqu'il n'est pas possible de réaliser ces algorithmes aujourd'hui. Bien qu'elles soient très intéressantes du point de vue de la recherche, il est important de considérer l'étude de cas pratiques plutôt que des pires cas théoriques, des facteurs tels que le cycle d'horloge et les surcoûts liés à la correction d'erreurs, ce qui rend l'accélération réelle plus incertaine, et en particulier concernant les accélérations quadratiques et polynomiales.

L'accélération quantique sur une entrée réelle par rapport aux algorithmes classiques existants n'est donc pas garantie en pratique. Il n'est pas clairement compris non plus à partir de quand cette accélération asymptotique se manifesterait, compte tenu de toute la machinerie interne et ses surcoûts qui sont dépendants des technologies utilisées et de leurs avancées. Les efforts portent principalement sur la réduction des coûts liés à la correction des erreurs, véritable barrière qui semble fléchir peu à peu, ainsi que sur la transposition des algorithmes quantiques sur l'architecture choisie, comme la décomposition des opérations en portes quantiques élémentaires en fonction de la connectivité des bits quantiques utilisés. Ces étapes doivent aussi être effectuées pour le chargement des données ainsi que pour les algorithmes classiques utilisés pour traiter en superposition des tâches classiques.

Certains groupes de recherche travaillent à estimer les ressources qui seraient nécessaires pour résoudre un problème utile. Citons quelques articles de revue reprenant les algorithmes existants, jusqu'aux cas d'usage, en estimant les ressources nécessaires, que ce soit en termes de qubits quantiques logiques ou en qubits physiques en prenant en compte la correction des erreurs :

- « *Assessing requirements to scale to practical quantum advantage*⁴ ».
- « *Quantum algorithms: A survey of applications and end-to-end complexities*⁵ ».

Des estimations de ressources sont régulièrement effectuées, elles tentent de prendre en considération l'ensemble des facteurs. Des outils sont même développés à cette fin pour des programmes écrits comme, par exemple :

- « *Using Azure Quantum Resource Estimator for Assessing Performance of Fault Tolerant Quantum Computation*⁶ ».

4 M. E. Beverland, P. Murali, M. Troyer *et al.* <https://arxiv.org/abs/2211.07629> (2022)

5 A. Dalzell, S. McArdle, M. Berta *et al.* <https://arxiv.org/abs/2310.03011> (2023)

6 W. van Dam, M. Mykhailova, M. Soeken, <https://arxiv.org/abs/2311.05801> (2023)

1.6. HEURISTIQUES ET APPROCHES EMPIRIQUES

Jusqu'à peu, le développement des algorithmes quantiques reposait sur une approche théorique puisqu'aucun des algorithmes quantiques de supériorité établie n'a pu être à ce jour mis en œuvre sur des données de taille réelle sur un ordinateur quantique. À juste titre, une approche heuristique, voire empirique, est maintenant largement déployée afin de tirer profit des premiers calculateurs existants ou à venir. Les algorithmes types *Variational Quantum Eigensolver* (VQE) et *Quantum Approximate Optimization Algorithm* (QAOA) mettent en œuvre de telles heuristiques, cependant, sans garantie d'accélération.

Cette approche est traditionnelle en informatique, et en particulier dans l'industrie, pour traiter des problèmes infaisables comme les problèmes NP-complets (SAT, MAXCUT,...), dont il existe au fond des solutions convenables en pratique. La voie médiane consiste à chercher des accélérations pour certains cas pratiques, même si la théorie nous dit que dans le pire cas aucune accélération n'est attendue.

Ces nouvelles approches heuristiques, mêlant théorie, expérimentations (sur plateforme NISQ ou simulées sur HPC) et conjectures, ont donc été activement développées. Inspirées de leurs analogues théoriques, elles simplifient grandement les algorithmes précédemment proposés en prenant en compte des hypothèses sur les données, et parfois aussi en s'affranchissant de validation théorique. On peut retrouver ici une certaine approche de l'apprentissage profond qui a fait ses preuves, même si pour le quantique on en est encore loin, et qu'il faudra sans doute commencer par dépasser le NISQ.

Cependant, jusqu'à ce jour, aucun avantage n'a été démontré. Pire, les engouements des premiers résultats sont souvent gommés ultérieurement par des avancées algorithmiques (classiques) qui viennent égaler les calculs effectués sur les premiers circuits quantiques.

Ceci n'est au fond qu'une motivation supplémentaire pour réaliser un calculateur de taille suffisamment grande, tolérant aux fautes, et le plus universel possible.

1.7. CAS D'USAGE

L'identification précise de cas d'usage du calcul quantique tolérant aux fautes est difficile, en partie probablement parce qu'il est difficile de démontrer l'utilité avant d'atteindre la faisabilité. Évaluer l'impact économique de la résolution de ces cas d'usage est un problème encore plus complexe et il est très difficile d'y apporter une réponse précise aujourd'hui.

Certaines filières industrielles sont plus impliquées que d'autres dans la recherche sur les applications du calcul quantique tolérant aux fautes, et ces filières varient selon les pays. En France, les domaines de l'énergie, des services financiers et de la défense semblent bien positionnés. Notons aussi le domaine de la chimie computationnelle pour la découverte de médicaments.

On observe toutefois un certain consensus sur le fait que le calcul quantique tolérant aux fautes sera plus avantageux pour les applications intensives en calcul (*compute-intensive*) que pour les applications intensives en données (*data intensive*). Ces dernières, telles que l'apprentissage automatique, consacrent la majeure partie de leur temps d'exécution à la manipulation des entrées et des sorties, alors que l'accélération quantique est plutôt liée à l'exécution du calcul en lui-même et que le chargement des données dans un ordinateur quantique est un processus physiquement lent.

La motivation première de la création d'ordinateurs quantiques est de permettre la résolution de problèmes dont le temps de résolution sur ordinateurs classiques est *a priori* exponentiel en fonction du nombre de paramètres. En pratique, cette quête s'est quelque peu élargie, car plusieurs algorithmes quantiques ont été rattrapés par leurs homologues classiques, notamment parce que ceux-ci ont pu connaître des évolutions stimulées par l'avantage quantique potentiel.

Ainsi la notion d'avantage quantique intègre maintenant différents paramètres: une accélération du temps de calcul qui est en général polynomial ou exponentiel, une meilleure qualité des résultats, la capacité à générer de bons résultats avec moins de données d'entraînement dans le cas de l'apprentissage automatique et, *in fine*, un avantage économique avec une solution coûtant moins cher dans l'absolu, et notamment du point de vue du coût énergétique qui est très élevé dans les centres de calcul de puissance.

1.7.1. CLASSIFICATION PAR TYPE DE PROBLÈME

En reprenant plus précisément les sections 1.5 et 1.6, nous pouvons classifier les problèmes actuels pouvant potentiellement bénéficier de l'apport du calcul quantique selon les problématiques suivantes sachant que ces bénéfices restent à prouver d'un point de vue théorique et pratique. Cet inventaire assez classique ne reflète pas un tri logique. L'intérêt de ces problèmes dépend des secteurs d'activité des entreprises. La capacité d'ordinateurs quantiques à tolérance aux fautes à les résoudre est encore sujette à caution pour différentes raisons évoquées dans ce rapport. La variété des algorithmes, cas d'usage et solutions matérielles envisagés, est tellement grande qu'aucune généralité ne peut être tirée du savoir actuel dans le domaine.

- **Les simulations de systèmes physiques quantiques**, qui concernent la physique des solides tout comme la chimie quantique. Il s'agit généralement de déterminer la configuration énergétique au repos de ces systèmes (*ground-state*) avec une meilleure précision qu'avec les méthodes classiques. Par extension, d'autres algorithmes quantiques visent à déterminer la spectrographie de molécules, leur structure vibrationnelle ou rotationnelle, des états excités, comment elles interagissent entre elles et comment fonctionnent diverses réactions chimiques. Cela permettrait, par exemple, de créer des molécules *ab initio*. Les cas d'usage visent à la création de nouveaux matériaux solides, comme pour la création de batteries plus efficaces en termes de densité énergétique ou de vitesse de chargement, ou de nouveaux composés chimiques dans le domaine de l'énergie comme pour la captation du carbone, l'identification de nouveaux catalyseurs plus efficaces énergétiquement pour la production d'engrais ou de solutions thérapeutiques diverses^{7, 8, 9, 10}. L'existence d'accélération

7 [Quantum-centric Supercomputing for Materials Science: A Perspective on Challenges and Future Directions](#) by Yuri Alexeev, Liang Jiang *et al.*, DoE, CERN, RIKEN, University of Toronto, University of Maryland, Inflection, Dell, IBM, BMW, Boeing, Bosch, Algorithmiq, ExxonMobil, *et al.*, *arXiv*, December 2023 (60 pages).

8 [Quantum Chemistry in the Age of Quantum Computing](#) by Yudong Cao, Alan Aspuru-Guzik *et al.*, 2018 (194 pages). © 2019 American Chemical Society

9 [Quantum chemistry, classical heuristics, and quantum advantage](#) by Garnet Kin-Lic Chan, *arXiv*, July 2024 (45 pages).

10 [Quantum Chemistry on Quantum Computers](#) by Libor Veis, 2021 (31 pages).

exponentielles pour ces types de calcul n'est pas garantie de manière générique¹¹. Par ailleurs, comme nous le verrons plus loin, les estimations actuelles des ressources en nombre de qubits logiques et physiques ainsi qu'en temps de calcul sont dans des plages rendant ces cas d'usage très incertains en l'état actuel de nos connaissances et des développements technologiques.

- **Les problèmes de décision et d'optimisation**, que l'on retrouve dans de nombreux métiers. Cela touche par exemple l'optimisation du trajet et du remplissage de véhicules pour les livraisons, celle de l'allocation de ressources dans des usines avec de nombreuses machines, des objets entrants et sortants, et des personnels techniques à allouer à ces outils. On y retrouve également de nombreux problèmes d'optimisation dans le cadre des services financiers ou des assurances¹². Les algorithmes d'optimisation connus présentent en général plutôt des accélérations polynomiales et non exponentielles. La littérature scientifique est moins abondante sur leur résolution avec des ordinateurs à tolérance aux fautes.
- **L'apprentissage automatique** (*machine learning*) aussi bien côté entraînement qu'inférences de modèles^{13,14}. Ces problèmes sont actuellement résolus assez efficacement avec des algorithmes classiques reposant sur des architectures matérielles à base de processeurs spécialisés, qui optimisent le calcul matriciel massif. Il existe un grand nombre d'algorithmes quantiques d'apprentissage automatique qui permettraient d'obtenir de meilleurs résultats ou à moindre coût dans un grand nombre de domaines (réseaux génératifs, reconnaissance d'images, traitement du langage), voire de les accélérer. L'une des motivations actuelles de la recherche dans le domaine est le coût énergétique énorme

11 [Is there evidence for exponential quantum advantage in quantum chemistry?](#) by Seunghoon Lee, Ryan Babbush, John Preskill *et al.*, *arXiv* August 2022 (81 pages).

12 [A Review on Quantum Approximate Optimization Algorithm and its Variants](#) by Kostas Blekos *et al.*, *Physics Reports* Volume 1068, 2 June 2024 (85 pages).

13 [Quantum Artificial Intelligence: A Brief Survey](#) by Matthias Klusch, Jörg Lässig, Daniel Müssig, Antonio Macaluso, and Frank K. Wilhelm, DFKI, *arXiv*, August 2024 (21 pages).

14 [A comprehensive review of Quantum Machine Learning: from NISQ to Fault Tolerance](#) by Yunfei Wang, and Junyu Liu, The University of Chicago and Brandeis University, *arXiv*, January-March 2024 (53 pages).

des grands modèles de langage. L'obtention d'un avantage quantique est cependant conditionnée par l'optimisation du chargement des données d'entraînement dans ces algorithmes. L'inadéquation du calcul quantique à l'ingestion de gros volumes de données reste un handicap certain. De plus, un avantage quantique générique n'a pas encore été démontré pour les algorithmes de *machine learning* quantiques¹⁵.

- **Les problèmes d'ingénierie** qui nécessitent en particulier la résolution d'équations aux dérivées partielles complexes¹⁶ avec des domaines d'applications vastes dans la conception de systèmes divers dans l'aérospatial, dans les moteurs, et dans la mécanique des fluides¹⁷. À noter que ces cas d'usage ne génèrent pas d'accélération exponentielle garantie.
- **La cryptanalyse** qui comprend les méthodes permettant de casser des clés publiques de chiffrement ou de signatures utilisées sur Internet, comme celles qui reposent sur l'algorithme de chiffrement et de déchiffrement RSA. L'algorithme quantique le plus connu est celui de la factorisation de nombres entiers de Peter Shor, mais il n'est pas le seul. L'algorithme de logarithme discret du même Peter Shor ainsi que les algorithmes de Grover et Simon pourraient servir à casser divers systèmes de cryptographie à clés publiques, quoique nécessitant de très longs temps de calcul. L'existence de cette menace future pèse par exemple sur les données interceptées aujourd'hui et qui auraient de la valeur dans un lointain futur (*Store Now Decrypt Later*). Cela a fait émerger la création de contre-mesures telles que les algorithmes de chiffrement dits post-quantiques, dont la standardisation par le NIST aux USA a été finalisée l'été 2024 pour trois protocoles sélectionnés sur quatre, et dont les déploiements commencent à être planifiés.

15 [Is quantum advantage the right goal for quantum machine learning?](#) by Maria Schuld and Nathan Killoran, *arXiv*, March 2022-February 2023 (13 pages) and [Why measuring performance is our biggest blind spot in quantum machine learning](#) by Maria Schuld, Xanadu, *PennyLane blog* March 2022.

16 [Investigation on a quantum algorithm for linear differential equations](#) by Xiaojing Dong, Yizhe Peng, Qili Tang, Yin Yang, and Yue Yu, *arXiv*, August 2024 (22 pages).

17 [Quantum computing for simulation of fluid dynamics](#) by Claudio Sanavio, and Sauro Succi, *arXiv*, January 2024 (11 pages).

La réalisation pratique de solutions de calcul quantique dans tous ces domaines est encore hypothétique. Elle dépend de nombreux facteurs et incertitudes scientifiques et technologiques qui seront évoqués dans ce rapport. Ils concernent bien entendu la capacité à monter en échelle au niveau du matériel et de la correction d'erreur, mais aussi à des considérations pratiques en termes effectifs de temps de calcul et d'accélération, et au cas par cas. La notion d'avantage quantique ne peut pas encore être affirmée de manière généralisée pour ces différents cas d'usage.

La viabilité de ces solutions dépend de nombreux facteurs et inconnues : la création d'algorithmes quantiques plus efficaces, l'évolution des méthodes de préparation et d'encodage des données dans des registres quantiques, l'amélioration de la qualité des qubits, le passage à l'échelle, la vitesse d'exécution des portes quantiques, la création de codes de correction d'erreurs encore plus efficaces, la capacité à interconnecter efficacement et de manière quantique des processeurs quantiques, et la capacité à paralléliser les circuits quantiques sur un grand nombre de machines, d'un coût abordable, pour réduire les temps de calcul. La diversité de ces défis, des solutions envisagées par les chercheurs et entreprises du secteur, et des incertitudes scientifiques comme technologiques et économiques associées rendent tout pronostic hasardeux. Une chose est à peu près certaine : compte tenu des cycles de mise au point et d'expérimentation, même en étant optimiste, la résolution de l'ensemble de ces problèmes prendra beaucoup de temps.

1.7.2. CLASSIFICATION PAR INDUSTRIE

À très haut niveau, comme présenté dans la figure 1 ci-dessous, on peut distinguer deux grandes catégories d'applications industrielles :

- la première correspond aux applications qui facilitent le travail des chercheurs dans le monde académique et industriel, notamment pour la découverte de nouveaux matériaux, molécules et procédés chimiques. Cela passe le plus souvent par la création de jumeaux numériques exploitant les lois de la physique quantique. Dans le cas de la recherche appliquée, les produits conçus à l'aide du calcul quantique seront ensuite fabriqués et distribués avec des procédés traditionnels ;

- la seconde est liée aux opérations quotidiennes des entreprises de nombreux secteurs, qui visent à les rendre plus efficaces, dans l'amélioration des services fournis ou dans la réduction de leurs coûts. On va y trouver de nombreux cas d'usage d'optimisations dans les services financiers, dans les transports, la logistique et la distribution ainsi que dans toutes les industries manufacturières. Les opérateurs de télécommunication sont aussi concernés pour l'optimisation de leurs réseaux (placement de stations de bases, plans de fréquence, routage de trafic, etc.).

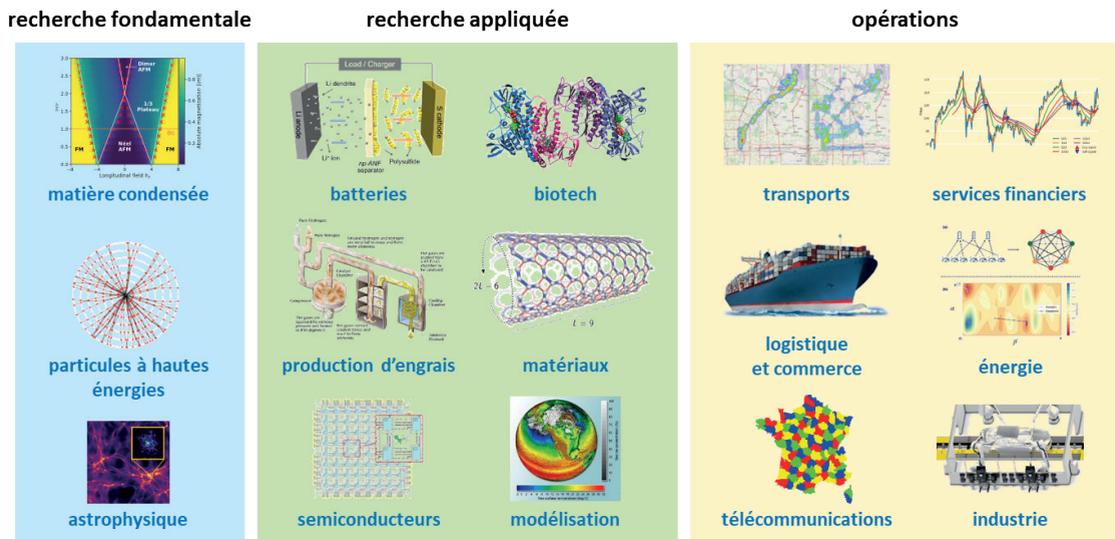


Figure 1: cartographie de cas d'usage en séparant les domaines de la recherche fondamentale, de la recherche appliquée et celui des opérations des entreprises. (cc) Olivier Ezratty, janvier 2025.

Le groupe de travail a auditionné plusieurs acteurs industriels français, dont des startups sur leurs cas d'usage potentiels du calcul quantique. Voici une synthèse de leurs cas d'usage identifiés.

1.7.2.1. APPLICATIONS DANS LA CHIMIE POUR LA DÉCOUVERTE DE MÉDICAMENTS

La chimie computationnelle vise à modéliser et à prédire le comportement des molécules afin de concevoir des médicaments atome par atome. C'est un domaine à la frontière entre la chimie et la mécanique quantique. Il est

crucial de reconsidérer les échelles de temps et de taille lorsqu'on essaie de prédire le comportement des molécules : un changement de nature survient lorsque l'on atteint des échelles suffisamment petites, lors du passage de la mécanique classique à la mécanique quantique.

L'objectif principal réside dans la découverte de médicaments grâce à l'exploitation de la précision accrue offerte par le calcul quantique. Parmi les algorithmes utilisés, on trouve le VQE (*Variational Quantum Eigensolver*) et la QPE (*Quantum Phase Estimation*). Le VQE, un algorithme hybride, combine des techniques d'optimisation classique et des routines quantiques. Il s'agit d'une heuristique, mais cela est très souvent le cas en chimie théorique, contrairement à la physique théorique. Le VQE est compatible avec le NISQ (*Noisy Intermediate-Scale Quantum*) et le FTQC, alors que la QPE représente une possibilité d'aller encore plus loin dans la précision, mais requiert du FTQC.

Simuler une molécule d'eau avec un ordinateur quantique requiert 400 à 600 qubits logiques. Avec 1000 qubits logiques, on pourrait résoudre des problèmes intéressants sur ce type de molécule. Pour des molécules plus grandes, dont on aurait besoin pour concevoir des vaccins par exemple, il faudra encore plus de qubits logiques.

1.7.2.2. APPLICATIONS DANS LA DÉFENSE

Les ambitions sont multiples: résoudre des problèmes intraitables par le HPC et résoudre des problèmes solubles plus vite ou à moindres coûts (énergétiques et économiques).

Les cas d'usage envisagés sont la résolution d'équations aux dérivées partielles pour des applications dans les optimisations d'antennes et de radars, les optimisations dans la commande de satellite et de leurs trajectoires, l'apprentissage machine comme pour la détection d'anomalies dans des images, les simulations Monte-Carlo pour la localisation et la simulation de matériaux.

Notons aussi, de façon orthogonale, la cryptographie (notamment le développement de la cryptographie post-quantique, qui requiert de tester des attaques quantiques).

1.7.2.3. APPLICATIONS DANS L'ÉNERGIE

Différents acteurs dans la production d'énergie électrique complètent leur expertise dans le calcul haute-performance par le calcul quantique en faisant le pari que, dans quelques années, ces acteurs pourront disposer d'ordinateurs quantiques de taille appropriée. Ces équipes travaillent sur la simulation de matériaux, les études de sûreté et les équations aux dérivées partielles. Elles s'intéressent aussi à l'optimisation de la recharge de véhicules électriques.

Jusqu'à présent, les études n'ont porté quasiment que sur de l'émulation, avec très peu de tests sur des machines réelles. Avec 100 à 1000 qubits logiques, il serait possible de résoudre des cas d'usage intéressants.

Un autre axe concerne la recherche des énergies fossiles, les acteurs s'intéressent aux cas d'usage du calcul quantique dans la chimie quantique, l'optimisation combinatoire, et la résolution d'équations aux dérivées partielles.

Parmi les cas d'usage intéressants sur la décarbonation de la production d'énergie, on trouve la simulation pour la capture de CO_2 et l'optimisation des fermes d'éoliennes. À partir de 300 qubits logiques, il semble possible de pouvoir résoudre des problèmes intéressants.

1.7.3. CLASSIFICATION PAR RESSOURCE

Nous terminons cette partie par une représentation graphique de ces cas d'usage en fonction des ressources nécessaires. La figure 2 inventorie des études de cas documentées avec des estimations de ressources précises et dans des papiers scientifiques. Les études de cas de la figure sont assez représentatives de ce qui est actuellement envisagé en fonction du nombre de qubits tolérants aux fautes disponibles et du nombre de portes quantiques à exécuter. La figure 3 inventorie quelques classes d'algorithmes avec leurs ressources logiques: nombre de portes logiques (génériques, portes-T ou Toffoli selon les cas, sachant que les portes-T et Toffoli sont souvent utilisées comme repère, car elles coûtent très cher à corriger par rapport aux autres portes quantiques comme les X, Z, H et CNOT), fidélité des qubits physiques ou logiques et nombre de qubits logiques. Les fourchettes correspondent à des études de cas avec problèmes et sous-problèmes. Ainsi, en matière

de simulation chimique pour la création de nouveaux procédés comme la recherche de nouveaux catalyseurs pour la production d'ammoniaque ou la création de matériaux résistant à la corrosion, plusieurs simulations sont nécessaires avec des composés et données recherchées de complexités différentes.

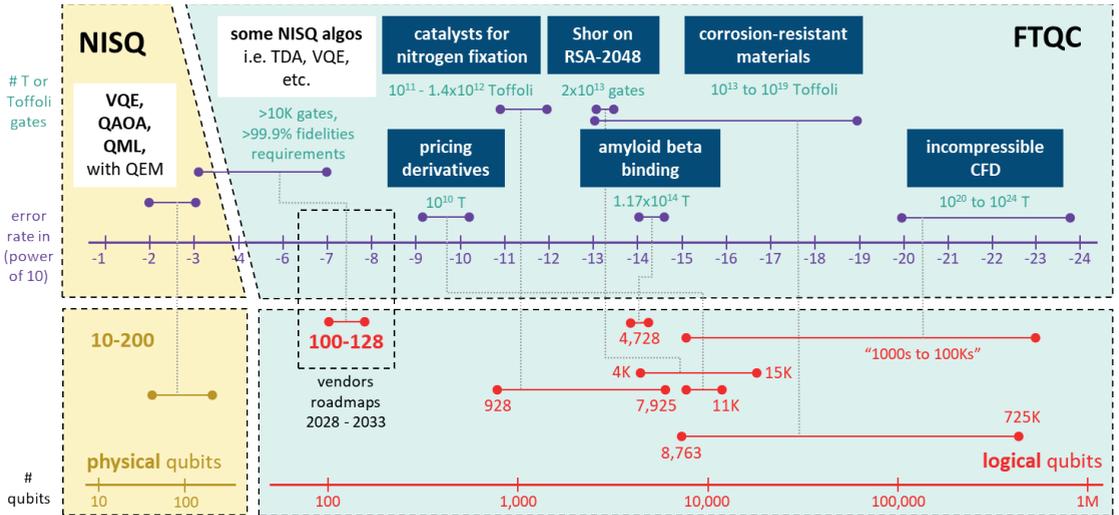


Figure 2: Cartographie des cas d'usage en fonction des ressources nécessaires. Elle illustre le fait que les applications générant le plus de valeur dans la simulation chimique et de matériaux, le calcul financier et la cryptanalyse demandent un très grand nombre de portes logiques ainsi que de qubits logiques. Les premières applications viables du calcul à tolérance aux fautes pourraient être celles qui sont conçues pour les ordinateurs quantiques bruités (NISQ), mais nécessitent des qubits en plus grande quantité et qualité que ce qui est actuellement disponible. (cc) Olivier Ezratty, janvier 2025.

Nous y retrouvons notamment¹⁸:

- **simulation de systèmes physiques quantiques**: VQE (en NISQ et FTQC), catalyseurs pour la fixation de l'azote (pour une production plus efficace d'ammoniac via le procédé Haber-Bosch), matériaux résistants à la corrosion, liaison bêta-amyloïde (en lien avec le traitement de la maladie d'Alzheimer);
- **problèmes de décision et d'optimisation**: QAOA (résolution de problèmes combinatoires en NISQ et FTQC), évaluation des dérivés financiers (dans les services financiers);
- **apprentissage automatique**: QML (en NISQ et FTQC), TDA (FTQC), pour l'analyse topologique des données, une méthode de clustering automatique relevant de l'apprentissage automatique;
- **problèmes d'ingénierie**: CFD incompressible, en mécanique des fluides;
- **cryptanalyse**: Algorithme de Shor pour RSA 2048.

On constate une sorte de glissement des scénarios d'usages. Une bonne partie des études de cas actuelles dites NISQ nécessitent en pratique des ordinateurs quantiques à tolérance aux fautes, y compris pour des algorithmes variationnels dont les circuits sont trop profonds pour être exécutés avec les processeurs actuels, y compris avec l'emploi de techniques de mitigation d'erreurs. Il est donc probable que les premiers cas d'usage des ordinateurs à tolérance aux fautes seront les algorithmes NISQ déjà conçus

18 Sources: TDA: [Towards Quantum Advantage on Noisy Quantum Computers](#) by Ismail Yunus Akhalwaya *et al.*, September 2022-March 2024, [Feasibility of accelerating homogeneous catalyst discovery with fault-tolerant quantum computers](#) by Nicole Bellonzi *et al.*, June 2024, [Real Option Pricing using Quantum Computers](#) by Alberto Manzano *et al.*, March 2023, [How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits](#) by Craig Gidney and Martin Ekerå, 2019, [Quantum Resources Required for Binding Affinity Calculations of Amyloid beta](#) by Matthew Otten *et al.*, June 2024, [Quantum computing for corrosion-resistant materials and anti-corrosive coatings design](#) by Nam Nguyen *et al.*, June 2024, [Feasibility of accelerating homogeneous catalyst discovery with fault-tolerant quantum computers](#) by Nicole Bellonzi *et al.*, June 2024, [Feasibility of accelerating incompressible computational fluid dynamics simulations with fault-tolerant quantum computers](#) by John Penuel *et al.*, June 2024.

et qui ont besoin de qubits ayant des fidélités dépassant les 99,9%. Cela va correspondre aux premières générations des ordinateurs à tolérance aux fautes avec une centaine de qubits logiques ayant des taux d'erreur allant de 10^{-4} à 10^{-8} .

Les cas d'usage actuellement identifiés pour les ordinateurs à tolérance aux fautes ont de leur côté besoin de ressources physiques qui iront au-delà de ces caractéristiques, avec des milliers de qubits logiques et plus de 10^{12} opérations, les TeraQops évoqués plus loin dans le document.

La société d'analystes GQI a créé une base de données alimentée par 174 études de cas en août 2024¹⁹. Elle a ensuite exploité l'outil Microsoft Azure *Resource Estimator* pour normaliser les estimations de ressources que l'on trouve dans la figure ci-dessous. Elle montre que, pour les cas de simulation chimique les plus intéressants (QPE, *Quantum Phase Estimation*), les temps de calcul sont prohibitifs sachant que les points positionnés entre le milieu et la droite des surfaces sont les plus crédibles en termes de fidélités de qubits physiques et de vitesse de portes quantiques. Ces simulations pourraient être réalisées en exécutant leur circuit en parallèle sur plusieurs processeurs quantiques indépendants. Cela ne sera envisageable qu'à la condition que le prix et le coût d'exploitation de chaque processeur soient raisonnables. En revanche, les simulations de dynamiques quantiques semblent pouvoir être réalisées dans des temps raisonnables (à gauche), mais toujours en requérant un très grand nombre de qubits physiques.

19 [The GQI Quantum Resource Estimator Playbook - Quantum Computing Report](#) by Doug Finke, *Quantum Computing Report*, August 2024.

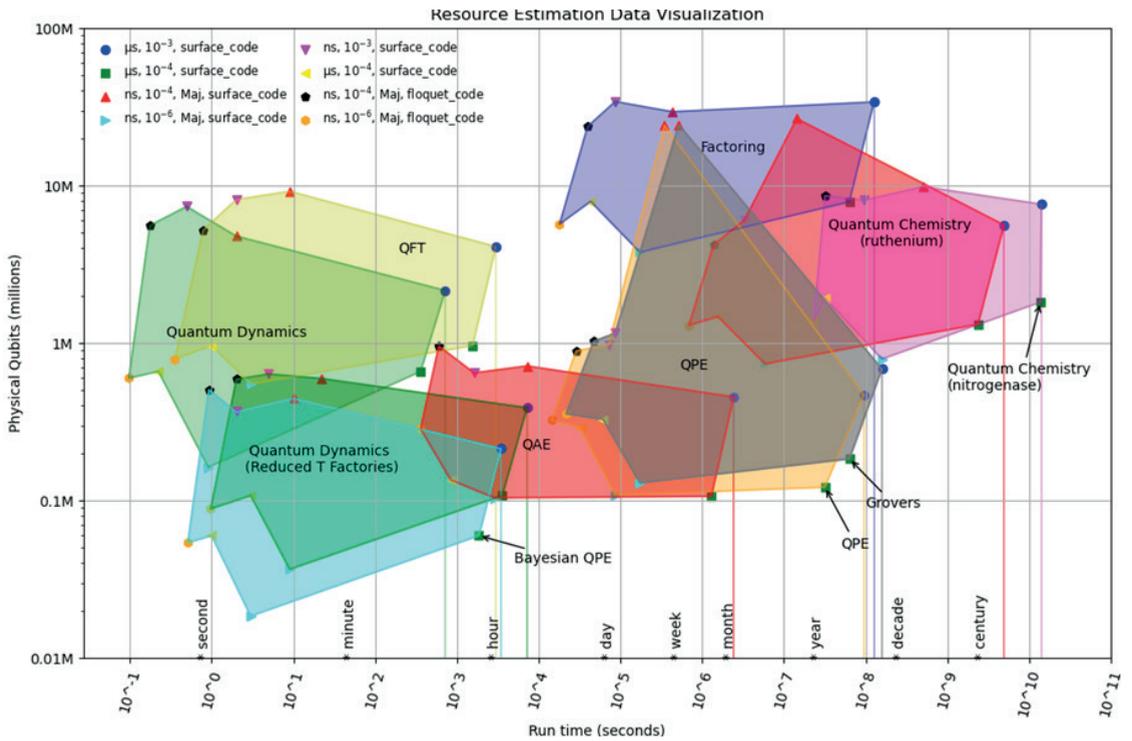


Figure 3: Classes d'algorithmes et leurs ressources physiques en nombre de qubits et en temps de calcul. ns = portes quantiques réalisées en environ 100 ns. μs = portes quantiques réalisées en environ 100 μs . Les puissances de 10 correspondent à des taux d'erreurs de portes physiques à deux qubits. Maj correspond aux qubits à base de fermions de Majorana de Microsoft (qui n'existent pas encore). Les autres correspondent aux qubits supraconducteurs (pour les portes en ns) ou ions piégés (pour les portes en μs).

Chapitre 2

LES CODES CORRECTEURS D'ERREURS

2.1. LA TOLÉRANCE AUX FAUTES, SEULE VOIE VERS DES ALGORITHMES QUANTIQUES PROFONDS²⁰

L'accélération des progrès expérimentaux pour le contrôle de systèmes quantiques a conduit en 2018 John Preskill à identifier l'ère du NISQ (*Noisy Intermediate-Scale Quantum*), c'est-à-dire ce moment de l'histoire où des processeurs quantiques de quelques centaines de qubits deviennent disponibles et peuvent tolérer des milliers d'opérations (ou portes) avant qu'une erreur ne se produise. Si ces nombres restent bien trop petits pour mettre en œuvre les algorithmes quantiques les plus connus, ils ont fait naître l'espoir de trouver des applications intéressantes pour ces processeurs qui sont à la limite de ce qu'on peut émuler avec des supercalculateurs classiques, par exemple par la mise en œuvre d'algorithmes d'optimisation. Cet espoir, poursuivi depuis quelques années par une grande partie de la communauté, est aujourd'hui largement déçu : il semble qu'un ordinateur quantique ne devienne utile que s'il peut effectuer un très grand nombre d'opérations logiques, au moins 10^{10} . L'ordre de grandeur typique est celui du TeraQuop, correspondant à 1000 milliards d'opérations logiques sans erreur. Par exemple, l'algorithme de factorisation de Shor pour casser RSA 2028 requiert une dizaine de TeraQuops (Eker, Gidney 2021). Les problèmes de simulations chimiques semblent être tout aussi gourmands en termes d'opérations logiques.

Atteindre ce régime du TeraQuop signifie que chaque opération élémentaire sur un ou deux qubits ne tolère qu'un taux d'erreur de l'ordre de 10^{-12} . De telles valeurs sont facilement accessibles pour des transistors classiques, mais beaucoup plus difficiles à obtenir dans le monde quantique. L'état de

²⁰ Un algorithme avec un très grand nombre de cycles de portes quantiques est dit « profond ».

l'art expérimental est aujourd'hui autour de 10^{-3} , et même si l'on peut espérer une amélioration d'un ou deux ordres de grandeur à l'avenir, il semble peu probable que l'on puisse gagner les 9 ordres de grandeur nécessaires simplement en améliorant les dispositifs expérimentaux que sont les qubits physiques et leurs systèmes de contrôle.

La solution heureusement est bien connue depuis les travaux fondateurs de Peter Shor et repose sur la correction d'erreur quantique et la tolérance aux fautes. Un temps pensée impossible à cause du caractère continu des états et des erreurs quantiques, la correction d'erreur repose désormais sur des bases théoriques solides. L'idée est ici d'encoder l'information logique, que l'on souhaite protéger, de façon délocalisée sur un grand nombre de systèmes physiques. Ces derniers sont typiquement perturbés par des phénomènes locaux, peu corrélés à longue distance, et qui ne seront pas en mesure d'accéder à l'information protégée. En particulier, des mesures de parité régulières vont permettre d'identifier les erreurs qui se sont produites et de les corriger. À moins de découvrir des mécanismes d'erreur complètement nouveaux où la nature conspirerait à perturber les systèmes physiques de manière à systématiquement interdire le calcul quantique, ces codes correcteurs quantiques permettront de protéger l'information logique au niveau requis pour effectuer les algorithmes que l'on souhaite.

Une notion cruciale dans ce contexte est celle de qubit logique, qui correspond à un bit quantique défini sur un espace physique de plus grande dimension. Cet espace peut consister en un grand nombre de systèmes physiques à deux niveaux, des qubits physiques donc, ou bien en un ou plusieurs modes bosoniques, qui sont des espaces de dimension infinie. Pour être utiles, ces qubits logiques doivent posséder deux propriétés importantes: leur état quantique doit pouvoir être manipulé grâce à des opérations physiques simples mises en œuvre sur les systèmes physiques qui les composent, et ces opérations doivent pouvoir être réalisées avec des niveaux d'erreurs plus bas que le niveau d'erreurs physiques intrinsèques. Ceci est obtenu grâce à la correction d'erreur quantique.

Ce que montre la théorie de la tolérance aux fautes, c'est que pour des modèles de bruit réalistes, il existe une valeur seuil pour le taux d'erreur physique, telle que si le vrai taux d'erreur est au-dessous de ce seuil, alors on peut en principe effectuer des calculs quantiques arbitrairement longs en encodant

l'information logique dans un plus grand nombre de qubits physiques. Les valeurs précises de ce seuil et surtout de la redondance nécessaire pour la tolérance aux fautes ne sont pas encore bien connues aujourd'hui, mais l'on anticipe que le seuil se situe autour de 0,001, et qu'un qubit logique pourrait être encodé dans un millier de qubits physiques, possiblement beaucoup moins. Ce coût est certes très important puisque l'on passe par exemple pour la factorisation d'un calcul impliquant quelques milliers de qubits parfaits à un processeur physique comprenant de l'ordre de la dizaine de millions de qubits physiques bruités, mais n'est pas rédhibitoire. Par ailleurs, ces valeurs sont probablement très pessimistes et des améliorations de plusieurs ordres de grandeur sont envisageables avec le développement de meilleures techniques de correction d'erreur.

2.2. CORRECTION D'ERREURS ET TOLÉRANCE AUX FAUTES

Il convient de distinguer deux objectifs assez différents. La *correction d'erreurs* concerne la protection d'une mémoire contre un type d'erreurs très spécifiques. C'est par exemple le cas pour les communications classiques : on encode l'information de manière redondante avant de la transmettre sur un canal imparfait sujet aux erreurs, et le récepteur cherche à corriger les erreurs afin d'obtenir le message envoyé. Une mémoire est similaire : dans ce cas, le canal imparfait correspond aux interactions entre la mémoire quantique et son environnement pendant le temps où l'information reste stockée, et le but est que l'information reste intacte le plus longtemps possible. Ce scénario suppose de façon cruciale que les erreurs soient circonscrites à l'étape de transmission de l'information, mais que l'on ait accès à des techniques d'encodage et de décodage idéales, non perturbées par le bruit. Ce scénario ne modélise que très imparfaitement la tâche pertinente dans le monde quantique, où chaque manipulation de l'information est inévitablement bruitée : on ne peut donc pas faire l'hypothèse d'un encodage ou d'un décodage parfait. Bien au contraire, chaque opération physique visant à corriger le bruit est elle-même source de bruit ! On se retrouve à écopier une barque trouée en son flanc avec un seau lui-même percé : si les trous sont trop importants, l'embarcation sombrera inéluctablement, mais si les trous sont suffisamment petits, des solutions théoriques existent bel et bien. Il s'agit dans ce cas de corriger les erreurs aussi vite qu'elles apparaissent. En fait, parvenir à maintenir le nombre d'erreurs physiques dans le système au-dessous du seuil de correction pendant tout le calcul est suffisant, car

la toute dernière étape du calcul quantique suppose une mesure de l'état de l'ordinateur qui retourne une information classique, le résultat du calcul. Cette information étant de nature classique, elle est facile à protéger avec des techniques de codage classique, et les erreurs résiduelles peuvent être corrigées sans difficulté. En poursuivant l'analogie de la barque, les passagers auront les pieds mouillés, car il n'est pas possible d'éliminer toutes les erreurs, mais une fois à bon port, il leur est possible de se les sécher, car des outils supplémentaires deviennent alors disponibles (correspondant à la correction d'erreurs classique).

En plus de devoir s'accommoder d'opérations physiques qui sont toutes imparfaites, l'autre défi auquel se confronte la *tolérance aux fautes* est que l'on ne souhaite pas simplement protéger l'information logique, mais au contraire être en mesure de la manipuler. On se retrouve ainsi tiraillé entre deux objectifs contradictoires : isoler l'information le mieux possible de son environnement afin de la protéger, tout en la rendant manipulable afin d'effectuer le calcul désiré. Ces deux ambitions sont pertinentes à la fois au niveau du système physique et à celui de l'information logique. Au niveau physique, on doit être en mesure d'appliquer des opérations physiques sur les qubits, ce qui requiert l'existence de lignes de contrôle pour chaque système, qui peuvent être sources d'interférences ou d'imprécisions problématiques. Au niveau logique, on souhaite être capable d'effectuer des opérations simples à mettre en œuvre pour ne pas trop permettre aux inévitables erreurs de se propager dans le système, tout en restant protégé dans un code quantique. On sait aujourd'hui que les approches les plus naïves pour atteindre cet objectif sont vouées à l'échec : par exemple, le théorème d'Eastin-Knill montre qu'un encodage où chaque porte logique serait obtenue en appliquant la même porte physique à chacun des qubits physiques sous-jacents ne peut pas permettre à la fois de corriger les erreurs et d'effectuer un calcul difficile pour un ordinateur classique. Plusieurs solutions pour contourner ce problème sont connues aujourd'hui, notamment la distillation d'états magiques, qui est un protocole tolérant aux fautes permettant de produire des états quantiques très purs, dits états magiques, à partir de copies bruitées : ces états, qui ne peuvent être obtenus directement dans un code de correction d'erreurs de type stabilisateur, sont nécessaires pour implémenter des portes non-Clifford, comme la porte T, et donc rendre le calcul quantique universel. La distillation repose sur des circuits composés uniquement d'opérations

Clifford et de mesures, et joue un rôle central dans l'architecture des calculateurs quantiques tolérants aux fautes.

Toutes les solutions pour contourner le problème de l'apparition d'erreurs illustrent la difficulté à effectuer des calculs quantiques dans un monde où les dispositifs expérimentaux sont nécessairement imparfaits.

La mission de la tolérance aux fautes est donc la suivante: étant donné un algorithme quantique que l'on souhaite mettre en œuvre, et un modèle de bruit réaliste pour le système physique encodant l'information, il faut trouver une façon de protéger et de manipuler l'information logique permettant d'émuler le calcul théorique envisagé. Ceci a toujours un coût en termes de redondance: combien de systèmes physiques sont nécessaires par qubit logique? Le but est alors de comprendre comment réduire le plus possible ce facteur. Les sources potentielles d'amélioration sont diverses: améliorer la qualité des systèmes physiques et de leur contrôle, trouver de meilleurs codes correcteurs quantiques, mettre au point des techniques plus efficaces pour manipuler l'information encodée au niveau logique. Les solutions théoriques les plus étudiées reposent sur l'utilisation du code de surface, qui vise à corriger deux types d'erreurs (bit-flip et phase-flip). Ces solutions envisagent un coût de l'ordre de 1000 à 10 000 qubits physiques par qubit logique pour des algorithmes tels que la factorisation. Des solutions plus récentes, reposant par exemple sur de nouveaux codes correcteurs plus efficaces ou sur des qubits dits bosoniques dotés de mécanismes d'autocorrection d'erreur qui permettent de protéger intrinsèquement les qubits contre un type de cause d'erreur (bit-flip). Ces solutions pourraient permettre de gagner plusieurs ordres de grandeur, et seront discutées au paragraphe 2.5.

2.3. LE PRINCIPE DE LA CORRECTION D'ERREUR QUANTIQUE

L'état d'un bit quantique est un vecteur $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ dans un espace complexe de dimension 2. Ici, α et β sont deux nombres complexes, appelés amplitudes, tels que $|\alpha|^2 + |\beta|^2 = 1$, et les deux vecteurs $|0\rangle$ et $|1\rangle$ correspondent aux états 0 et 1. Le fait que les amplitudes prennent un continuum de valeurs possibles n'est pas sans rappeler les calculateurs analogiques, pour lesquels on ne sait pas corriger les erreurs. Dans le cas quantique, il existe également une infinité d'erreurs possibles pouvant perturber l'état du système. La différence cruciale entre les deux scénarios provient de la linéarité de la

mécanique quantique : celle-ci garantit que si l'on sait corriger les erreurs correspondant à une base des erreurs possibles, on peut alors corriger n'importe quelle erreur. En particulier, il suffit de savoir corriger des erreurs de bits (qui échangent les états $|0\rangle$ et $|1\rangle$), les erreurs de phase (qui mettent une phase additionnelle -1 à l'état $|1\rangle$), ainsi que la combinaison de ces deux erreurs pour pouvoir corriger n'importe quelle erreur. En d'autres termes, on se ramène à un modèle discret d'erreurs, où l'on doit considérer deux fois plus d'erreurs que dans le cadre de la correction d'erreur classique : les erreurs de bits sont les mêmes qu'en classique, et les erreurs de phase sont nouvelles et spécifiques au calcul quantique.

En particulier, les travaux de Daniel Gottesman qui a défini les codes stabilisateurs, ainsi que ceux de Calderbank, Shor et Steane permettent d'importer beaucoup de techniques de correction d'erreur classiques dans le monde quantique. L'idée générale est d'encoder un certain nombre de qubits logiques dans un plus grand nombre de qubits physiques, et de mesurer des parités pour projeter la vraie erreur sur une erreur de bit ou de phase, puis d'utiliser un algorithme de décodage classique pour identifier l'erreur en question et la corriger.

2.4. L'ÂGE D'OR DU CODE DE SURFACE

Rapidement, après les travaux pionniers mentionnés plus haut, le chercheur Alexei Kitaev a découvert un code correcteur quantique remarquable : le code de surface. Ce code permet d'encoder un qubit logique en un arrangement planaire d'un ensemble de $L \times L$ qubits physiques sur une grille carrée, avec une connectivité entre qubits voisins, parfaitement adaptée aux architectures à base de qubits supraconducteurs. Au-dessous du seuil, le taux d'erreur logique p_{log} décroît très rapidement avec le taux d'erreur physique p_{phys} . Ce code, et ses généralisations connues sous le nom de codes topologiques, dont les propriétés sont intimement liées à celles de la variété topologique (surface 2D ou code défini en 3 dimensions) qui les définit, ont été particulièrement étudiés depuis près de 20 ans. En particulier, on sait corriger les erreurs de façon efficace, et mettre en œuvre des portes logiques sur ces codes. Par exemple, l'idée générale pour faire du calcul quantique avec ces codes est d'encoder chaque qubit logique dans un code de surface. Les opérations logiques sont ensuite réalisées avec des techniques dites de chirurgie visant à combiner puis re-séparer deux codes de surface,

ainsi qu'avec de la distillation d'états magiques. En prenant la valeur de L suffisamment grande, typiquement autour de 30, on peut s'assurer que toutes les opérations logiques ont le niveau d'erreur souhaité, et donc avec un surcoût d'environ 1000 qubits physiques par qubit logique pour le régime du TeraQuop sachant que ce nombre dépend étroitement de la fidélité des portes quantiques physiques, qui a tendance à s'améliorer graduellement.

Pendant longtemps, les chercheurs ont pensé avoir tenu le code ultime pour le calcul quantique. La limitation à des architectures locales en deux (ou éventuellement trois) dimensions était dictée par les contraintes physiques des circuits supraconducteurs, et l'on sait aujourd'hui que le code de surface est essentiellement optimal en deux dimensions. Par ailleurs, les propriétés topologiques du code sont mises à profit pour mettre au point des portes logiques qui ne propagent pas les erreurs pendant le calcul. Pour ces raisons, les recherches sur des approches alternatives sont restées assez confidentielles pendant cette période.

État de l'art expérimental : plateforme des supraconducteurs

Avec les avancées des quinze dernières années sur la conception des qubits supraconducteurs, les techniques de nanofabrication, et les méthodes de filtrage de l'environnement micro-onde, cette plateforme a atteint la maturité nécessaire pour la réalisation des codes correcteurs d'erreur avec des taux d'erreurs physiques en dessous du seuil de la tolérance aux fautes. Parmi les qubits supraconducteurs, le transmon, par la simplicité de son design et ses très bons temps de cohérence, est actuellement le choix numéro un de plusieurs acteurs industriels et académiques pour la mise à l'échelle vers un ordinateur quantique tolérant aux fautes.

La contrainte de connectivité 2D sur une puce limite largement le choix de codes correcteurs d'erreur. En effet, l'approche dominante, suivie par exemple par Google et IBM, est de réaliser un code de surface à base de transmons. Dans une expérience récente publiée dans *Nature* en 2023,

l'équipe de Google a démontré, sur une puce constituée de 72 transmons, la réalisation d'un code de surface de distance 3 puis 5, correspondant respectivement à des tailles de 3×3 et 5×5 qubits physiques. Dans cette expérience, l'ensemble des qubits bénéficient de fidélités de portes à un qubit de l'ordre 99,9% -99,95% (soit des taux d'erreur de 0,0005 à 0,001) et de portes à deux qubits de l'ordre 99% -99,8%. Toutefois, la lecture des qubits est moins fidèle (96% -99%) et surtout souffre d'une durée très longue par rapport aux autres opérations (500 ns versus 25 ns pour les portes à 1qubit et 34 ns pour les portes à 2 qubits). À cette durée, il faudrait ajouter un temps de réinitialisation de 160 ns. Cette lenteur et l'infidélité du processus de mesure ainsi que les erreurs de portes à 2 qubits sont les principaux responsables d'un taux d'erreur de l'ordre de 2% à 4% par cycle de correction d'erreur. L'équipe de Google a néanmoins réussi à démontrer une légère amélioration du taux d'erreur logique en passant de $3,028 \pm 0,023\%$ (pour un code de surface de distance 3) à $2,914 \pm 0,016\%$ par cycle de correction d'erreur (pour un code de surface de distance 5). Cela indique que les performances moyennes des composants physiques dans cette expérience sont au niveau du seuil de tolérance aux fautes. Cette expérience représente l'implémentation la plus complète d'un protocole de correction d'erreur quantique à ce jour parmi toutes les plateformes existantes : réalisation de plusieurs cycles de corrections d'erreur répétés ainsi que la mise à l'échelle de distance 3 à distance 5. Une amélioration rapide des performances de cette réalisation est envisageable dans les années à venir. En effet, le composant majeur d'erreur physique par cycle de correction d'erreur correspond à la durée et la fidélité de la lecture des transmons. Toutefois, les performances atteintes dans l'expérience de Google ne sont pas au niveau de l'état de l'art. Notamment, avec une intégration des dernières techniques de filtrage, des groupes académiques (ETH Zurich, Riken) ont démontré des lectures bien plus rapides et fidèles (typiquement une durée de lecture de 40 ns et fidélité de 99,6%). Lors de la rédaction de ce rapport, des nouvelles avancées de l'équipe de Google sont apparues sous forme d'une prépublication sur arXiv (arXiv: 2408.13687). Dans cette prépublication, l'équipe de Google annonce la réalisation de deux nouvelles puces à 72 et à 105 qubits avec les fidélités de mémoire quantique améliorées par rapport à l'expérience de 2023. Cette amélioration est attribuée aux temps de relaxation T_1 et temps de cohérence T_2 plus élevés

(un facteur 3). Ces avancées permettent à l'équipe de démontrer le fonctionnement d'un code de surface de distances 3, 5 et 7 en dessous du seuil de tolérance aux fautes (par un facteur 2,14). Notamment, les codes de distance 5 et 7 atteignent aussi le *break-even* correspondant à un taux d'erreur logique par cycle de correction d'erreur moins élevé que le composant physique du système le plus cohérent. Enfin, la puce à 72 qubits est munie d'un décodeur temps réel avec une latence en moyenne de 63 microsecondes à distance 5 (à comparer avec le temps de cycle de correction d'erreur de 1,1 microseconde).

Il paraît plausible que cette approche atteigne à court terme un niveau de maturité où le taux d'erreur physique serait jusqu'à un ordre de grandeur au-dessous du seuil de tolérance aux fautes, sur des puces avec plusieurs centaines de qubits. Toutefois, même avec ce niveau de performance, nous aurons besoin d'un millier de transmons par qubit logique pour atteindre après correction d'erreurs des taux d'erreurs de l'ordre de 10^{-10} par cycle de correction d'erreur. Par ailleurs, pour assurer une correction d'erreur efficace par le code de surface, il faudrait éliminer les sources d'erreurs qui agissent de manière corrélée sur les qubits physiques du code de surface. Ces dernières années, deux sources majeures de corrélation ont été identifiées et étudiées: la fuite de la population de transmon vers des états excités au-delà de l'espace de calcul, qui peuvent ensuite se propager dans le circuit pour créer des corrélations problématiques d'erreurs dans le temps et l'espace; l'impact d'événements à haute énergie conduisant à la création de phonons se propageant dans le substrat et générant ainsi une surpopulation de quasi-particules dans tout l'échantillon. Ces deux sources d'erreurs corrélées ont été étudiées ces dernières années et des solutions ont été envisagées. L'expérience récente de Google montre qu'en appliquant ces solutions, des taux d'erreur logique de 10^{-10} sont potentiellement atteignables, mais qu'aller en dessous de ces taux nécessiterait la correction d'erreurs corrélées de natures différentes.

Avec ce surcoût important de la correction d'erreur (autour de 1000 transmons par qubit logique), une mise à l'échelle au-delà d'un qubit logique viendrait certainement avec des complications. Des systèmes plus grands, par exemple pour démontrer des portes logiques tolérantes aux fautes ou pour distiller des états magiques pour des portes non

Clifford, nécessitent certainement des avancées au niveau de la science des matériaux, par exemple pour mieux comprendre et contrôler la création des systèmes à 2 niveaux parasites qui viennent perturber le fonctionnement de ce système multiqubits. En parallèle de la recherche sur ce type de problème, permettant la maturation de la plateforme à base de transmons, les acteurs académiques et industriels travaillent aussi sur des voies alternatives permettant de réduire, parfois de manière significative, le surcoût de la correction d'erreur. Voici à titre d'exemple deux approches dominantes dans le contexte des circuits supraconducteurs :

- Remplacer les qubits transmon par d'autres qubits supraconducteurs : plusieurs candidats (Fluxonium, heavy Fluxonium, qubit $0-\pi$, qubit $\cos - 2\phi - \dots$) avec des niveaux de maturité différents sont actuellement étudiés. Ces qubits peuvent assurer un niveau de protection intrinsèque contre les sources dominantes de bruit (bruit de charge ou de flux), et permettent d'espérer atteindre plus facilement des taux d'erreur inférieurs (parfois bien inférieurs) au seuil de la tolérance aux fautes. Cela impliquerait qu'un code de surface de taille plus petite serait suffisant pour atteindre un taux d'erreur logé donné.
- Encodage *dual-rail* remplaçant les erreurs prises en compte par les codes de surface (bit-flip, phase-flip) par des erreurs d'*erasure* (effacement) : dans cette approche inspirée de la plateforme photonique (poursuivie par exemple par la startup QCI et par AWS), l'information d'un qubit est encodée sur l'état d'une excitation de deux modes supraconducteurs. Ainsi, la relaxation énergétique, comme source majeure de bruits des qubits, implique un effacement de l'information avec une transition vers l'état à zéro excitation, mais qui peut être observée par une lecture efficace de cet état. Cela donne lieu à un remplacement au premier ordre des erreurs de Pauli dominant par des erreurs d'effacement qui sont plus facilement corrigibles par un code de surface. En absence des erreurs de Pauli, cette simplification se traduit par un seuil de correction d'erreur passant de 0,5% à autour de 4%.

2.5. DE NOUVELLES APPROCHES MOINS GOURMANDES EN HARDWARE

Si le code de surface a longtemps été considéré comme la voie royale vers le calcul quantique tolérant aux fautes, de nouvelles idées ont émergé ces dernières années, et ont largement rebattu les cartes, à tel point qu'il est aujourd'hui très difficile d'identifier quelle architecture permettra de réaliser le calcul quantique tolérant aux fautes en premier. Deux hypothèses de base ont en effet été remises en question, à savoir le fait que l'on doive nécessairement encoder l'information physique sur des systèmes à deux niveaux et que les systèmes physiques soient contraints à une connectivité locale en deux dimensions. La remise en cause de la première hypothèse a conduit entre autres au développement des codes bosoniques, celle de la connectivité locale a permis l'avènement des codes LDPC quantiques ou qLDPC (*low-density parity-check*, c'est-à-dire des codes avec une faible densité). Ces deux voies offrent des perspectives remarquables en termes de réduction du nombre de systèmes physiques par qubit logique, typiquement d'un ordre de grandeur.

Dans les deux cas, les idées théoriques ne sont pas complètement nouvelles puisque des codes bosoniques avaient été étudiés dès la fin des années 90 dans le cadre des codes photoniques et des codes LDPC quantiques considérés au début des années 2000. Mais l'intérêt renouvelé pour ces approches exotiques repose sur des considérations expérimentales récentes. Par exemple, l'utilisation de fortes non-linéarités produites par des jonctions Josephson dans les circuits supraconducteurs permet de réaliser avec des photons micro-ondes ce qui n'était pas possible avec des photons optiques. D'autre part l'avènement de plateformes comme celle des atomes neutres permet de coupler des qubits arbitraires en déplaçant les atomes correspondants, et donc de se libérer de la contrainte des codes locaux en deux dimensions, au prix, cependant de portes quantiques à deux qubits qui sont pour l'instant très lentes (1 ms).

D'un point de vue informatique et codes correcteurs d'erreurs, ces deux approches illustrent parfaitement l'importance de la créativité pour résoudre des problèmes tels que la tolérance aux fautes. Le terrain de jeu est immense et il est à peu près certain que les solutions qui sont envisagées aujourd'hui ne seront pas celles qui seront déployées à terme, trop de voies restantes inexplorées à ce jour.

Ce que les codes bosoniques remettent en question, c'est l'idée qu'il faille encoder les qubits logiques sur des systèmes physiques à deux niveaux. En fait, pour un grand nombre de systèmes physiques, il n'existe pas nécessairement deux niveaux très naturels pour encoder un qubit physique. Par exemple, l'état du champ micro-ondes confiné par un circuit supraconducteur est décrit par un espace de Hilbert de dimension infinie, appelé espace de Fock, et l'approche traditionnelle est de considérer les deux niveaux de plus basse énergie pour définir un qubit physique. Pour cela, on ajoute une jonction Josephson au circuit qui génère une anharmonicité permettant de bien découpler les deux premiers niveaux des niveaux d'énergie plus élevés. Se débarrasser ainsi des autres niveaux a un coût expérimental et une idée intéressante est de comprendre si, au contraire, on ne pourrait pas faire de ces autres niveaux un atout pour la correction d'erreur. Après tout, le principe même de la correction d'erreur est d'exploiter la redondance physique pour protéger de l'information logique. L'idée des codes bosoniques est ainsi de définir un meilleur qubit au sein de cet espace de dimension infinie. Par exemple, l'espace engendré par deux états cohérents $|\alpha\rangle$ et $|\!-\alpha\rangle$, d'amplitudes opposées α et $-\alpha$, est le choix mis en avant par le qubit de chat. Expérimentalement, ce qubit peut être stabilisé grâce à une jonction Josephson. L'intérêt théorique de ce nouveau qubit physique est qu'il est déjà partiellement protégé grâce à la redondance offerte par le code bosonique. En particulier, en choisissant la valeur de α suffisamment grande, le qubit est intrinsèquement protégé contre les erreurs de bit, et l'encodage logique a juste besoin d'assurer une protection supplémentaire contre les erreurs de phase. Ceci peut être mis en œuvre grâce à un simple code classique, ce qui réduit dramatiquement le coût d'un qubit logique. Bien sûr, de nouvelles complications apparaissent avec ce schéma : en particulier, il est crucial que le circuit physique ne transforme jamais les inévitables erreurs de phase en erreurs de bit, qui sont supposées avoir été traitées par le code bosonique.

Ce qubit de chat n'est qu'une possibilité parmi une multitude d'autres. Par exemple, un encodage potentiellement plus intéressant est celui du code GKP dû à Gottesman, Kitaev et Preskill, qui permet une protection simultanée (mais partielle) contre les deux types d'erreur. Ceci est obtenu au prix d'une stabilisation plus complexe du qubit physique, mais pourrait être une solution très intéressante à plus long terme.

État de l'art expérimental : les supraconducteurs, les ions et la photonique

La non-linéarité forte et sans dissipation assurée par les jonctions de Josephson, permet de générer, manipuler et stabiliser les états non classiques du champ micro-ondes. Les qubits de chat peuvent ainsi être stabilisés par un mécanisme d'échange à deux photons. Une expérience récente de la startup Alice&Bob et l'équipe Qumatic (ENS, Mines, Inria, CNRS) montre que les qubits ainsi stabilisés sont exponentiellement protégés contre les erreurs de bit, atteignant des temps de bit *flip* de l'ordre de dix secondes (une amélioration de 6 à 7 ordres de grandeur par rapport au cas non protégé). Cette expérience démontre aussi l'implémentation d'une porte à un qubit (rotations autour de l'axe Z) maintenant la même protection. Pour corriger l'autre type d'erreur, les erreurs de phase, il suffit alors d'utiliser les codes correcteurs d'erreur conventionnels, ne corrigeant qu'un seul type d'erreur comme dans le cas des communications classiques, et qui peuvent maintenant être très proches d'un code classique (avec quelques spécificités liées au fait qu'on souhaite pouvoir effectuer des opérations logiques qui n'introduisent pas non plus d'erreurs de bit). Cela donne lieu à plusieurs simplifications et raccourcis au niveau du surcoût matériel: il est par exemple possible de concaténer un tel encodage avec un code LDPC classique dans une architecture 2D et atteindre des taux d'encodage très intéressants. Une démonstration de portes (notamment la porte CNOT à deux qubits) préservant la protection intrinsèque contre les *bit-flip*, ainsi qu'une mise à l'échelle vers des dizaines de qubits de chat pour démontrer la correction des flips de phase, sont les étapes suivantes pour démontrer la viabilité de cette approche. Il s'agit de l'approche suivie par la startup Alice&Bob ainsi que par AWS. Par ailleurs, l'encodage GKP (poursuivi par exemple par la startup québécoise Nord-Quantique) assure une protection bas niveau plus symétrique, éliminant à la fois les erreurs de bit et les erreurs de phase. Une démonstration de cette correction bas-niveau tolérante aux fautes (qui élimine la propagation des erreurs du système de mesure de syndromes vers les erreurs non corrigibles de l'oscillateur harmonique), des portes logiques préservant la protection ainsi que la mise à l'échelle dans un petit code de surface, sont des étapes nécessaires pour démontrer la viabilité de

cette approche. En parallèle de ces avancées sur la plateforme des supraconducteurs, des expériences similaires sont menées à l'ETH de Zurich sur la plateforme des ions piégés. Ici, l'information est encodée dans des états GKP du mode de vibration d'un ion. La non-linéarité, nécessaire pour la génération des états, la mesure des syndromes, et la correction d'erreur, est assurée par le couplage de ce mode vibrationnel à l'état interne de l'ion. L'état d'avancement de ces expériences est assez similaire au cas des expériences GKP avec les circuits supraconducteurs.

Avec des qubits photoniques, le paradigme de calcul privilégié est celui du calcul quantique basé sur la mesure (*Measurement-Based Quantum Computing* - MBQC)²¹, qui s'appuie sur un réseau de qubits intriqués et des mesures par couches de qubits successives. Cette approche est également universelle (voir chapitre 1) et a donc la même puissance calculatoire que le modèle le plus répandu des circuits quantiques, et elle peut également être rendue tolérante aux fautes^{22,23}. Dans ce cas, les codes correcteurs d'erreur décrits plus haut se déclinent dans une version MBQC par le procédé de foliation, et il existe en outre des codes correcteurs spécifiquement construits pour le modèle MBQC qui n'ont pas de pendant par circuit²⁴. Pour exécuter un calcul en MBQC, il faut disposer préalablement d'un grand réseau de qubits intriqués. Celui-ci peut être créé au fur et à mesure que le calcul avance, mais un certain nombre de qubits et de liens d'intrication doivent tout de même exister simultanément, et produire un tel réseau de qubits intriqués n'est pas facile. Un moyen de répondre à ce défi est de créer des petits états intriqués, dits états-ressources, et d'intriquer ces états entre eux à l'aide d'opérations dites de fusion²⁵, qui correspondent à une mesure de Bell, un type de mesure à deux qubits particulièrement bien adapté à la

-
- 21 R. Raussendorf, H. J. Briegel, "A one-way quantum computer", *Phys. Rev. Lett.* **86** 5188–5191 (2001).
 - 22 R. Raussendorf, J. Harrington, K. Goyal. "A fault-tolerant one-way quantum computer", *Annals of physics*, **321**(9):2242–2270 (2006).
 - 23 H. J. Briegel, D. E. Browne, W. Dür, R. Raussendorf, M. Van den Nest. "Measurement-based quantum computation", *Nature Physics*, **5**(1):19–26 (2009).
 - 24 N. Nickerson, H. Bombín, "Measurement-based fault tolerance beyond foliation", *arXiv*:1810.09621 (2018).
 - 25 D. E. Browne, T. Rudolph, "Resource-Efficient Linear Optical Quantum Computation", *Phys. Rev. Lett.* **95** 010501 (2005).

photonique. Cependant, les opérations de fusion sont probabilistes, et construire un réseau de qubits intriqués de la sorte repose sur la théorie de la percolation : des fusions entre plus de qubits que nécessaire à l'état souhaité sont réalisées, et si la probabilité de succès de chaque fusion est suffisamment importante, l'état visé pourra être réalisé. Une approche plus récente, dite calcul quantique basé sur la fusion (*Fusion-Based Quantum Computing* - FBQC)²⁶ prend directement en compte ce procédé de fusion, et permet d'intégrer la nature probabiliste de la fusion dans le protocole de correction d'erreurs. Une architecture de calcul en FBQC correspond alors à la spécification d'un type d'état-ressource et d'un réseau de fusion, et, pour un réseau de fusion donné, un calcul est spécifié par le choix des bases de mesure pour les différentes fusions.

Avec des photons, les démonstrations de correction d'erreur à petite échelle sont plus difficiles qu'avec des qubits stationnaires, car les photons sont consommés au fur et à mesure de l'exécution des portes. L'effet de seuil caractérisant le passage dans une région où la correction d'erreur est avantageuse est donc plus marqué, et il est difficile de réaliser des expériences où les erreurs logiques sont du même ordre de grandeur que les erreurs physiques, comme c'est le cas avec les expériences décrites ci-dessus pour des qubits supraconducteurs, des atomes ou des ions piégés. Des démonstrations de correction d'erreurs existent toutefois, comme la réalisation d'un code Shor encodant un qubit logique sur neuf qubits²⁷ et sont utiles pour le développement du calcul aussi bien que pour des communications quantiques. Mais certains acteurs trouvent plus probant de démontrer que les composants de base sont en passe d'atteindre les valeurs nécessaires pour passer le seuil et de se concentrer sur la capacité de fabrication qui permettra le passage à l'échelle²⁸, plutôt que de réaliser des preuves de concept à petite échelle. Enfin, lorsque plusieurs degrés de liberté sont disponibles, par exemple avec des émetteurs quantiques dotés d'un spin contrôlable,

26 S. Bartolucci, P. Birchall, H. Bombín, *et al.* "Fusion-based quantum computation", *Nat. Commun* **14** 912 (2023).

27 R. Zhang *et al.* "Loss-tolerant all-photon quantum repeater with generalized Shor code", *Optica* **9** 152 (2022).

28 K. Alexander *et al.* "A manufacturable platform for photonic quantum computing", *arXiv:2404.17570* (2024).

des architectures hybrides sont envisageables, ce qui permet une grande modularité dans la mise en œuvre des protocoles de correction d'erreurs et de tolérance aux fautes^{29,30}.

Même en se cantonnant à des qubits physiques définis sur des systèmes à deux niveaux, il est possible de faire bien mieux que le code de surface. Pour cela, l'idée est d'autoriser des connexions entre des qubits qui ne sont pas voisins sur une grille bidimensionnelle. Dans ce cas, si l'on requiert toujours que les diverses parités à mesurer pour la correction d'erreur ne fassent intervenir qu'un petit nombre de qubits, on a affaire à un code dit LDPC quantique. L'intérêt de ces codes est qu'ils offrent des performances bien supérieures à celles du code de surface. Quand ce dernier encode k qubits logiques dans $k L^2$ qubits physiques tout en pouvant corriger des erreurs affectant $(L-1)/2$ qubits, les codes LDPC quantiques permettent eux d'encoder k qubits logiques dans ck qubits physiques et de corriger des erreurs affectant $c'k$ qubits, pour des constantes $c, c' > 0$. Si ces résultats d'existence sont théoriques pour le moment, des petits codes LDPC quantiques ont déjà été optimisés notamment par IBM et permettent un gain d'un facteur 10 en termes de redondance par rapport au code de surface pour encoder 12 qubits logiques pendant un million de cycles de correction d'erreur [Bravyi *et al*, *Nature* 2024]. Ici également, cette amélioration est accompagnée de difficultés nouvelles, par exemple sur comment manipuler efficacement l'information logique encodée grâce à ces codes. L'approche théorique des chercheurs d'IBM vise la plateforme des circuits supraconducteurs et propose une architecture biplanaire avec des coupleurs *long-distances*. Alors qu'une architecture biplanaire paraît la bonne voie avec le développement de la technologie *flip-chip*, l'efficacité des coupleurs *long-distances* reste à être prouvée par des expériences. D'autres plateformes, notamment celles basées sur les atomes, se prêtent particulièrement bien à ces encodages au-delà d'une connectivité 2D.

29 S. Simmons, "Scalable Fault-Tolerant Quantum Technologies with Silicon Color Centers", *PRX Quantum* **5** 010102 (2024).

30 G. de Gliniasty *et al*. "A Spin-Optical Quantum Computing Architecture", *Quantum* **8** 1423 (2024).

État de l'art expérimental : plateforme des atomes neutres

Les atomes neutres piégés dans des pinces optiques ont vu un sursaut significatif dans leur degré de contrôlabilité durant les dernières années. Ces avancées majeures ont promu cette plateforme, développée initialement comme candidat idéal pour la simulation analogique de systèmes multicorps quantiques, vers un excellent candidat pour le calcul quantique digital tolérant aux fautes. L'encodage de l'information quantique dans les états hyperfins d'horloge de l'atome piégé (Rubidium dans le cas des startups Pasqal et QuEra) assure la robustesse (les temps de cohérences longs). Ensuite, une excitation vers les niveaux de Rydberg assure une interaction forte entre les atomes pour implémenter des portes à 2 qubits (ou multiqubits) de haute fidélité.

Plus précisément, les portes à un qubit sont implémentées par des processus Raman et atteignent aujourd'hui des fidélités de l'ordre de 99,97%, avec des durées de l'ordre de 500 ns. Les portes à deux qubits de CZ reposent sur le phénomène de blocage de Rydberg : en approchant deux atomes, le passage d'un atome par le niveau de Rydberg interdit le passage de l'autre. Il est ainsi possible de préparer des états intriqués de deux atomes en proximité et en bénéficier pour implémenter une porte CZ. Dans les expériences récentes à Harvard et QuEra, des fidélités de l'ordre de 99,5% et des temps de porte de 200 ns ont été démontrés. La lecture haute-fidélité de ces qubits est assurée par l'imagerie de la fluorescence. Alors que des hautes fidélités de l'ordre de 99,9% ont été démontrées, ces mesures souffrent de certaines limitations. Les mesures non destructives sont possibles, mais restent très lentes par rapport aux autres opérations (dizaines de millisecondes). Une mesure relativement rapide (10 microsecondes) est possible, mais est accompagnée par la perte des atomes mesurés. Il est donc nécessaire de remplacer, en permanence et de manière efficace, ces atomes mesurés par des atomes fraîchement préparés.

Au niveau de l'architecture de calcul, cette plateforme diffère largement des circuits supraconducteurs. Les qubits supraconducteurs bénéficient chacun de leur ligne de contrôle et de lecture, ce qui rend possible l'implémentation des circuits logiques complexes et assure une

décorrélation des erreurs de contrôle. En revanche, cela vient certainement avec des complexités liées à la mise à l'échelle et au multiplexage. De plus, cette plateforme est limitée par une connectivité 2D ou proche de 2D (e.g. biplanaire). L'adressage des atomes neutres, pour des opérations à un qubit, peut se faire de manière directe en combinant une excitation micro-onde globale, et les faisceaux laser focalisés, pour produire des déplacements lumineux de fréquences sur des qubits sélectionnés. Mais pour toutes autres opérations (portes multiqubits et la lecture) et même pour une mise à l'échelle plus facile avec des opérations à un qubit, l'approche la plus prometteuse consiste à transporter les atomes de manière cohérente à l'aide des défecteurs acousto-optiques 2D. En transférant les atomes dans des zones appropriées, il est alors possible d'effectuer l'opération nécessaire sur plusieurs atomes de manière simultanée. Cette approche diminue de manière significative le nombre de lignes de contrôle. De plus, ce transport peut permettre d'atteindre des connectivités plus ou moins arbitraires, ce qui peut rendre possible l'implémentation de codes LDPC de performances bien meilleures que le code de surface. Toutefois, cette parallélisation des opérations peut être accompagnée par des limitations du type erreurs corrélées. Typiquement, le bruit de laser qui excite collectivement les atomes peut donner lieu à des erreurs corrélées sur ces atomes. Il est donc nécessaire de démontrer dans les prochaines expériences que cette corrélation ne constitue pas une limite dure à l'efficacité de la correction d'erreur.

Dans une expérience récente, publiée dans *Nature* en 2024, l'équipe de Harvard et la startup QuEra combinent ces capacités pour réaliser un ensemble de briques de base d'un ordinateur tolérant aux fautes sur un dispositif constitué de 280 qubits. Cela inclut la préparation des états logiques d'un code de surface de distances 3, 5 et 7 et la réalisation d'une porte CNOT transversale entre deux qubits logiques ainsi encodés. Au-delà du code de surface, les auteurs ont réalisé plusieurs qubits logiques encodés dans des codes couleur 2D encodant un qubit logique dans 7 qubits physiques, avec une distance 3, et utilisés par la suite dans une préparation tolérante aux fautes d'un état intriqué GHZ (Greenberger-Horne-Zellinger) entre 4 qubits logiques ainsi encodés. Ils démontrent également leur capacité à effectuer des lectures mi-circuits efficaces en réalisant un protocole de téléportation d'intrication par *feed-forward*.

Enfin, la connectivité plus riche entre les qubits leur permet de préparer les états logiques des codes détecteurs d'erreur 3D encodant 3 qubits logiques dans 8 qubits physiques avec une distance 2, qui permettent notamment de réaliser des portes non Clifford CCZ de manière transversale au sein d'un bloc de code.

Malgré cet ensemble impressionnant de démonstrations, l'expérience se limite à la préparation et la manipulation des états de codes et non pas à la correction des erreurs par des mesures répétées des syndromes d'erreurs. Il reste donc à démontrer que l'implémentation de la correction d'erreur peut en effet donner lieu à une amélioration exponentielle des taux d'erreurs. L'obstacle majeur dans ce cadre est dû au fait que les erreurs dominantes des opérations de cette plateforme ne sont pas des erreurs de Pauli pour lesquelles ces codes ont été conçus. Notamment, deux types d'erreurs majeures sont la fuite de l'information en dehors de l'espace de calcul et la perte des atomes dans les pinces optiques. Pour le premier type d'erreur, il est possible de convertir ces erreurs de fuite vers des effacements, similaires à celles discutées dans l'approche alternative 2 des circuits supraconducteurs. Mais cela nécessiterait certainement de remplacer le rubidium par d'autres espèces atomiques comme l'ytterbium ou le strontium. En effet, la structure plus riche des niveaux d'énergie électronique de l'ytterbium et le strontium permet d'observer la fuite de la population et de ramener l'atome dans l'espace computationnel sans perturber le fonctionnement normal en absence de fuites. Pour le deuxième type d'erreur, il est aussi possible de les traiter comme des erreurs d'effacement après une injection efficace et rapide des atomes fraîchement préparés. Il paraît donc nécessaire de démontrer l'ensemble des capacités ci-dessus avec ces modifications avant de pouvoir réaliser une suppression exponentielle³¹ des erreurs avec les codes correcteurs d'erreurs.

31 Le gain obtenu avec la correction d'erreurs est dit exponentiel lorsque l'on réduit exponentiellement le taux d'erreur des qubits logiques tandis que le nombre de qubits physiques augmente de manière non exponentielle (par exemple de manière polynomiale seulement)

2.6. LES DÉFIS À VENIR

Comme on le voit, le domaine de la correction d'erreur quantique et de la tolérance aux fautes est en pleine effervescence. Les premières expériences démontrant que ces méthodes fonctionnent sont réalisées en ce moment même dans plusieurs laboratoires, et de nombreuses pistes théoriques d'amélioration sont étudiées par la communauté.

Si les bases théoriques du domaine sont bien comprises, les expériences à venir vont être déterminantes, car elles permettront d'explorer des régimes complètement nouveaux, correspondant à des probabilités d'erreur logique inférieures à 10^{-5} ou 10^{-6} à court terme. Ces expériences seront cruciales pour comprendre si les modèles d'erreurs étudiés aujourd'hui restent bien pertinents, ou si de nouvelles erreurs, par exemple corrélées, entrent en jeu à ces régimes. On sait déjà que des particules à haute énergie peuvent créer des erreurs problématiques pour des circuits supraconducteurs. Sans doute découvrirons-nous d'autres phénomènes similaires. Ces erreurs corrélées sont éminemment problématiques pour les codes quantiques que l'on considère aujourd'hui, mais sont très probablement corrigibles une fois identifiées et comprises. Il suffira de mettre au point de nouveaux codes correcteurs avec les propriétés requises.

D'une manière générale, on est encore au début de la recherche sur les codes correcteurs quantiques et la tolérance aux fautes. Les deux dernières décennies ont été consacrées en grande partie au code de surface, mais il est clair aujourd'hui que de nombreuses alternatives existent et que de nombreuses voies restent à explorer.

Une difficulté est la petite taille de la communauté de recherche, probablement quelques dizaines de chercheurs en France, moins d'un millier dans le monde, face à une tâche assez colossale. Un enjeu des années à venir sera de former davantage d'étudiants sur ces sujets, et peut-être également permettre la réorientation d'une partie de la communauté qui travaillait sur le NISQ vers les questions de correction d'erreur.

Métriques pour juger le succès des expériences

Afin d'évaluer le succès des diverses expériences, les acteurs du domaine utilisent des métriques différentes, liées aux limitations de chaque plateforme. L'assurance de la viabilité d'une approche vers un processeur tolérant aux fautes passe par la démonstration de la suppression exponentielle des erreurs en augmentant la distance du code. Il est donc nécessaire de répéter plusieurs cycles de correction d'erreurs avec des codes de distances différentes et réaliser cette suppression exponentielle en dessous du seuil de la tolérance aux fautes. Il s'agit des expériences menées par exemple par l'équipe de Google avec le code de surface de distances 3, 5 et 7. L'expérience récente de Quantinuum/Microsoft sur une plateforme constituée de 32 qubits encodés dans les états des ions piégés montre aussi ces cycles de correction d'erreurs répétés sur un code $[[12,2,4]]$ appelé « Carbon code ». Ici, la distance étant fixée à 4, les auteurs démontrent une amélioration du taux d'erreur logique en dessous de l'erreur physique (nous parlons alors de *break-even*). Cette métrique justifie le succès de la correction dans l'élimination des erreurs, mais ne permet pas de voir si avec une mise à l'échelle de la distance, nous pouvons atteindre des taux d'erreurs logiques très bas du type 10^{-10} . Chaque code bénéficiant d'une capacité de détection d'erreur plus élevée que de la correction d'erreur, les expériences utilisent souvent une post-sélection des événements sans erreurs qui permet des erreurs logiques de taux bien plus bas. Aussi les plateformes qui souffrent des limitations en ce qui concerne la lecture mi-circuit des qubits, ou des erreurs non Pauli (fuite ou perte d'atomes), bénéficient de ces expériences de post-sélection pour anticiper les performances de leur plateforme, une fois ces limitations levées. Même si cette post-sélection peut être utilisée pour atténuer les erreurs dans des calculs de taille moyenne, c'est la suppression exponentielle du taux d'erreur logique dans une expérience de correction d'erreur qui assure la viabilité vers un processeur tolérant aux fautes capable de traiter des problèmes de taille arbitraire.

Chapitre 3

LES TECHNOLOGIES DE QUBITS : DÉFIS ET FEUILLES DE ROUTE

Dans cette partie du rapport, nous examinons l'état de l'art, les défis et les feuilles de route qui visent à créer des ordinateurs quantiques à tolérance aux fautes. Nous nous focalisons sur cinq principales catégories de qubits : les supraconducteurs, les atomes neutres, les ions piégés, les spins en boîte quantiques et les photons. Ce sont les catégories présentant le niveau de maturité technologique le plus élevé du marché³².

On peut identifier en tout neuf grandes catégories de types de qubits, elles-mêmes habituellement regroupées de manière simplifiée en trois groupes : les qubits utilisant des atomes isolés, ceux qui s'appuient sur des électrons et leur spin dans des structures variables (atomes artificiels supraconducteurs, électrons piégés dans des puits de potentiel, électrons dans des lacunes de structures cristallines, qubits topologiques, etc.), et enfin, les qubits volants qui sont généralement des photons, mais pourraient être aussi potentiellement des électrons.

32 D'autres types de qubits comme les qubits topologiques de Microsoft ou les cavités dans les diamants ont des niveaux de maturité plus bas à ce stade.

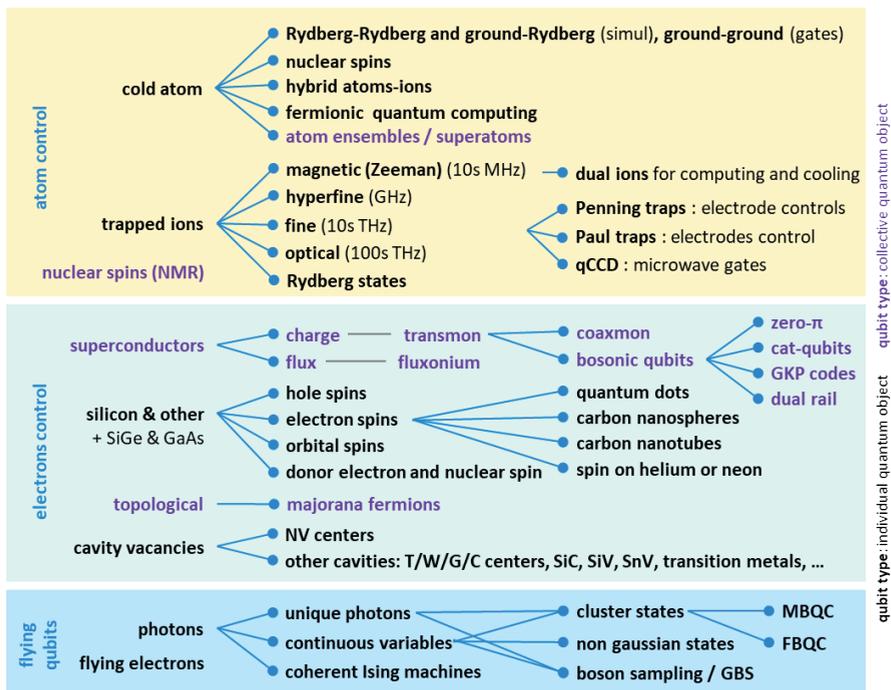


Figure 4: une cartographie et généalogie des principaux types de qubits connus. Les qubits en violets ont un support physique reposant sur plusieurs objets quantiques. (cc) Olivier Ezratty, 2021-2024.

La grande majorité des types de qubits inventoriés (figure 4) sont supportés par des acteurs industriels, témoignant de la grande diversité des paris technologiques faits par les chercheurs, les industriels, les investisseurs privés qui les supportent et les gouvernements qui les financent directement ou indirectement.

Début 2025, un peu plus de 90 acteurs industriels étaient identifiés (figure 5). Le niveau de maturité technologique des offres est très variable. Certains n'ont même pas encore démontré le fonctionnement d'un qubit ou même d'une porte quantique à deux qubits. D'autres ont dépassé la centaine de qubits fonctionnels, notamment dans les qubits supraconducteurs et les atomes neutres. Les ions piégés se distinguent avec de très bonnes fidélités des portes quantiques, mais avec une plus grande difficulté à monter en nombre.

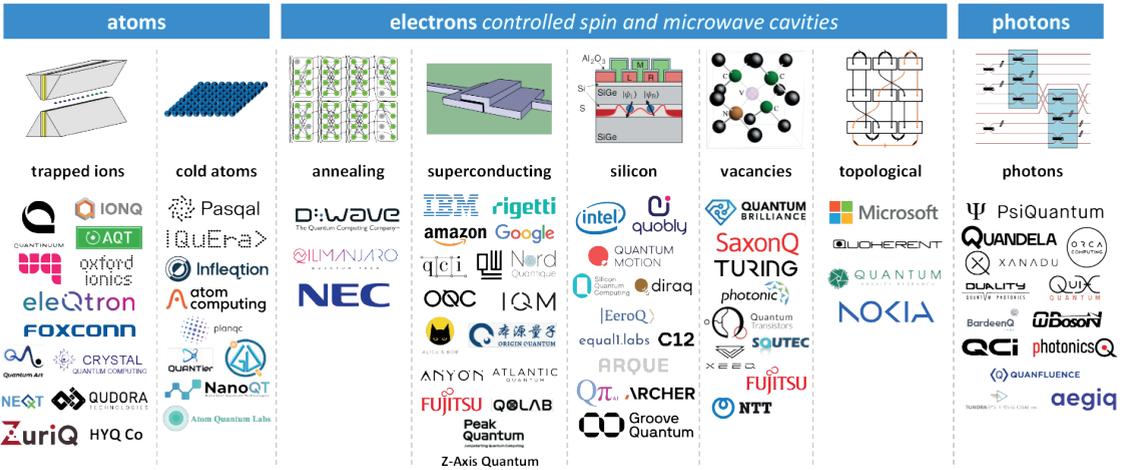


Figure 5: Panorama des acteurs industriels du marché (cc), Olivier Ezratty, mars 2025.

| | atoms | atoms | electrons superconducting & spins | electrons superconducting & spins | photons | photons |
|----------------------------------|---|---|-----------------------------------|-----------------------------------|---------------------------|---|
| | cold atoms | trapped ions | superconducting | silicon | NV centers | photons |
| qubit size | about 1 μm space between atoms | about 1 μm space between atoms | (100 μm) ² | (100nm) ² | <(100nm) ² | nanophotonics waveguides lengths, MZI, PBS, etc |
| best two qubits gates fidelities | 99.5% (QuEra) | 99.84% (56 q, Quantinuum) | 99.68% (IBM Heron r2) | >99% (SiGe) | 99.2% | 99% (but probabilistic) |
| best readout fidelity | 97% | 99.99% | 99.4% | 99% (SiGe) | 98% | 89% (efficiency) |
| best gate time | ≈ 1 ns | 0.1 to 4 μs | 20 ns to 300 ns | ≈ 5 μs | 10-700 ns | <1 ns |
| best T ₁ | > 1 s | 0,2s-10mn | 100-400 μs | 20-120 μs | 2.4 ms | ∞ & time of flight |
| qubits temperature | < 1mK 4K for vacuum pump | <1mK 4K cryostat | 15mK dilution cryostat | 100mK-1K dilution cryostat | 4K to RT | 1.8K-4K for photons gen. & det. |
| operational qubits | 1,600 (Inflexion) | 56 (Quantinuum) | 156 (IBM) 72 (China) | 12 (Intel) in SiGe | 5 (Quantum Brilliance)-10 | 216 modes GBS (Xanadu) |
| scalability | up to 10,000s per QPU | 1000s, with multiple traps | <1,000 per chip | potentially millions | unknown | 100s-1M in multiple circuits |

Figure 6: Figures de mérite des principaux types de qubits. Les durées de portes intègrent le contrôle électronique, mais pas la partie classique du traitement. Les T₁ sont les meilleurs temps de relaxation des qubits. La fidélité des portes à deux qubits évalue en pourcentages la probabilité que l'opération génère le résultat attendu. Ce sont les meilleures figures de mérite prises isolément. Cela ne signifie pas qu'un ordinateur quantique rassemble toutes les figures de mérite d'une seule colonne !

Quelques sources de données : [Neutral Atom Quantum Computing Hardware: Performance and End-User Perspective](#) by Karen Wintersperger *et al.*, April-May 2023 (27 pages), trapped ions ([Trapped Ion Quantum Computing: Progress and Challenges](#), 2019, [Materials Challenges for Trapped Ion Quantum Computers](#), 2020, [Infineon](#), IonQ and Quantinuum, [High-Fidelity Bell-State Preparation with 40Ca+ Optical Qubits](#) by Craig R. Clark *et al.*, PRL, September 2021 (7 pages)), silicon ([Roadmap on quantum nanotechnologies](#), 2020), superconducting (many IBM papers), NV centers ([Quantum computer based on color centers in diamond](#), 2021). I list only the most demanding two qubit gates and readouts fidelities. Cold atoms systems are usually simulators, but data pertains to gate-based implementations. Olivier Ezratty, 2020-2024.

Comparer la maturité technologique de ces approches est très délicat, en particulier dans la perspective de la création d'ordinateurs quantiques à tolérance de pannes (figure 6). Par analogie, on est plus situé dans le domaine de la climatologie que dans les prévisions météorologiques, au sens où l'on peut certainement comparer les figures de mérite d'aujourd'hui (météo), mais leur évolution dans le temps dépend d'un très grand nombre de paramètres, d'interdépendances et d'incertitudes (climat).

Voici une autre synthèse présentant les fidélités des portes à deux qubits qui correspondent à l'indicateur le plus pertinent pour comparer les plateformes, a minima, dans un régime NISQ (figure 7). Elle illustre le défi de la capacité à monter à la fois en puissance du côté de la fidélité de ces portes et de l'autre, de le faire avec un grand nombre de qubits. Idéalement, en régime NISQ, il faudrait disposer de fidélités supérieures à 99,9%, celle-ci croissant avec le nombre de qubits employés. Cela correspond aussi au seuil qu'il faudrait atteindre pour que la correction d'erreur soit viable et à grande échelle.

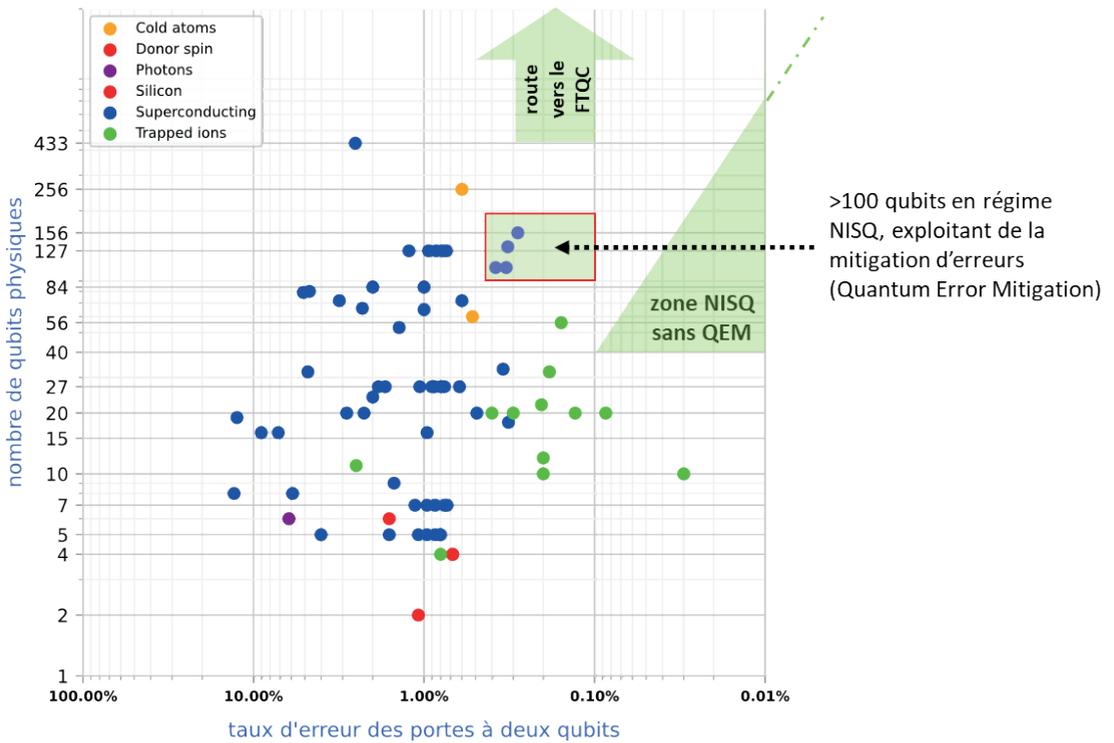


Figure 7 : Comparaison des taux d'erreur des portes à deux qubits par types de qubits (en X) en regard du nombre de qubits physiques (en Y).

Chaque point correspond à un ordinateur quantique d'un acteur industriel.

Source : compilation Olivier Ezratty, janvier 2025.

La figure 8 présente un résumé des défis qui se présentent pour chaque type de qubits. Pour chacun de ces défis, de nombreux groupes académiques et industriels envisagent des solutions très variées qui restent difficiles à évaluer.

| | superconducting | neutral atoms | trapped ions | silicon spins | photons |
|-------------------|---|--|--|--|--|
| challenges | <ul style="list-style-type: none"> • noise and crosstalk \propto with # of qubits. • electronics energetic cost. • scaling cabling, circulators. • scaling cryostats. | <ul style="list-style-type: none"> • atom controls beyond 1,000 qubits. • harder to implement gate-based QC and QND. | <ul style="list-style-type: none"> • slow gate speed. • scaling >50 qubits. • ion heating. • control signals variability. | <ul style="list-style-type: none"> • controlled electrostatic potential. • error correction. • qubits entanglement. • fab cycle time. | <ul style="list-style-type: none"> • creating entangled photons cluster states. • photon losses in circuits. • photon detectors efficiency. |
| solutions | <ul style="list-style-type: none"> • materials improvement. • 3D chipset stacking. • cryo-CMOS or SFQ. • microwave signals multiplexing. • more powerful cryostats, JJ circulators. • scale-out with photons. | <ul style="list-style-type: none"> • movable atoms for 2-qubit gates and readout. • multiple elements. • more powerful lasers. • atoms/photon conversion for interconnect. | <ul style="list-style-type: none"> • QCCD and microwave qubit drive. • ions shuttling. • multiple elements. • Rydberg states ions. • QPU photonic interconnect. | <ul style="list-style-type: none"> • material and interfaces improvement. • integrated cryoelectronics. • more powerful cryostats. • more efficient fabs (GF). | <ul style="list-style-type: none"> • bright & deterministic photon sources. • deterministic sources of cluster states. • MBQC / FBQC models. • hybrid integrated nanophotonics. • photon routing. |
| caveats | <ul style="list-style-type: none"> • photonic interconnect overhead and statistics. • energetic cost of microwave multiplexing and control drive. • SFQ backaction on qubits. | <ul style="list-style-type: none"> • gate control precision. • losing the atom while computing. • potential applicability limited to mid-scale simulations. | <ul style="list-style-type: none"> • photonic interconnect viability. • photonic interconnect statistics and impact on speedups. | <ul style="list-style-type: none"> • understanding noise sources. • scalability potential is capital intensive. • 2-qubit gates fidelities improving slowly. | <ul style="list-style-type: none"> • photon statistics. • small cluster states. • nanophotonic circuit losses. • probabilities everywhere. |

Figure 7 bis: Défis technologiques par types de qubits pour la montée en échelle des ordinateurs quantiques. Source : Olivier Ezratty, 2022-2024.

Voici de plus une compilation des feuilles de route publiques d'une bonne partie des industriels du secteur, qui sont décrites dans les cinq parties suivantes sur chaque type de qubit. Ces feuilles de route sont généralement documentées avec un à trois indicateurs comprenant : le nombre de qubits logiques, le nombre de portes quantiques exécutables (qui conditionnent la fidélité de ces qubits logiques) et parfois également le nombre de qubits physiques associés. La médiane de l'obtention prévue d'une centaine de qubits logiques est située aux alentours de 2029 tandis que certains acteurs tels qu'IBM prévoient d'atteindre le millier de qubits logiques vers 2033.

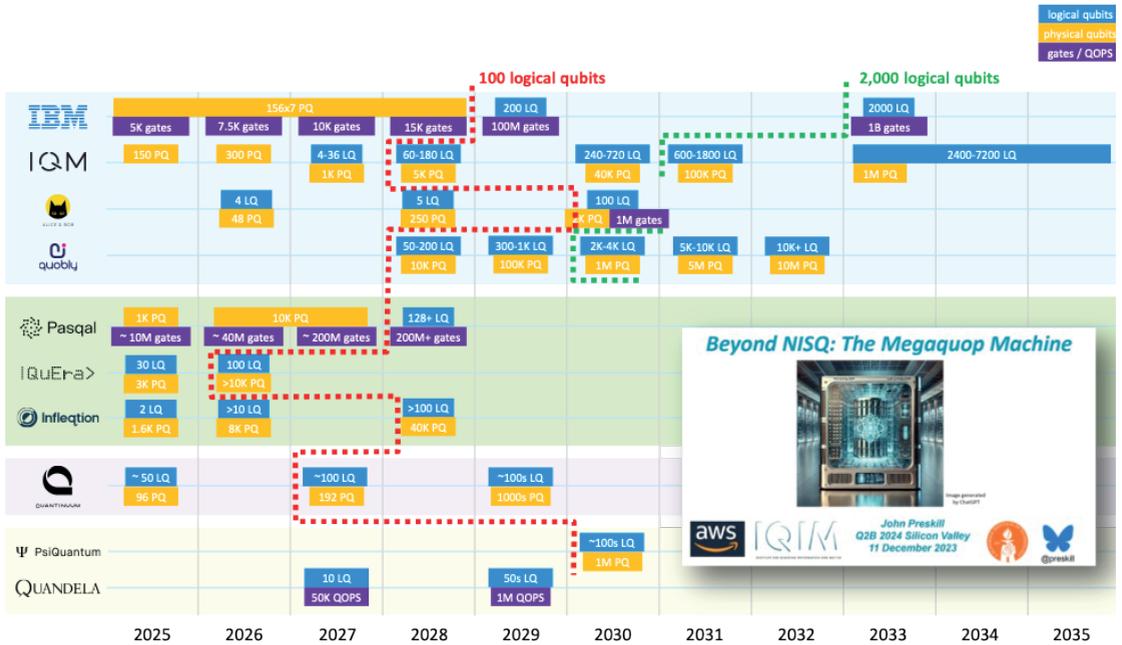


Figure 8 : Compilation des feuilles de route des principaux industriels du calcul quantique. Le megaquop présenté par John Preskill dans son intervention à la conférence Q2B de Santa Clara de décembre 2024 correspond à une centaine de qubits logiques. (cc) Olivier Ezratty, mars 2025.

Au bout du compte, la grande question qui subsiste est : jusqu'où pourrions-nous aller dans le contrôle d'objets quantiques intriqués avec de bonnes fidélités ?

Du côté de la consommation d'énergie, les chercheurs se demandent actuellement si les ordinateurs quantiques pourraient consommer moins d'énergie qu'un ordinateur classique lorsqu'ils effectuent des tâches de calcul utiles. Il s'agit d'une question importante qui pourrait ouvrir la voie à de nombreuses applications de l'informatique quantique dans un monde en quête d'économies d'énergie.

Cependant, la question reste entièrement ouverte, car la communauté des chercheurs commence à peine à développer des moyens d'évaluer et d'optimiser la consommation d'énergie des petits ordinateurs quantiques bruyants (souvent appelés ordinateurs NISQ), et le problème est encore plus difficile pour les futurs ordinateurs quantiques tolérants aux fautes.

Le coût énergétique des ordinateurs quantiques dépend du type de qubit, de leur qualité, et du coût de la correction d'erreurs. Il est généralement réparti entre électroniques de contrôle des qubits (générateurs de micro-ondes, lasers, câbles, amplificateurs...), cryogénie et calcul classique pour le pilotage de l'ensemble, aussi bien au niveau du contrôle de l'ordinateur quantique avec notamment la partie classique de la correction d'erreurs, mais aussi avec la partie classique des algorithmes quantiques qui peut être particulièrement coûteuse. Ces coûts augmentent significativement lorsque l'on utilise des qubits logiques qui sont des assemblages d'un nombre pouvant être très grand de qubits physiques.

Deux scénarios peuvent être envisagés :

- celui d'ordinateurs quantiques qui réalisent des traitements que l'on peut aussi réaliser avec des ordinateurs classiques ;
- celui d'ordinateurs quantiques à tolérance de fautes qui réaliseront des traitements inaccessibles aux ordinateurs classiques. Il faudra alors qu'ils aient une empreinte énergétique raisonnable, si possible, ne dépassant pas celles des plus puissants des supercalculateurs actuels (de 20 à 40 MW en puissance). Les premières estimations de ce côté-là sont très variables. 100 qubits logiques chez PsiQuantum (à base de photons) pourraient demander une puissance de l'ordre de 10 à 20 MW. Or il faudrait 4000 qubits logiques pour faire des calculs utiles, par exemple en simulation chimique. À plusieurs centaines de MW, la puissance demandée deviendrait énorme et difficile à accepter, ce d'autant plus que les calculs correspondants pourraient durer plusieurs mois. À titre de comparaison, le CERN consomme une puissance de pointe de 200 MW, mais seulement une faible partie du temps de fonctionnement. D'autres technologies pourraient significativement faire baisser cette addition par exemple avec les qubits de chat d'Alice&Bob qui pourraient demander beaucoup moins de ressource pour résister aux erreurs., Quandela grâce à des sources de photons intriqués plus efficaces ou encore les qubits de spin de Quobly et enfin certains types d'ions piégés. Certains envisagent de supporter des milliers de qubits logiques avec moins de 1 MW. Mais toutes les hypothèses évoquées dans ce paragraphe restent à valider.

Ce travail d'estimation et d'optimisation de ressources, ainsi que de standardisation et de *benchmarking*, est fédéré par la Quantum Energy Initiative³³, une communauté internationale de chercheurs académiques et des industriels du secteur qui planche sur la question et a été lancée à l'initiative de la France en 2022.

3.1. ATOMES NEUTRES

Les qubits à base d'atomes neutres étaient jusqu'à il y a peu réservés au champ spécifique des simulations quantiques. Depuis 2023, de nombreuses avancées scientifiques et technologiques les ont vus prendre le devant de la scène pour le calcul quantique à porte, ouvrant le champ du possible vers la tolérance aux fautes.

Les atomes neutres sont habituellement piégés sous vide par des lasers appliquant l'effet Doppler et l'effet Sisyphé³⁴, ce dernier ayant été découvert par Claude Cohen-Tannoudji et Jean Dalibard au LKB de l'ENS en 1987. La préparation des atomes se fait en plusieurs étapes. Un nuage d'atomes est d'abord piégé et refroidi dans un piège magnéto-optique exploitant des bobines créant un champ magnétique et six lasers dans trois directions. D'autres lasers sont alors combinés avec des outils de façonnage de la lumière (SLMs, des modulateurs spatiaux de lumière qui contrôlent la phase des photons issus des lasers, et AODs, des défecteurs acousto-optiques de lumière qui modifient l'orientation des faisceaux de lumière) pour créer des pinces optiques servant à déplacer et piéger à volonté les atomes dans le vide, et en général dans des structures géométriques à deux dimensions.

Les deux états quantiques des atomes utilisés pour créer des qubits correspondent à des niveaux d'énergie atomique différents, où les transitions sont contrôlées par un mélange variable de faisceaux laser et de micro-ondes, notamment des états dits de Rydberg à haute énergie. Ces états peuvent être utilisés comme état de qubit et/ou pour coupler des qubits entre eux avec

33 Quantum Energy Initiative – Creating an interdisciplinary research line for quantum technologies energetics (quantum-energy-initiative.org)

34 https://www.college-de-france.fr/sites/default/files/documents/serge-haroche/UPL313866821288387325_Aperc_u_de_Cours2015.II.B.20_03.pdf

des portes à deux qubits ou pour configurer un hamiltonien pour réaliser des simulations quantiques.

Les qubits d'atomes neutres peuvent en effet être utilisés de deux manières : avec le calcul basé sur des portes quantiques à un et deux qubits et pour les simulations quantiques, en utilisant un état préparé de qubits interconnectés qui convergent vers un niveau d'énergie minimum, aidant à trouver une solution à la physique à N corps et à divers problèmes d'optimisation. Les simulations quantiques peuvent, par exemple, simuler des modèles Fermi-Hubbard qui modélisent des matériaux électroniques fortement corrélés comme la matière condensée et les matériaux supraconducteurs à haute température. On peut aussi les utiliser pour résoudre des problèmes de combinatoire via la formalisation de problème de type QUBO (*Quadratic Unconstrained Binary Optimization*).

neutral atoms qubits key takeaways

| highlights | challenges |
|---|---|
| <ul style="list-style-type: none"> operational systems with 100-300 atoms in simulation mode and not far from a provable quantum advantage. long qubit coherence time and fast gates. identical atoms, that are controlled with the same laser and micro-wave frequencies. first logical qubits thanks to movable atoms. works in both simulation and gate-based paradigms. no need for specific integrated circuits. uses standard apparatus: lasers, optics, controls, cryogenics. low energy consumption. | <ul style="list-style-type: none"> crosstalk between qubits: can be mitigated with two-elements atom architectures. slow operations: 1 Hz simulation cycle. harder to implement with gate-based model: need a stable universal gate set with support for error correction. need to move atoms around: to enable many-to-many two-qubit gates and reducing QEC overhead, enabling qLDPCC, but with risk of losing the atoms on the way. implement full QND measurement: needed for error correction. losing atoms during computing while disconnecting the tweezers. |
| variations | path to scalability |
| <ul style="list-style-type: none"> dual species qubits: to improve QND measurement. nucleus spin qubits: with longer coherence times, in seconds. circular Rydberg atoms: more stable. fermionic computing: better for chemical simulations. bosonic codes (cat-codes, GKP) with atom qubits: better QEC. hybrid gate-based and analog: for specific case studies. atoms trapped on nanophotonic circuits: enabling interactions. hybrid neutral atoms and ions: getting the best of both worlds. atom ensembles: studied particularly in China. | <ul style="list-style-type: none"> powerful lasers: needed to control >300 atoms, with stabilized power, fiber lasers. atoms positioning: large scale SLM+AOD to trap up to 10K atoms. QND measurement: using dual species and/or atoms shuttling. faster operations and duty cycle: better and more powerful lasers, fast classical controls (FPGA, ASIC). implement full universal gate set: T gate & magic state distillation. QPU interconnect: photon based, including for memories, can also use nanophotonic circuit traps. |

Figure 9: points forts, défis, variétés et options d'évolutivité des qubits à base d'atomes froids.

3.1.1. AVANCÉES

En 2017, Mikhaïl Lukin de Harvard et une équipe du MIT contrôlaient 51 atomes de rubidium³⁵. Ce record est passé à 256 atomes en juillet 2021³⁶. En 2023, la même équipe opérait des portes quantiques à deux qubits (CZ) avec 60 atomes avec une fidélité de 99,5%. En France, l'équipe d'Antoine Browaeys de l'Institut d'Optique et Pasqal atteignait 72 atomes froids dans une structure 3D en 2018, 196 en 2020³⁷, 500 en 2021 et 828 en 2024³⁸.

L'évolutivité peut être améliorée principalement en augmentant la durée de vie des interactions atomiques. Cela nécessite également l'amélioration continue de la fidélité des portes à un ou deux qubits, un objectif étant d'atteindre 99,9% de fidélité pour les portes à deux qubits. Un record a été atteint en 2022 par l'Université de Calgary avec des fidélités de 99,85% pour des portes CZ et des atomes de césium³⁹.

Une approche, également testée avec des ions piégés, consiste à mélanger deux espèces d'atomes neutres. Elle est évaluée par l'Université de Chicago, avec 512 atomes dans un réseau utilisant une proportion équivalente d'atomes de césium et de rubidium. Ces espèces d'atomes ont une longueur d'onde laser différente pour l'entraînement de porte, ce qui réduit^{40,41}.

35 [Probing many-body dynamics on a 51-atom quantum simulator](#) by Hannes Bernien, Mikhail Lukin *et al.*, 2017 (24 pages).

36 [Quantum phases of matter on a 256-atom programmable quantum simulator](#) by Sepehr Ebadi, Dolev Bluvstein, Vladan Vuletić, Mikhail D. Lukin *et al.*, *Nature*, July 2021 (20 pages).

37 [Synthetic three-dimensional atomic structures assembled atom by atom](#) by Daniel Barredo, Antoine Browaeys *et al.*, 2018 (4 pages).

38 [Rearrangement of single atoms in a 2000-site optical tweezers array at cryogenic temperatures](#) by Grégoire Pichard, Adrien Signoles, Antoine Browaeys, Thierry Lahaye, Davide Dreon *et al.*, *arXiv*, May 2024 (6 pages).

39 [Two-qubit gate in neutral atoms using transitionless quantum driving](#) by Archismita Dalal and Barry C. Sanders, University of Calgary, June 2022 (22 pages).

40 [Dual-Element, Two-Dimensional Atom Array with Continuous-Mode Operation](#) by Kevin Singh *et al.*, University of Chicago, February 2022 (11 pages).

41 [A dual-species Rydberg array](#) by Shraddha Anand, Conor E. Bradley, Ryan White, Vikram Ramesh, Kevin Singh, and Hannes Bernien, University of Chicago, *arXiv*, January 2024 (24 pages).

De nombreux travaux de recherche sont en cours pour améliorer les capacités et la mise à l'échelle des simulations quantiques, en estimant la fidélité des simulateurs quantiques à base d'atomes neutres⁴², en mesurant l'intrication de grande dimension⁴³, en comprenant l'effet du bruit et en renforçant la résilience aux erreurs^{44, 45}. D'autres travaux étudient la capacité d'organiser les atomes en 3D⁴⁶, avec jusqu'à 30 000 atomes⁴⁷.

D'autres avancées concernent l'utilisation d'atomes de Rydberg à orbites circulaires (CRA)^{48, 49}. Les atomes de Rydberg à faible moment angulaire ont de grandes orbitales elliptiques, créant un dipôle. Leur durée de vie est limitée à quelques millisecondes et un atome sur 100 est perdu dans ce laps de temps⁵⁰.

D'autres chercheurs utilisent, au lieu du rubidium, de l'ytterbium qui est plus stable et le strontium est également considéré en raison de ses temps de stabilité plus longs⁵¹.

-
- 42 [Preparing random states and benchmarking with many-body quantum chaos](#) by Joonhee Choi and Manuel Endres, Caltech, MIT, Harvard, Berkeley, University of Illinois at Urbana-Champaign, University of Innsbruck, *Nature*, January 2023 (25 pages).
 - 43 [Detecting high-dimensional entanglement in cold-atom quantum simulators](#) by Niklas Euler and Martin Gärtner, Universität Heidelberg, May 2023 (26 pages).
 - 44 [Quantum advantage and stability to errors in analogue quantum simulators](#) by Rahul Trivedi, Adrian Franco Rubio and J. Ignacio Cirac, December 2022 (23 pages).
 - 45 [Optimization of Algorithmic Errors in Analog Quantum Simulations](#) by Nikita A. Zemlevskiy *et al.*, August 2023 (18 pages).
 - 46 [Scalable multilayer architecture of assembled single-atom qubit arrays in a three-dimensional Talbot tweezer lattice](#) by Malte Schlosser, February 2019-March 2023 (13 pages).
 - 47 [Picosecond-Scale Ultrafast Many-Body Dynamics in an Ultracold Rydberg-Excited Atomic Mott Insulator](#) by V. Bharti *et al.*, *PRL*, September 2023 (7 pages).
 - 48 [Array of Individual Circular Rydberg Atoms Trapped in Optical Tweezers](#) by Brice Ravon, Jean-Michel Raimond, Michel Brune, Clément Sayrin *et al.*, April 2023 (9 pages).
 - 49 [Quantum Computing with Circular Rydberg Atoms](#) by Sam R. Cohen and Jeff D. Thompson, Princeton, *PRX Quantum*, March-August 2021 (26 pages).
 - 50 [Long-Lived Circular Rydberg Qubits of Alkaline-Earth Atoms in Optical Tweezers](#) by C. Hölzl, A. Götzelmann, E. Pultinevicius, M. Wirth, and F. Meinert, Universität Stuttgart, *PRX*, May 2024 (11 pages).
 - 51 [Cavity-enhanced optical lattices for scaling neutral atom quantum technologies to higher qubit numbers](#) by A. J. Park *et al.*, November 2022 (18 pages).

En décembre 2023, QuEra, Harvard et le MIT annonçaient avoir créé 48 qubits logiques avec 280 atomes. Dans leur dispositif, les atomes sont déplacés pour permettre la mise en œuvre de portes à deux qubits entre n'importe quelle paire de qubits avec des interactions de Rydberg et des mesures à mi-circuit dans des cavités⁵². Leur porte logique à deux qubits a une erreur de 7%, alors que les portes physiques sont fidèles à 99,5%. La bonne fidélité d'état intriqué GHZ à 4 qubits est obtenue grâce à de la post-sélection, ce qui est une astuce inapplicable en pratique pour du calcul quantique. Il s'agit plus de détection d'erreurs que de véritable correction d'erreurs. De plus, ils n'avaient pas encore mis en place un ensemble complet de portes universelles. Dans le même article de *Nature*, les chercheurs expérimentaient leur propre « avantage quantique » en utilisant un algorithme IQP (*Instantaneous Quantum Polynomial-Time*) utilisant leurs qubits logiques de 48 qubits. Comme si l'histoire se répétait, il a été démontré par des chercheurs d'IBM que cela pouvait être facilement simulé de manière classique, jusqu'à 96 qubits logiques et même 192 qubits logiques en utilisant des processeurs spécialisés de type TPU de Google⁵³.

52 [Logical quantum processor based on reconfigurable atom arrays](#) by Dolev Bluvstein, Mikhail D. Lukin *et al.*, *Nature*, December 2023 (42 pages).

53 [Fast classical simulation of Harvard/QuEra IQP circuits](#) by Dmitri Maslov, Sergey Bravyi, Felix Tripier, Andrii Maksymov, and Joe Latone, IBM and IonQ, *arXiv*, January 2024 (9 pages).

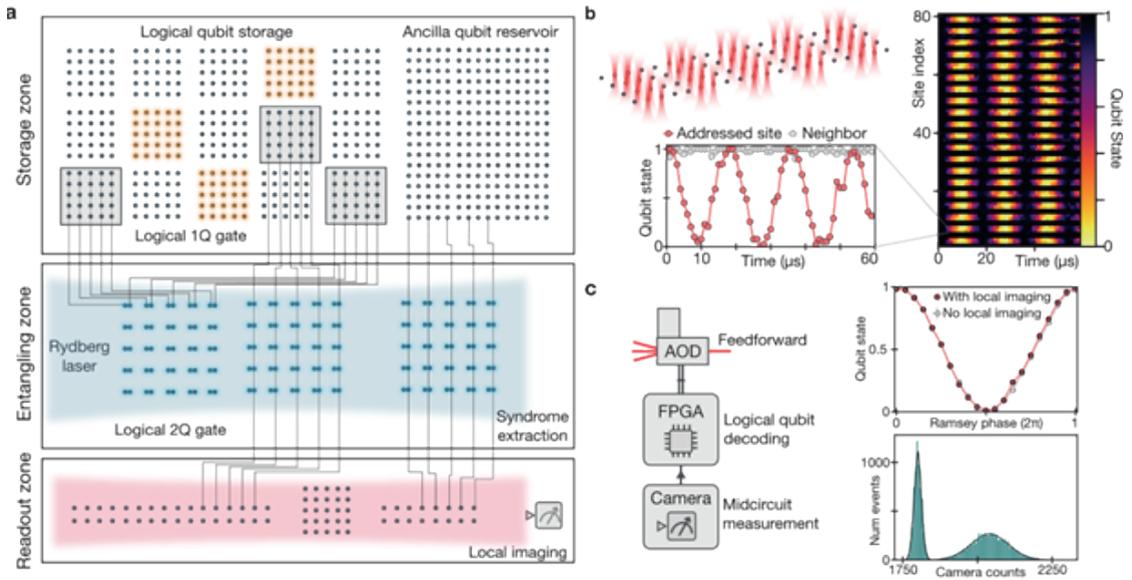


Figure 10 : l'architecture de déplacement des atomes présentée par QuEra/Harvard/MIT en décembre 2023. Une zone sert à l'exécution de portes quantiques à deux qubits, permettant de créer des portes entre n'importe quelle paire de qubits, et une autre sert aux mesures non destructives.

Les atomes neutres présentent divers avantages qui méritent d'être mentionnés. Ils ne nécessitent pas de circuits semi-conducteurs spécifiques et coûteux, contrairement à toutes les autres modalités de qubits. Ils utilisent des technologies habilitantes relativement standards: des lasers, des dispositifs optiques discrets, et même la cryogénie. Les derniers systèmes nécessitent une cryogénie à base d'hélium -4 à 4K pour refroidir à la fois la pompe ionique à ultraviolette et la chambre contenant les atomes dans le piège magnéto-optique (MOT). Enfin, ces systèmes semblent *a priori* être peu gourmands en énergie. Plusieurs milliers d'atomes peuvent *a priori* être contrôlés pour un budget de puissance inférieur à 20 kW.

3.1.2. DÉFIS

Voici les défis subsistant pour continuer à faire progresser ces qubits et leur permettre d'être mis en œuvre dans des architectures à tolérance de pannes.

Lenteur des opérations : chaque déplacement des atomes pour la réalisation de portes à deux qubits dure 10 microsecondes. Les portes quantiques à deux qubits sont donc très lentes, même si cette lenteur est compensée par la capacité à relier ainsi tous les qubits du système sans passer par de coûteuses portes SWAP. En mode analogique, un cycle de simulation dure actuellement environ une seconde. Il existe des perspectives technologiques pour gagner un à deux ordres de grandeur dans cette durée de cycle.

Diaphonie entre les qubits : elle peut être atténuée avec des architectures atomiques à deux éléments.

Complexité du modèle à portes : il est plus difficile à mettre en œuvre que les simulations quantiques analogiques. Il faut disposer d'un ensemble de portes universelles stables avec prise en charge de la correction d'erreurs, notamment des portes-T et de la distillation d'états magiques.

Déplacer les atomes : c'est la technique actuellement retenue pour la mise en œuvre de portes à deux qubits avec une connectivité maximale, pour réduire la surcharge de la correction d'erreur et permettre l'emploi de codes de correction qLDPC, mais avec le risque de perdre les atomes en cours de route.

Perte des atomes : pendant le calcul en déconnectant les pinces optiques au moment de l'exécution de portes quantiques.

3.1.3. VARIATIONS

Comme pour toutes les modalités de qubits, il existe de nombreuses variantes d'ordinateurs quantiques à base d'atomes neutres.

Qubits d'espèces duales: qui associent deux éléments, dont les transitions énergétiques sont différentes comme l'association du césium avec le rubidium. Cela permet, par exemple, de mettre en œuvre une mesure non destructive de l'état des atomes, indispensable pour la correction d'erreurs⁵⁴.

Qubits de spin de noyau: avec des temps de cohérence plus longs, en secondes. C'est le choix technologique de la startup nord-américaine Atom Computing qui a dépassé le contrôle d'un millier de qubits en 2023⁵⁵.

Atomes de Rydberg circulaires: qui ont de bonnes stabilités de l'ordre de 30 ms, meilleures que celle des atomes à orbites elliptiques^{56,57}. La technologie est notamment étudiée au Collège de France et au LKB, mais semble plus adaptée aux simulations quantiques qu'au calcul à base de portes quantiques.

Calcul fermionique: il est notamment adapté aux simulations chimiques et à la résolution de problèmes de structures électroniques de molécules. Une proposition du MIT associe des paires d'atomes froids dans des réseaux optiques 2D dans lesquels l'information quantique est codée dans l'état vibratoire des paires d'atomes⁵⁸. À noter également les travaux internationaux qui associent le LPMMC à Grenoble avec Anna Minguzzi et

54 [Dual-Element, Two-Dimensional Atom Array with Continuous-Mode Operation](#) by Kevin Singh *et al.*, University of Chicago, February 2022 (11 pages).

55 [Assembly and coherent control of a register of nuclear spin qubits](#) by Katrina Barnes, Michael Yarwood *et al.*, *Atom Computing*, August 2021 (11 pages).

56 [High-fidelity gates with mid-circuit erasure conversion in a metastable neutral atom qubit](#) by Shuo Ma, Guido Pupillo, Shruti Puri, Jeff D. Thompson *et al.*, *Nature*, May-October 2023 (17 pages).

57 [Long-Lived Circular Rydberg Qubits of Alkaline-Earth Atoms in Optical Tweezers](#) by C. Hölzl, A. Götzelmann, E. Pultinevicius, M. Wirth, and F. Meinert, Universität Stuttgart, *PRX*, May 2024 (11 pages).

58 [Quantum register of fermion pairs](#) by Thomas Hartke, Botond Oreg, Ningyuan Jia and Martin Zwierlein, MIT, 2021 (10 pages).

Benoit Vermersch⁵⁹. Là encore, on est plutôt dans le régime de la simulation quantique et pas du FTQC.

Cat-codes: il existe un moyen de mettre en œuvre des *cat-codes* avec des atomes de Rydberg, la variété *cat-manifold* exploitant le spin du noyau des atomes⁶⁰.

Calcul hybride basé sur des portes et de l'analogique: un mélange de circuits analogiques et basés sur des portes⁶¹.

Ensembles d'atomes: ils sont notamment étudiés en Chine. Il s'agit d'ensembles d'atomes ou de « super-atomes », à la fois pour le calcul à portes et pour des simulations quantiques⁶².

Hybridation atomes et ions: dans des architectures combinant des atomes froids et des ions piégés⁶³.

3.1.4. CHEMINS VERS L'ÉVOLUTIVITÉ

La mise en œuvre de calcul à tolérance de pannes avec des atomes neutres comprend de nombreux défis scientifiques et technologiques que voici :

59 [Fermionic quantum processing with programmable neutral atom arrays](#) by Daniel González-Cuadra, Dolev Bluvstein, Marcin Kalinowski, Raphael Kaubruegger, Nishad Maskara, Piero Naldesi, Torsten V. Zache, Adam M. Kaufman, Mikhail D. Lukin, Hannes Pichler, Benoît Vermersch, Jun Ye, and Peter Zoller, *arXiv*, March 2023 (13 pages).

60 [Fault-tolerant quantum computation using large spin cat-codes](#) by Sivaprasad Omanakuttan, Vikas Buchemmavari, Jonathan A. Gross, Ivan H Deutsch, and Milad Marvian, University of New Mexico, Google AI, *arXiv*, January 2024 (22 pages).

61 [Quantum simulation of fermionic systems using hybrid digital-analog quantum computing approach](#) by Nikita Guseynov and Walter Pogosov, December 2021-May 2022 (20 pages).

62 [Rydberg superatoms: An artificial quantum system for quantum information processing and quantum optics](#) by Xiao-Qiang Shao, Shi-Lei Su, Lin Li, Rejish Nath, Jin-Hui Wu, and Weibin Li, *arXiv*, April 2024 (32 pages).

63 [Performing Non-Local Phase Estimation with a Rydberg-Superconducting Qubit Hybrid](#) by Juan Carlos Boschero, TU Eindhoven, *arXiv*, February 2024 (98 pages).

Fidélité des portes : il faudra pouvoir préserver une bonne qualité de portes quantiques à deux qubits, en s'approchant de 99,9% et à grande échelle. Le tout sans perdre les atomes au moment de leur déplacement dans les zones dédiées à la mise en œuvre de ces portes quantiques.

Positionnement des atomes : l'enjeu est de pouvoir contrôler et déplacer dans l'espace un grand nombre d'atomes neutres avec des pinces optiques. La technique préférée est celle qui exploite des pinces optiques à base de SLM et d'AOD à grande échelle pour piéger jusqu'à plusieurs milliers d'atomes. On peut noter le record de Caltech annoncé en mars 2024, avec le contrôle de l'emplacement de 6100 atomes avec des pinces optiques⁶⁴.

Puissance des lasers : au gré de l'augmentation du nombre d'atomes contrôlé au-delà de quelques centaines, les lasers positionnant et contrôlant les atomes doivent être plus puissants et stabilisés. La technologie envisagée est celle des lasers fibrés. L'offre commerciale n'est pas encore très abondante.

Mesure non destructive : celle-ci est nécessaire pour la mise en œuvre de la correction d'erreurs. Les solutions envisagées relèvent de l'usage de deux espèces d'atomes ou du déplacement des atomes dans des zones de mesure dédiées dans des cavités.

Opérations et cycle de service plus rapides : les portes quantiques actuelles, notamment à deux qubits, sont trop lentes, de l'ordre de la milliseconde. Il en va de même de la durée d'un cycle complet de simulation quantique qui dure environ une seconde. Il faudra pouvoir raccourcir ces temps. Cela passe par l'usage de lasers plus puissants et fibrés et par une optimisation de l'électronique de commande classique.

Positionnement des atomes en les ionisant au préalable et à l'aide d'électrodes : c'est une technique envisagée par l'équipe de la startup slovène Atom Quantum Lab.

64 [A tweezer array with 6100 highly coherent atomic qubits](#) by Hannah J. Manetsch, Gyohei Nomura, Elie Bataille, Kon H. Leung, Xudong Lv, and Manuel Endres, Caltech, *arXiv*, March 2024 (21 pages).

Interconnexion entre processeurs : même si l'on pourra contrôler plusieurs milliers d'atomes dans un seul processeur pour créer quelques dizaines de qubits logiques, il faudra les interconnecter entre eux de manière quantique pour pouvoir monter en échelle. La connexion envisagée passe par des photons optiques et des mémoires quantiques comme celles de Weling. L'avantage de ce type de liaison est que l'on interagit aussi sur des atomes avec des photons optiques. Reste à faire en sorte que les longueurs d'onde soient compatibles entre ces différents systèmes et à s'assurer que les portes quantiques distantes soient de bonne qualité.

3.1.5. FEUILLES DE ROUTE

Plusieurs startups se positionnent sur le marché du calcul quantique à base d'atomes froids, notamment Infleqtion (anciennement ColdQuanta, 2007, États-Unis, travaillant initialement sur les capteurs quantiques), Pasqal (2019, France), QuEra (2020, États-Unis, lié à Mikhael Lukin et Harvard) et PlanQC (2022, Allemagne).

En janvier 2024, QuEra a annoncé sa feuille de route FTQC, prévoyant d'obtenir 100 qubits logiques d'ici 2027 en utilisant plus de 10 000 qubits physiques, et avec un taux d'erreur logique de 10^{-6} à 10^{-8} . Le support de portes quantiques non Clifford (T) arriverait en 2025.

En février 2024, Infleqtion annonçait sa feuille de route à 5 ans. Elle présentait son QPU Sqorpius contrôlant 1600 atomes de césium neutres disposés en réseau 40×40 , sans indication de fidélités de portes. Elle prévoit de supporter 100 qubits logiques avec 40 000 atomes avec des fidélités physiques de portes à deux qubits de 99,95% d'ici 2028. Elle le fera en utilisant deux éléments, le rubidium et le césium⁶⁵.et envisage d'utiliser des codes de correction d'erreur de type qLDPC⁶⁶.

65 [Infleqtion Unveils 5-Year Quantum Computing Roadmap, Advancing Plans To Commercialize Quantum At Scale by Infleqtion](#), February 2024.

66 [Architecture for fast implementation of qLDPC codes with optimized Rydberg gates](#) by C. Poole, T. M. Graham, M. A. Perlin, M. Otten, and M. Saffman, Infleqtion and University of Wisconsin-Madison, *arXiv*, April 2024 (12 pages).

En mars 2024, Pasqal a annoncé sa nouvelle feuille de route, ouvrant la voie au calcul à portes quantiques en régime FTQC d'ici 2028^{67,68}. Elle prévoit de proposer une approche hybride analogique/numérique⁶⁹. Elle positionne ses simulateurs analogiques en utilisant un équivalent en nombre de portes quantiques.

Les grands jalons scientifiques récents de Pasqal et de l'équipe de recherche de l'IOGS comprennent le contrôle 2D de 196 qubits⁷⁰, l'exécution de portes parallèles⁷¹ et le contrôle de 324 atomes froids dans un réseau 2D, avec l'utilisation d'un cryostat 4K refroidissant la pompe à ultraviolette, ce qui permet de créer un meilleur vide et de prolonger la durée de vie des qubits atomiques, ainsi que la chambre à vide, pour éviter l'effet des rayonnements électromagnétiques^{72,73}. En mai 2024, Pasqal et l'IOGS ont battu un record en manipulant 828 atomes dans 2000 sites dans leur QPU Humber à l'aide de pinces optiques et de deux lasers utilisant des longueurs d'onde légèrement différentes⁷⁴.

-
- 67 [PASQAL Announces New Roadmap Focused on Business Utility and Scaling Beyond 1,000 Qubits Towards Fault Tolerance Era](#), Pasqal, March 2024.
 - 68 [Roadmap to Quantum Readiness with a Full Stack Approach & Transformative Use Cases](#) by Pasqal, April 2024.
 - 69 [Microwave Engineering of Programmable XXZ Hamiltonians in Arrays of Rydberg Atoms](#) by P. Scholl, Loic Henriet, Thierry Lahaye, Antoine Browaeys *et al.*, *PRX*, April 2022 (10 pages).
 - 70 [Enhanced atom-by-atom assembly of arbitrary tweezers arrays](#) by Kai-Niklas Schymik, Antoine Browaeys, Thierry Lahaye *et al.*, November 2020 (10 pages).
 - 71 [Pulse-level Scheduling of Quantum Circuits for Neutral-Atom Devices](#) by Richard Bing-Shiun Tsai, Loic Henriet *et al.*, Pasqal, June 2022 (8 pages).
 - 72 [Single Atoms with 6000-Second Trapping Lifetimes in Optical-Tweezer Arrays at Cryogenic Temperatures](#) by Kai-Niklas Schymik, Sara Pancaldi, Florence Nogrette, Daniel Barredo, Julien Paris, Antoine Browaeys, and Thierry Lahaye, *IOGS, PRA*, September 2021 (8 pages).
 - 73 [In situ equalization of single-atom loading in large-scale optical tweezer arrays](#) by Kai-Niklas Schymik, Adrien Signoles, Florence Nogrette, Daniel Barredo, Antoine Browaeys, and Thierry Lahaye, *PRA*, August 2022 (6 pages).
 - 74 [Rearrangement of single atoms in a 2000-site optical tweezers array at cryogenic temperatures](#) by Grégoire Pichard, Adrien Signoles, Antoine Browaeys, Thierry Lahaye, Davide Dreoni *et al.*, *arXiv*, May 2024 (6 pages).

3.1.6. CONCLUSION

Les ordinateurs à tolérance de panne à base d'atomes froids sont prometteurs avec la capacité potentielle de délivrer une centaine de qubits logiques d'ici la fin de la décennie, ouvrant la voie à un avantage quantique possible. Comme toutes les modalités de qubits, la question est de savoir jusqu'où il sera possible d'aller au sein d'un seul processeur en termes de contrôle fiable d'atomes. Au-delà, une interconnexion photonique sera indispensable. Elle reste difficile à mettre au point, en particulier à grande échelle, et notamment en termes de capacité à permettre l'exécution de portes quantiques à deux qubits fiables entre deux processeurs ainsi connectés. C'est indispensable pour pouvoir envisager de créer des ordinateurs à tolérance de panne distribués avec des qubits logiques résidant sur plusieurs processeurs pouvant dialoguer entre eux.

3.2. QUBITS SUPRACONDUCTEURS

Les qubits supraconducteurs sont actuellement la modalité la plus étudiée dans le monde académique et avec la communauté de fournisseurs commerciaux la plus importante et la mieux financée, comprenant de grands acteurs comme IBM, Google, IQM et Rigetti. Par abus de langage, cette catégorie comprend aussi les qubits bosoniques à base de photons micro-ondes intriqués piégés dans des cavités, avec des acteurs tels qu'Alice&Bob (*cat-qubits*) et Nord Quantique (GKP).

Les qubits supraconducteurs les plus courants s'appuient sur l'usage d'oscillateurs anharmoniques de courants supraconducteurs traversant une ou plusieurs jonctions Josephson. Les deux niveaux d'énergie les plus bas de ces oscillateurs encodent les états $|0\rangle$ et $|1\rangle$ de chaque qubit. Ces oscillateurs opèrent à une fréquence d'environ 10 MHz et sont contrôlés par des pulsations micro-ondes d'environ 5 GHz qui génèrent des portes à un qubit. Les portes à deux qubits sont habituellement créées par le contrôle de coupleurs accordables reliant des qubits adjacents dans les circuits. La lecture de l'état des qubits passe par l'usage d'un résonateur situé à proximité du qubit. Celui-ci est excité par une pulsation micro-onde qui est réfléchiée, amplifiée et analysée. La combinaison de sa phase et de son amplitude permet de déterminer l'état du qubit. Cette mesure est dite non destructive, car le qubit reste opérationnel après sa mesure, dans l'état généré qui est $|0\rangle$ ou $|1\rangle$.

superconducting qubits key takeaways

| highlights | challenges |
|---|--|
| <ul style="list-style-type: none"> • key technology in the academic world and with the largest and well funded commercial vendors community including large players like IBM, Google, IQM and Rigetti. • record of 156 programmable qubits with 99.7% two qubit gates fidelities (IBM Heron r2, 2024). • noise reduction constant progress in regular transmons with tunable couplers and with bosonic qubits which could enable a record low ratio of physical/logical qubits. • first break-even logical qubits: Google in August 2023. • enabling technologies are abundant with cryostats, cabling, analog electronics, amplifiers, and sensors. • quantum error mitigation and quantum error correction known techniques to enable NISQ applications and future FTQC designs. | <ul style="list-style-type: none"> • qubits variability: requires calibration and complex micro-wave frequency maps and need to contain crosstalk. • qubit connectivity: limited to neighbor qubits in 2D structures. • qubit coherence time: usually < 300 μs with some lab records >1ms. • cryogeny: constrained technology at <15 mK, but not a scientific obstacle per se, more an engineering one. Yield can be improved. • logical qubits: are not yet under break even. They are currently worse than physical qubits in most experiments. • cabling clutter: complexity and many passive and active electronic components to control qubits with micro-waves and other signals. • qubits size: uneasy miniaturization limits qubit # per chips and requires QPU interconnect solutions. • qubit fidelities: have a hard time reaching 99.9%, needed for QEC. |
| variations | path to scalability |
| <ul style="list-style-type: none"> • bosonic qubits: cat-qubits, GKP, dual rail with self-correction and lower QEC overhead. They are less mature but promising. • fluxonium qubits: with better fidelities but a more complicated designs and few involved vendors. • qutrits: with larger Hilbert space, which are exotic in the commercial world. • Andreev spin qubits: localized excitation of the BCS condensate that natively has only two levels, using a nanowire. • hybrid quantum analog-digital architectures: to solve specific problems, not generic. | <ul style="list-style-type: none"> • materials: improve elements purity, identify other promising ones. • EDA: full stack electronic design automation tools. • manufacturing: industrialization, 300 mm wafers epitaxial deposition. • qubit mid-range coupling: to enable lower overhead qLDPC QEC. • interconnect: using transduction and photonic gate teleportation. • signals multiplexing or SFQ control electronics: to reduce cabling overhead and cryogenic requirements. • QEC syndrome detection speed improvements using ASICs. • cryostats: larger and more efficient. |

Figure 11: Points forts, défis, variétés et options d'évolutivité des qubits supraconducteurs.

3.2.1. AVANCÉES

Les premiers qubits supraconducteurs sont apparus en laboratoire en 1999 au Japon⁷⁵ puis en France et aux USA au début des années 2000, avec en particulier la création de l'électrodynamique en circuit à l'Université de Yale en 2004 qui a mené au développement des qubits transmon⁷⁶. Le premier

75 [Coherent control of macroscopic quantum states in a single-Cooper-pair box](#) by Yasunobu Nakamura, Yuri Pashkin and Jaw-Shen Tsai, *Nature*, 1999 (4 pages).

76 [Cavity quantum electrodynamics for superconducting electrical circuits: An architecture for quantum computation](#) by Alexandre Blais, Ren-Shou Huang, Andreas Wallraff, Steve Girvin and Rob. Schoelkopf, *PRA*, 2004 (14 pages) and [Strong coupling of a single photon to a superconducting qubit using circuit quantum electrodynamics](#) by Andreas Wallraff, David Schuster, Alexandre Blais, Steve Girvin, Rob Schoelkopf *et al.*, *Nature*, 2004 (7 pages).

processeur commercial de ce type a été mis en ligne par IBM en 2016, avec 5 qubits.

En 2019, Google a défrayé la chronique avec son processeur Sycamore de 53 qubits qui avait atteint un régime de suprématie quantique correspondant à la difficulté à réaliser le calcul du circuit sur un supercalculateur classique avec des temps de calcul estimés à 10 000 ans puis 2 jours et demi⁷⁷. Il s'est avéré que ce calcul n'en était pas un, car il n'exploitait aucune donnée en entrée et qu'il ne générait un résultat correct que dans 0,14% des cas. Quatre ans plus tard, ce processus physique était simulé numériquement en 6 secondes sur le supercalculateur Frontier du Département de l'énergie américain grâce à l'emploi de réseaux de tenseurs. Néanmoins, l'expérience de Google, renouvelée depuis avec 72 qubits de qualité légèrement améliorée, était tout de même une prouesse technologique. Sa simulation demanderait 46 jours avec des réseaux de tenseurs sur le supercalculateur Frontier et n'a pas encore été réalisée classiquement⁷⁸.

En août 2024, Google réalisait ses premiers qubits logiques ayant des fidélités supérieures à celle de ses qubits physiques et sur deux processeurs, l'un de 72 qubits et l'autre de 105 qubits, dénommé Willow en décembre 2024. Google réalisait la correction d'erreur d'un qubit logique en *surface code* de distance 5 sur le premier en temps réel et sur le second, avec un code de distance 7 et 101 qubits, un record pour des qubits supraconducteurs. Ils ne corrigeaient cependant pas encore de portes logiques quantiques sur ces processeurs.

Depuis 2019, les évolutions sur ce type de qubit se sont poursuivies. Le nombre de qubits opérationnels a augmenté raisonnablement, mais pas de manière exponentielle. Leur qualité a progressé, même si de manière moins spectaculaire que celle des ions piégés. Les qubits de type transmon exploitant des coupleurs accordables ont atteint une fidélité record de 99,7%

77 [Quantum supremacy using a programmable superconducting processor](#) by Frank Arute, John Martinis *et al.*, October 2019 (12 pages) and [Supplementary information for "Quantum supremacy using a programmable superconducting processor"](#) by Frank Arute, John Martinis *et al.*, October 2019 (58 pages)

78 [Phase transition in Random Circuit Sampling](#) by A. Morvan *et al.*, Google AI, April-December 2023 (45 pages).

pour les portes à deux qubits (CZ) sur les 133 qubits du processeur Heron Torino d'IBM en décembre 2023⁷⁹.

IBM et ses partenaires ont alors publié un grand nombre de travaux scientifiques relevant de «l'utilité quantique» avec une capacité à réaliser des calculs qui ne seraient pas accessibles à des calculateurs classiques, même en exploitant des réseaux de tenseurs⁸⁰. De nombreux chercheurs ont cependant réussi à reproduire l'expérience d'IBM de juin 2023 avec ces réseaux de tenseurs^{81, 82, 83}. Ces cas d'usage ne correspondent cependant pas encore à des besoins d'entreprises, mais à des simulations physiques relevant de la recherche fondamentale^{84, 85}. De son côté, la startup finlandaise IQM a obtenu des fidélités de portes à deux qubits de 99,5% en 2024 sur 20 qubits. En Chine, Origin Quantum est plus en retrait avec des fidélités de 97% de portes à deux qubits (CZ) obtenues sur 6 qubits sélectionnés dans un processeur de 72 qubits⁸⁶. Les autres acteurs de ce marché tels qu'OQC, Rigetti et Anyon Systems obtiennent des résultats encore moins bons.

79 La fidélité des qubits se mesure habituellement à plusieurs endroits: l'initialisation des qubits, les portes à un qubit, les portes à deux qubits, puis la lecture des qubits. En pratique, on se concentre sur la fidélité des portes à deux qubits qui sont les plus difficiles à obtenir et qui conditionnent la qualité de l'intrication entre qubits et, de ce fait, l'efficacité des algorithmes quantiques. D'autres figures de mérite importantes sont la durée de ces opérations. Les portes à deux qubits et la lecture sont les opérations généralement les plus lentes et diverses techniques sont proposées pour en réduire la durée.

80 [Evidence for the utility of quantum computing before fault tolerance](#) by Youngseok Kim, Kristan Temme, Abhinav Kandala *et al.*, IBM Research, RIKEN iTHEMS, University of Berkeley and the Lawrence Berkeley National Laboratory, *Nature*, June 2023 (8 pages).

81 [Efficient tensor network simulation of IBM's Eagle kicked Ising experiment](#) by Joseph Tindall, Matt Fishman, Miles Stoudenmire and Dries Sels, *PRX Quantum*, June 2023-January 2024 (16 pages).

82 [Fast and converged classical simulations of evidence for the utility of quantum computing before fault tolerance](#) by Tomislav Begušić *et al.*, Caltech, August 2023 (17 pages).

83 [Effective quantum volume, fidelity and computational cost of noisy quantum processing experiments](#) by K. Kechedzhi *et al.*, Google AI, NASA, June 2023 (15 pages).

84 [Realizing the Nishimori transition across the error threshold for constant-depth quantum circuits](#) by Edward H. Chen, Sarah Sheldon, Simon Trebst, Abhinav Kandala *et al.*, September 2023 (16 pages).

85 [Uncovering Local Integrability in Quantum Many-Body Dynamics](#) by Oles Shtanko, Derek S. Wang, Haimeng Zhang, Nikhil Harle, Alireza Seif, Ramis Movassagh, and Zlatko Mineev, July 2023 (8 pages) on spin lattices simulation with 124 qubits.

86 [Demonstrating a universal logical gate set on a superconducting quantum processor](#) by Jiaxuan Zhang, Guo-Ping Guo *et al.*, Origin Quantum, CAS *et al.*, *arXiv*, May 2024 (15 pages).

On range habituellement les qubits bosoniques dans les qubits supraconducteurs. Ils en partagent certaines des caractéristiques, même si, en pratique, le qubit exploite des photons micro-ondes piégés dans des cavités et dans des états superposés les protégeant contre certains types d'erreur. Ce sont des qubits à erreurs dites biaisées. Dans ce domaine, les qubits de chat réduisent un type d'erreur (*flip*) aux dépens de l'augmentation d'un autre type d'erreur (*phase*). Ils atteignent des temps de stabilité de plusieurs secondes et une capacité à corriger de manière autonome les erreurs de flip, aux prix d'une faible augmentation du bruit de phase⁸⁷. Ces qubits permettent d'envisager la création de qubits logiques avec un plus faible ratio de qubits physiques par qubit logique, de l'ordre de 15 pour obtenir 100 qubits logiques et un taux d'erreur logique de l'ordre de 10^{-8} à 10^{-6} , selon Alice&Bob⁸⁸. En septembre 2024, Nord Quantique publiait de premiers résultats sur ses qubits bosoniques GKP avec une proposition d'architecture pour monter en échelle⁸⁹. Amazon faisait de même avec une démonstration d'une puce de 5 qubits de chats associés à quatre qubits auxiliaires transmon mettant en œuvre une correction d'erreur pour créer des portes logiques à un et deux qubits. Les fidélités obtenues n'étaient cependant pas meilleures que celles des meilleurs qubits physiques transmon⁹⁰.

Les technologies habilitantes couvrant les besoins des qubits supraconducteurs sont abondantes avec les cryostats et leur système à dilution, les câbles supraconducteurs ou en nappes flexibles, l'électronique analogique et hybride digitale-analogique, les amplificateurs basse température et les capteurs. Chacune de ces technologies a progressé en cinq ans. La cryogénie est de plus en plus puissante et efficace. L'électronique de contrôle est plus dense, à commencer par celle qui fonctionne à température ambiante. Ainsi,

87 [Quantum control of a cat-qubit with bit-flip times exceeding ten seconds](#) by Ulysse Réglade, Pierre Rouchon, Alain Sarlette, Mazyar Mirrahimi, Philippe Campagne-Ibarcq, Raphaël Lescanne, Zaki Leghtas *et al.*, July 2023 (17 pages).

88 [LDPC-cat codes for low-overhead quantum computing in 2D](#) by Diego Ruiz, Jérémie Guillaud, Anthony Leverrier, Mazyar Mirrahimi, and Christophe Vuillot, *arXiv*, January 2024 (23 pages).

89 [Hardware-Efficient Fault Tolerant Quantum Computing with Bosonic Grid States in Superconducting Circuits](#) by Marc-Antoine Lemonde, Philippe St-Jean *et al.*, *Nord Quantique*, *arXiv*, September 2024 (17 pages).

90 [Hardware-efficient quantum error correction using concatenated bosonic qubits](#) by Harald Putterman, Fernando G. S. L. Brandão, Oskar Painter *et al.*, AWS, *arXiv*, September 2024 (60 pages).

IBM a réussi à intégrer en 2022 dans un seul rack l'électronique de contrôle de 433 qubits. Ce record était étendu à 1121 qubits avec le processeur Condor en décembre 2023. Le système a été ensuite démantelé, car les puces associées étaient insatisfaisantes du point de vue de la fidélité avec des portes à deux qubits ayant des erreurs excédant les 2%. Les amplificateurs qui opèrent à la limite quantique (TWPA) ont aussi progressé en rendement et en bande passante tout comme l'intégration du câblage, notamment avec des câbles flexibles, notamment, chez Delft Circuits, aux Pays-Bas.

Enfin, dans le régime NISQ, des techniques de mitigation d'erreurs sont apparues pour permettre d'atteindre une utilité quantique, qui reste limitée à quelques cas d'usage spécialisés. Elles sont pertinentes lorsqu'elles sont mises en œuvre avec au moins une cinquantaine de qubits physiques. En deçà, les algorithmes quantiques peuvent généralement être émulés classiquement plus efficacement en temps comme en énergie.

3.2.2. DÉFIS

De nombreux défis subsistent pour continuer à faire progresser ces qubits et notamment, leur permettre d'être mis en œuvre dans des architectures à tolérance de panne.

Les **fidélités des qubits** pour les portes à deux qubits n'arrivent pas encore à atteindre 99,9%. Ce niveau de fidélité est jugé nécessaire pour la correction d'erreurs, qu'elle repose sur des codes de surface, leurs dérivés ou même sur des codes qLDPC inspirés des codes classiques à détection de parité de type LDPC. Les chercheurs doivent lutter contre de très nombreuses sources de bruit et de décohérence des qubits avec, notamment, l'influence des circuits externes connectés au qubit (résonateurs, filtres...), le bruit de charge provenant du mouvement des charges dans les diélectriques et les oxydes, le bruit de courant critique provenant du mouvement des charges dans la jonction Josephson, les fluctuations de spins paramagnétiques dans l'interface de l'isolant de boucle supraconductrice, l'empoisonnement par effet tunnel de quasi-particules uniques à l'intérieur et à l'extérieur de l'îlot supraconducteur, les pertes diélectriques des substrats dues à l'effet tunnel, divers autres effets tunnel dans les matériaux amorphes, la diaphonie (crosstalk) entre les qubits générée par leurs signaux de commande et leur

routage, les effets des rayons cosmiques générant des erreurs corrélées et enfin, des perturbations provenant des basses fréquences générées par les compresseurs et les tubes à impulsions qui refroidissent le cryostat en 4 K.

Les **temps de cohérence** des qubits sont généralement assez courts, de l'ordre de 100 à 300 μs avec certains records en laboratoire dépassant la milliseconde, mais en général pour la variante fluxonium de ces qubits⁹¹. À l'envers, Origin Quantum (Chine) a un T_2 (stabilité en phase) d'à peine 2 μs ⁹².

Les **erreurs de fuite** (*leakage*) et les **erreurs corrélées** issues des rayons cosmiques et de la radioactivité ambiante ne sont pas traitées par les codes de correction d'erreur envisagés pour la tolérance de panne et nécessitent un traitement particulier. Ces erreurs sont difficiles à éviter et à corriger, mais des solutions sont proposées, notamment par Google et Michel Devoret, à base de modifications de la géométrie des jonctions Josephson dans les qubits^{93,94}.

Les premières **expériences de qubits logiques** ont été réalisées, notamment par ETH Zurich⁹⁵, Google⁹⁶, IBM⁹⁷ et Origin Quantum. Elles n'ont pas encore permis d'atteindre l'équilibre, le « *break even* ». Ces qubits logiques sont actuellement moins performants que les qubits physiques. Les taux d'erreur des portes logiques à deux qubits sont supérieurs à celui des portes physiques.

91 [Millisecond coherence in a superconducting qubit](#) by Aaron Somoroff, Vladimir Manucharyan *et al.*, University of Maryland, *PRL*, March 2021-June 2023 (14 pages).

92 [Enabling Large-Scale and High-Precision Fluid Simulations on Near-Term Quantum Computers](#) by Zhao-Yun Chen, Guo-Ping Guo *et al.*, Origin Quantum, *arXiv* June 2024 (31 pages).

93 [Direct evidence for cosmic-ray-induced correlated errors in superconducting qubit array](#) by Xue-Gang Li *et al.*, *arXiv*, February 2024 (7 pages).

94 [Resisting high-energy impact events through gap engineering in superconducting qubit arrays](#) by Matt McEwen, Michel Devoret, Alex Opremcak *et al.*, *arXiv*, February 2024 (14 pages).

95 [Realizing repeated quantum error correction in a distance-three surface code](#) by Sebastian Krinner, Alexandre Blais, Andreas Wallraff *et al.*, *Nature*, May 2022 (28 pages).

96 [Suppressing quantum errors by scaling a surface code logical qubit](#) by Rajeev Acharya *et al.*, Google AI, *Nature*, July 2022-February 2023 (44 pages).

97 [Encoding a magic state with beyond break-even fidelity](#) by Riddhi S. Gupta, Benjamin J. Brown *et al.*, IBM, *Nature*, January 2024 (24 pages).

La **variabilité des qubits** nécessite un étalonnage et des plans de fréquence complexes des micro-ondes de pilotage pour limiter les effets de la diaphonie. Cet étalonnage est fréquent et coûteux. Sa complexité peut augmenter avec le nombre de qubits utilisé.

La **connectivité des qubits** est actuellement limitée aux qubits voisins dans des structures de circuits 2D, ce qui entraîne un fort taux de redondance nécessaire pour la correction d'erreurs, le plus élevé étant celui des codes de surface avec un besoin de milliers de qubits pour créer des qubits logiques ayant la fidélité requise par les applications comme celles de la simulation chimique.

La **taille des qubits** reste grande, de l'ordre minima du mm^2 . Elle rend la miniaturisation difficile dans les circuits et limite le nombre qubits par puce, ce d'autant plus que la dominante actuelle avec les transmons consiste à les relier entre eux par des coupleurs accordables, qui prennent autant de place qu'un qubit. Cela entraîne le besoin de faire appel à des techniques d'interconnexion entre puces, certaines ayant des niveaux de faisabilité encore très incertains. IBM envisage de créer des circuits se contentant de 156 qubits physiques et de les assembler ensuite avec diverses techniques d'interconnexion.

Le **câblage de contrôle** des qubits est très encombrant, à raison de deux à cinq câbles coaxiaux par qubit physique. Cela remplit tout l'intérieur des cryostats. Il en va de même pour de nombreux composants électroniques passifs et actifs qui servent à contrôler les qubits avec des micro-ondes et lire leur état. Cela concerne notamment les amplificateurs (TWPA à 15 mK, HEMT à 4 K) et les circulateurs (à 15 mK) qui sont tous par ailleurs très encombrants, et avec une capacité limitée de multiplexage de la lecture simultanée d'une dizaine de qubits, du fait du multiplexage en fréquence utilisé et de la bande passante nécessaire par qubit qui est comprise entre 200 et 400 MHz. L'électronique de contrôle fonctionnant à température ambiante consomme beaucoup d'énergie, à raison, actuellement d'environ 100 W par qubit physique, ce qui est inacceptable à grande échelle avec des millions de qubits physiques. Les techniques couramment envisagées d'électronique basse température de type cryo-CMOS déplacent le problème dans le cryostat. Ils réduisent le câblage entrant dans le cryostat, mais, comme ces circuits chauffent, ils sont actuellement positionnés à 4 K où le budget de refroidissement est bien

plus important (1W actuellement) qu'à 15 mK (environ 20 μ W) et il faut trouver comment relier ces composants à 4 K aux puces quantiques fonctionnant à 15 mK.

La **cryogénie** est souvent mise en avant comme étant un facteur limitant. Les qubits supraconducteurs sont en effet ceux qui nécessitent une cryogénie active capable d'atteindre des températures de l'ordre du mK. Les cryostats associés utilisant des dilutions à sec ont des puissances de refroidissement limitées à quelques dizaines de μ W à 15 mK et quelques W à 4 K. Cela limite la capacité à exploiter de l'électronique basse température.

3.2.3. VARIATIONS

Comme pour chaque type de qubits, les qubits supraconducteurs sont très divers avec des propositions de conception très nombreuses qui nécessitent un travail d'analyse approfondi pour les départager.

Les **qubits fluxonium**, qui sont des variantes de qubits de flux, ont actuellement de meilleures fidélités, mais reposent sur des conceptions plus compliquées qui n'ont pas encore été éprouvées à grande échelle, et avec peu d'acteurs commerciaux dans le domaine (Atlantic Quantum). Ces qubits sont étudiés à de nombreux endroits (aux USA, au Japon, en Chine, en France au CNRS à Grenoble). Alibaba avait obtenu de très bons résultats⁹⁸, mais a abandonné en 2023 son activité dans le calcul quantique. Elle a été transférée à l'Université de Zhejiang qui poursuit les recherches dans le domaine⁹⁹.

Les **qutrits** utilisent un espace Hilbert d'encodage plus grand avec trois niveaux d'énergie pour l'oscillateur anharmonique du qubit. La technique n'est pas proposée dans l'offre commerciale¹⁰⁰. Les qutrits pourraient permettre de

98 [Native approach to controlled-Z gates in inductively coupled fluxonium qubits](#) by Xizheng Ma *et al.*, Alibaba, August 2023 (19 pages).

99 [Achieving millisecond coherence fluxonium through overlap Josephson junctions](#) by Fei Wang, Hui-Hai Zhao, Chunqing Deng *et al.*, Zhejiang University and Z-Axis Quantum, *arXiv*, May 2024 (12 pages).

100 [High-fidelity qutrit entangling gates for superconducting circuits](#) by Noah Goss, Irfan Siddiqi *et al.*, *Nature Communications*, November 2022 (6 pages).

limiter les effets du bruit en régime NISQ, mais les fondements théoriques pour les mettre en œuvre en régime FTQC avec de la correction d'erreur ne sont pas encore là.

Les **qubits de spin d'Andreev** utilisent une excitation localisée de condensat BCS qui n'a nativement que deux niveaux, à l'aide d'un nanofil¹⁰¹. C'est une technique de laboratoire non éprouvée, sans acteurs commerciaux. On est donc encore loin du FTQC.

Les **qubits bosoniques** intègrent une correction d'erreur totale ou partielle autonome au niveau physique. On en trouve de plusieurs sortes comme les qubits de chats (*cat-qubits*) et les qubits GKP (Gottesman-Kitaev-Preskill). Ces qubits nécessitent tout de même de la correction d'erreurs, mais celle-ci est plus légère à mettre en œuvre. Les premières réalisations de qubits physiques avec correction d'erreur de flip et de qubit logique ont été réalisées par Alice&Bob fin 2023 et début 2024. Nord Quantique a aussi annoncé début 2024 un qubit logique GKP, mais dont les performances ne sont pas entièrement documentées¹⁰². Amazon travaille de son côté sur plusieurs pistes en parallèle, les qubits de chat, les qubits GKP¹⁰³ et les qubits dual-rail¹⁰⁴.

Des **architectures analogiques-numériques quantiques hybrides** sont aussi proposées pour résoudre des problèmes spécifiques. Elles ne sont pas génériques et dédiées au régime NISQ. Peu d'acteurs les proposent, à l'instar de Kipu Quantum en Allemagne, qui est un acteur du logiciel quantique.

101 [Circuit-QED with phase-biased Josephson weak links](#) by C. Metzger, Christian Urbina, Hugues Pothier *et al.*, January 2021 (22 pages).

102 [Autonomous quantum error correction of Gottesman-Kitaev-Preskill states](#) by Dany Lachance-Quirion, Philippe St-Jean *et al.*, *Nord Quantique*, October 2023 (32 pages).

103 [Low overhead fault-tolerant quantum error correction with the surface-GKP code](#) by Kyungjoo Noh, Christopher Chamberland, and Fernando G. S. L. Brandão, *arXiv*, March 2021-January 2022 (41 pages).

104 [Demonstrating a Long-Coherence Dual-Rail Erasure Qubit Using Tunable Transmons](#) by H. Levine *et al.*, The Hebrew University of Jerusalem, University of Chicago, Caltech and AWS, *Physical Review X*, March 2024 (21 pages).

3.2.4. CHEMINS VERS L'ÉVOLUTIVITÉ

Voici un inventaire des techniques envisagées pour faciliter la montée en échelle de ces qubits et leur mise en œuvre avec de la tolérance de pannes.

L'amélioration de la **qualité de la fabrication des circuits** qui passe par la mise en place de lignes de fabrication de qualité préindustrielle et industrielle, l'emploi de *wafers* de 300 mm de diamètre et de techniques de déposition par épitaxie. Cela permettrait de limiter la variabilité des qubits, de limiter les défauts de déposition de matériaux et d'améliorer les rendements de fabrication. Ces techniques sont actuellement étudiées par IMEC en Belgique et prévues par IQM et Alice&Bob dans le cadre de la création d'une ligne de production semi-industrielle opérée par le CEA-Leti à Grenoble. Les premières expériences d'IMEC ne sont pas encore concluantes, mais des progrès sont possibles¹⁰⁵.

L'amélioration de la **pureté des éléments** est aussi envisageable pour éviter les défauts de structure dans les circuits. C'est un domaine d'étude d'une équipe de recherche en Slovénie qui collabore avec Google¹⁰⁶. Différents éléments alternatifs ont été étudiés pour la création des circuits, notamment au niveau des résonateurs, comme le tantale, mais au bout du compte, les résultats ne sont pas meilleurs qu'avec le niobium. Les jonctions Josephson sont toujours réalisées avec un sandwich d'aluminium entourant de l'oxyde d'aluminium.

La création d'**outils de simulation numérique** «*full-stack*» et «*multi-physique*» des qubits permettra de mieux simuler le fonctionnement des circuits et de les optimiser. Alice&Bob développe notamment une telle chaîne logicielle dans le cadre du projet i-Démo «*Usine à chats*».

105 [High-coherence superconducting qubits made using industry-standard, advanced semiconductor manufacturing](#) by Jacques Van Damme, Kristiaan De Greve *et al.*, IMEC, *arXiv*, March-April 2024 (17 pages).

106 [Slovenian physicist helps unlock quantum computer utility in breakthrough finding](#), *The Slovenia Times*, April 2024.

Le **couplage à distance moyenne** des qubits pour permettre une mise en œuvre des codes de correction d'erreur de type qLDPC. La technique est actuellement étudiée par IBM¹⁰⁷, IQM¹⁰⁸, IMEC¹⁰⁹ et le MIT. Les qubits de chats d'Alice&Bob se contentent de codes qLDPC classiques 1D pour la correction d'erreurs de phase permettant de supporter jusqu'à 100 qubits logiques¹¹⁰. Au-delà, afin de corriger l'erreur de flip résiduelle, des codes de correction d'erreur 2D seront nécessaires et entraîneront le besoin d'améliorer la connectivité entre qubits.

La **simplification de l'électronique de contrôle** à basse température est une voie étudiée dans plusieurs domaines. Le multiplexage des signaux de contrôle des qubits passant par une conversion en photons optiques est étudié par la startup Viqthor (France). L'électronique cryo-CMOS est envisagée par de nombreux acteurs, dont IQM. L'électronique de contrôle supraconductrice (SFQ, pour *single-flux quantum*) est très séduisante du fait de sa faible charge thermique. Elle est proposée par la société américaine SeeQC et étudiée dans divers laboratoires académiques en Finlande (VTT), en France (chez Pascal Febvre à Chambéry), au Japon (RIKEN). Enfin, des techniques de remplacement des circulateurs à base de ferrites par des circuits supraconducteurs sont aussi envisagées, notamment par Analog Quantum Circuits¹¹¹ (Australie) ainsi que par Google¹¹².

L'amélioration de la **vitesse de détection des syndromes d'erreurs** pour la correction d'erreurs devra faire appel à des circuits ASIC en lieu et place de FPGA. Ce remplacement sera justifié d'un point de vue économique lorsque

107 [High-threshold and low-overhead fault-tolerant quantum memory](#) by Sergey Bravyi, Andrew W. Cross, Jay M. Gambetta, Dmitri Maslov, Patrick Rall, Theodore J. Yoder, *Nature*, March 2024 (11 pages).

108 [Long-Distance Transmon Coupler with cz-Gate Fidelity above 99.8%](#) by Fabian Marxer *et al.*, *PRX Quantum*, February 2023 (23 pages).

109 [A superconducting quantum information processor with high qubit connectivity](#) by Gürkan Kartal *et al.*, *IMEC*, July 2023 (8 pages).

110 [LDPC-cat codes for low-overhead quantum computing in 2D](#) by Diego Ruiz, Jérémie Guillaud, Anthony Leverrier, Mazyar Mirrahimi, and Christophe Vuillot, *arXiv*, January 2024 (23 pages).

111 [Passive superconducting circulator on a chip](#) by Rohit Navarathna, Thomas M. Stace, Arkady Fedorov *et al.*, *PRL*, August 2022-January 2023 (11 pages).

112 [Josephson parametric circulator with same-frequency signal ports, 200 MHz bandwidth, and high dynamic range](#) by Randy Kwende *et al.*, Google AI, May 2023.

la technologie sera stabilisée et que les volumes de fabrication d'ordinateurs quantique le justifieront. Ce passage est envisagé par Riverlane (UK) qui est notamment partenaire d'Alice&Bob ainsi que d'IQM.

L'**interconnexion entre processeurs quantiques** est envisagée. Elle passera dans un premier temps par une interconnexion à courte portée par des liaisons directes de puces à puces via des connexions à base d'indium (Rigetti, IBM) puis avec des guides micro-ondes à moyenne portée (IBM). Au-delà, il est envisagé d'exploiter une transduction entre micro-ondes (5 GHz) et photons optiques (QPhox¹¹³, Pays-Bas) et l'établissement de liaisons synchronisées par des mémoires à base d'ensembles d'atomes neutres (Welinq¹¹⁴, France). Toutes ces techniques sont encore très expérimentales et pas encore éprouvées. Le lien via des photons optiques est basé sur l'établissement d'intrications à base de paires de Bell qui ne sont pas déterministes et dont l'impact sur les calculs doit être évalué. Le but ultime étant de réaliser des portes à deux qubits, par exemple de type CNOT, entre qubits situés dans deux processeurs distants. Ces portes devront avoir des fidélités autour de 99,9% pour supporter la correction d'erreurs et pouvoir être établies entre plusieurs qubits des processeurs interconnectés, afin de ne pas trop alourdir les algorithmes.

Les **cryostats** devront augmenter en puissance et en capacité à supporter un plus grand nombre de câbles. Le record commercial actuel est le Bluefors KIDE avec 9 compresseurs et 3 dilutions, supportant une très grande charge. IBM prévoit de supporter des milliers de qubits physiques avec ce type de cryostat. Air Liquide envisage de créer des systèmes de production de froid à base d'hélium liquide apportant un meilleur rendement et une plus grande puissance de refroidissement.

113 [An integrated microwave-to-optics interface for scalable quantum computing](#) by Matthew J. Weaver, Simon Gröblacher, Robert Stockill *et al.*, QphoX, *Nature Nanotechnology*, October 2022-October 2023 (14 pages).

114 [Connecting heterogeneous quantum networks by hybrid entanglement swapping](#) by Giovanni Guccione, Tom Darras *et al.*, May 2020 (7 pages).

3.2.5. FEUILLES DE ROUTE

Des feuilles de route d'acteurs commerciaux comprenant la capacité à créer des systèmes à tolérance de panne ont été annoncées par IBM, Google et Alice&Bob. Elles ne sont en général pas détaillées sur l'axe technologique du fait de changements fréquents dans les options technologiques retenues. D'autres acteurs du marché des qubits supraconducteurs tels qu'Amazon, Nord Quantique, IQM, Rigetti, OQC et Atlantic Quantum n'ont pas encore annoncé de *roadmap* publique pour la tolérance de pannes.

Les premières feuilles de route d'IBM annoncées entre 2020 et 2022 prévoyaient l'usage de codes de surface et l'obtention d'une centaine de qubits logiques avec 100 000 qubits physiques. Depuis leur annonce de l'adoption de codes qLDPC en 2023 et l'usage de ce qu'ils appellent les *gross codes*, le nombre de qubits logiques réalisable avec ce nombre de qubits physiques a augmenté. Comme de nombreux autres acteurs du marché, IBM fournit, comme indicateur de performance de ces systèmes, le nombre de portes quantiques exécutables dans un algorithme. Cet indicateur est commun entre les régimes NISQ et FTQC. IBM prévoit d'assembler des dizaines de qubits physiques avec des processeurs de taille modeste, d'environ 150 qubits, qui sont connectés entre eux avec au moins trois types de coupleurs : micro-ondes courte distance, micro-ondes moyenne distance puis liaisons photoniques optiques (infrarouge) avec de la transduction de signal.

On pourra remarquer qu'IBM a respecté sa *roadmap* depuis 2020, qui était décrite en nombre de qubits. La *roadmap* a ensuite été réajustée pour l'adoption d'une stratégie modulaire, construite à base de puces comprenant 156 qubits physiques et des coupleurs accordables pour la création de portes à deux qubits.

Chez Google, le planning n'a pas beaucoup changé depuis 2020 et consiste à assembler un million de qubits physiques d'ici le début de la décennie 2030, pour obtenir de l'ordre d'une centaine de qubits logiques. Le tout repose toujours sur l'usage de codes de surface. Mais sans plus de détails sur la mise en œuvre technologique. Cela créerait un système de taille démesurée. Google n'est pas encore en mesure d'avancer dans sa *roadmap* du fait de fidélités de qubits physiques qui n'évoluent quasiment pas depuis 2020 et

plafonnent à 99,4% pour les portes à deux qubits. En tenant compte de la création de leurs premiers qubits logiques sous le seuil du *break-even* en août 2024, à savoir des qubits logiques avec de meilleures fidélités que les qubits physiques, les projections ne changent pas trop. Il leur faudra des milliers de qubits physiques pour créer un qubit logique avec des taux d'erreurs compris entre 10^{-6} et 10^{-14} . Et ces qubits physiques ne tiendront pas sur une seule puce. Leur capacité à monter en échelle dépendra donc étroitement de la disponibilité de techniques d'interconnexions entre puces à base de guides micro-ondes et de photons optiques, via des moyens de transduction, et dont les taux d'erreur et efficacités devront être compatibles avec les exigences des codes de correction d'erreurs.

Alice&Bob prévoit de supporter une centaine de qubits logiques avec un taux d'erreurs de 10^{-6} avec une puce d'environ 2000 qubits physiques d'ici 2030, le tout avec des étapes intermédiaires. Les techniques de fabrication permettant de loger tous ces qubits physiques sur une seule puce restent à mettre en place. Le nombre de puces qui seront nécessaires pour atteindre un régime FTQC de plusieurs centaines puis de milliers de qubits logiques n'est pas encore déterminé, ni les techniques d'interconnexion envisagées entre ces puces.

3.2.6. CONCLUSION

Les défis à surmonter pour créer des architectures à tolérance de pannes sont nombreux. Comme pour tous les types de qubits, ces défis couvrent à la fois des défis scientifiques théoriques et expérimentaux ainsi que des défis de nature plus technologique et d'ingénierie. Le principal reste toutefois de créer des puces de plus d'une centaine de qubits physiques avec des fidélités de porte à deux qubits de 99,9% puis de relier entre elles ces puces avec des ressources d'intrication en préservant la qualité des opérations au même niveau.

3.3. PHOTONS

Les photons constituent une catégorie à part de qubits, celle des « qubits volants ». Ils n'ont ni masse ni charge électrique, et se déplacent dans le vide à la vitesse de la lumière. Dans tous les autres types de qubits, les photons interagissent avec des atomes, des circuits supraconducteurs ou des spins d'électron pour modifier leur état quantique ou créer de l'intrication entre ces qubits, qu'il s'agisse de photons dans le régime des micro-ondes ou dans celui de la lumière visible ou du proche infrarouge.

Les photons sont eux-mêmes porteurs d'information quantique sur une ou plusieurs de leurs propriétés : leur polarisation, leur fréquence, le moment de leur émission, leur nombre, leur chemin, tout comme leur moment angulaire orbital. Les photons sont moins sujets que les autres types de qubits au phénomène de décohérence. Ils présentent aussi l'avantage d'être utilisés pour les communications quantiques, notamment celles qui relieront à terme les ordinateurs quantiques entre eux pour augmenter leur puissance.

Cependant, il est difficile de les faire interagir entre eux du fait de pertes à plusieurs niveaux : dans leur source, dans les guides d'ondes qui les véhiculent, dans les systèmes optiques qui les transforment (déphaseurs, polariseurs, interféromètres) et enfin, dans les détecteurs. Leur comportement est éminemment probabiliste à chacun de ces niveaux.

Comme pour les autres types de qubits, les photons peuvent être exploités de nombreuses manières. La première classification à prendre en compte distingue les photons à variables discrètes ou continues^{115, 116}.

- Les qubits photons à **variables discrètes** où l'information peut être encodée sur des degrés de liberté différents (polarisation, chemin, énergie, temps,

115 [Photonic Quantum Computing](#) by Jacqueline Romero, and Gerard Milburn, University of Queensland, *arXiv*, April 2024 (26 pages).

116 [Quantum computing overview: discrete vs. continuous variable models](#) by Sophie Choe, June 2022 (12 pages)

moment angulaire orbital...) qui peuvent même être combinés^{117, 118, 119, 120}. Ils reposent sur des sources déterministes ou probabilistes de photons uniques et indiscernables. Ils s'appuient sur la dimension particulaire des photons. C'est l'approche de PsiQuantum et Quandela.

- Les qubits photons à **variables continues** encodent l'information dans les fluctuations du champ électromagnétique, en exploitant leur décomposition en quadrature. Ces qubits sont appelés qumodes chez Xanadu. Ils exploitent en priorité la nature ondulatoire des photons. Ces photons peuvent aussi être mis en œuvre avec des modèles de type qubit de chat et états GKP^{121, 122, 123}.

Le principe général des ordinateurs quantiques à base de photons repose sur les étapes suivantes, en prenant l'exemple des variables discrètes :

- la **génération de photons** qui associent des lasers et des générateurs de photons uniques et indiscernables¹²⁴. Ces photons sont produits à une fréquence donnée et peuvent ensuite être répartis sur plusieurs guides d'ondes via des lignes à retard. Les figures de mérite de ces sources sont l'indiscernabilité des photons (ils doivent tous avoir les mêmes propriétés quantiques), la luminosité de la source (combien de photons sont émis par

117 [Programmable Photonic Quantum Circuits with Ultrafast Time-bin Encoding](#) by Frédéric Bouchard, Benjamin Sussman *et al.*, University of Ottawa, *arXiv*, April 2024 (7 pages).

118 [Time-bin entanglement in the deterministic generation of linear photonic cluster states](#) by David Bauch, Nikolas Köcher, Nils Heinisch, and Stefan Schumacher, Paderborn University, *arXiv*, March 2024 (11 pages).

119 [Efficient qudit based scheme for photonic quantum computing](#) by Márton Karácsony, László Oroszlány and Zoltán Zimborás, February 2023 (19 pages).

120 [Deterministic Generation of Qudit Photonic Graph States from Quantum Emitters](#) by Zahra Raissi, Edwin Barnes, and Sophia E. Economou, *PRX Quantum*, November 2022-May 2024 (20 pages).

121 [Robust Preparation of Wigner-Negative States with Optimized SNAP-Displacement Sequences](#) by Marina Kudra, Jonas Bylander, Simone Gasparinetti *et al.*, Chalmers University, *PRX Quantum*, September 2022 (12 pages).

122 [Gottesman-Kitaev-Preskill encoding in continuous modal variables of single photons](#) by Éloi Descamps, Arne Keller, and Pérola Milman, *PRL*, October 2023-April 2024 (8 pages).

123 [Logical states for fault-tolerant quantum computation with propagating light](#) by Shunya Konno, Akira Furusawa *et al.*, *Science*, January 2024 (11 pages).

124 [Near-ideal spontaneous sources in silicon quantum photonics](#) by S. Paesani *et al.*, 2020 (6 pages).

unité de temps), l'efficacité du système (la probabilité qu'au moins un photon soit créé par impulsion), la pureté d'un seul photon (probabilité d'obtenir un maximum d'un photon par impulsion), le taux de photons (taux de génération de photons) et l'anti-corrélation entre photons, mesurée par la valeur de cohérence du second ordre $g^2(0)$ qui correspond à la probabilité d'émettre deux photons simultanément, idéalement à zéro. D'autres aspects opérationnels comprennent la stabilité et la cohérence du temps (cohérence de la source dans le temps), les propriétés spectrales, et la capacité à contrôler la longueur d'onde des photons émis et la température des opérations, généralement à 4K. La pureté et la forte probabilité d'obtenir un photon par cycle d'horloge permettent de générer des interférences et des portes quantiques à deux photons. Il existe plusieurs types de sources de photons uniques^{125, 126} : les sources à base de boîtes quantiques comme celles de Quandela et Sparrow Quantum qui ont de très bonnes figures de mérite (pureté de 99,7%, efficacité d'extraction de 65%, indistingabilité de 99%), les sources paramétriques de paires de photons qui exploitent du pompage laser dans des cavités non linéaires et peuvent être directement intégrés dans des circuits de nanophotonique, mais ont des efficacités moins bonnes. C'est le choix de PsiQuantum ;

- **les portes à un qubit sont faciles à réaliser et utilisent des dispositifs optiques simples comme des déphaseurs, des séparateurs de faisceaux, des polariseurs et des miroirs semi-réfléchissants.** Par exemple, une porte de Hadamard utilise un séparateur de faisceau, une porte X combine un séparateur et une porte Hadamard, et enfin, une porte-Z s'appuie sur un déphaseur à 180°;
- **les portes à deux qubits sont plus difficiles à réaliser parce qu'il est très difficile, mais pas impossible, de faire interagir entre eux des photons de manière déterministe.** Dans le modèle KLM¹²⁷, ces portes sont réalisées avec des séparateurs de faisceaux et assemblées en interféromètres dits de Mach-Zehnder. Elles ne sont malheureusement

125 [Integrated photonic quantum technologies](#) by Jianwei Wang *et al.*, May 2020 (16 pages).

126 [Solid-state single-photon sources: recent advances for novel quantum materials](#) by Martin Esmann *et al.*, December 2023 (35 pages).

127 [A scheme for efficient quantum computation with linear optics](#) by Emanuel Knill, Raymond Laflamme and Gerard Milburn, 2001 (7 pages).

pas déterministes et le modèle KLM repose sur un mécanisme dit de post-sélection qui fait le tri des opérations en fonction de leur succès, avec une perte en ligne évidente à chaque opération ; la **lecture des qubits** exploite des détecteurs de photons uniques ou des détecteurs de photons multiples (« *photon number resolving detectors* », PNRD). Plusieurs technologies sont disponibles: les diodes à avalanche (SPAD) qui détectent les occurrences de photons, mais pas leur nombre^{128, 129}, les « transition edge sensors » (TES) qui détectent les nombres de photons et les nanofils supraconducteurs (SNSPDs) qui savent aussi détecter les nombres de photons^{130, 131}. Ces détecteurs sont généralement refroidis entre 800 mK et 3 K^{132, 133}. Les principaux fournisseurs de détecteurs de photons uniques sont Single Quantum, Photon Spot, Quantum Opus et IDQ, utilisant principalement des SNSPDs;

- L'intégration de tout ou partie de ces éléments dans des **circuits de nanophotonique**^{134, 135}. Les opérations sur les photons sont alors contrôlées électriquement au niveau des circuits individuels comme les déphaseurs et polariseurs. Ces circuits sont gravés en technologie CMOS (silicium) et/

128 [Low-noise photon counting above 100 × 106 counts per second with a high-efficiency reach-through single-photon avalanche diode system](#) by Michael A. Wayne *et al.*, *NIST*, December 2020 (6 pages).

129 [Photon Number Resolving Detection with a Single-Photon Detector and Adaptive Storage Loop](#) by Nicholas M. Sullivan *et al.*, University of Ottawa, November 2023 (16 pages).

130 [GHz detection rates and dynamic photon-number resolution with superconducting nanowire arrays](#) by Giovanni V. Resta *et al.*, *ID Quantique*, March 2023 (26 pages).

131 [Optically-Sampled Superconducting-Nanostrip Photon-Number Resolving Detector for Non-Classical Quantum State Generation](#) by Mamoru Endo, Akira Furusawa *et al.*, *arXiv*, May 2024 (24 pages).

132 [The potential and challenges of time resolved single-photon detection based on current-carrying superconducting nanowires](#) by Hengbin Zhang *et al.*, October 2019 (19 pages) and [Superconducting nanowire single-photon detectors for quantum information](#) by Lixing You, June 2020 (20 pages). Dark counts are detected photons coming from the environment due to thermal or tunneling effects.

133 [Optimal Amplitude Multiplexing of a Series of Superconducting Nanowire Single Photon Detectors](#) by Fabio Chiarello *et al.*, March 2023 (6 pages).

134 Voir par exemple les travaux d'InPhyNi présentés [High-quality photonic entanglement based on a silicon chip](#) by Dorian Oser, Sébastien Tanzilli *et al.*, 2020 (9 pages).

135 Voir la revue [The potential and global outlook of integrated photonics for quantum technologies](#) by Emanuele Pelucchi, Dirk Englund, Jian-Wei Pan, Fabio Sciarrino, Christine Silberhorn *et al.*, *Nature Review Physics*, December 2021 (no open access).

ou III/V¹³⁶ (germanium...) ou hybrides, avec un substrat CMOS sur lequel sont collés des éléments III/V. Les techniques de fabrication impliquent des composés tels que le nitrure de silicium (SiN), le niobate de lithium (LiNbO₃)¹³⁷ et des matériaux III/V (GaAs¹³⁸, InP...) ^{139,140}. Les guides de lumière sont généralement en silicium et entourés d'oxyde de silicium, le point clé étant de minimiser les pertes de photon¹⁴¹. Un autre défi est de réduire la chaleur générée par les déphaseurs et d'optimiser leur calibrage¹⁴².

Le modèle KLM en usage aujourd'hui ne permet pas encore d'atteindre l'avantage quantique. On le considère comme faisant partie du régime NISQ, mais pas pour la raison habituelle. Ici, l'écueil est que l'efficacité du calcul diminue de manière exponentielle avec le nombre de portes à deux qubits mises en œuvre du fait de leur aspect probabiliste.

Le paradigme de calcul envisagé pour le passage à l'échelle et la tolérance aux fautes est le MBQC, ou calcul par la mesure. Il s'agit d'une approche basée sur la téléportation quantique, qui utilise des états cluster représentés par des graphes, dans lesquels les sommets correspondent aux qubits et les arêtes sont des liens d'intrication. Dans cette approche, on ne met pas en œuvre de portes à deux qubits, mais seulement des portes à un qubit et des mesures de qubits uniques, ce qui la rend particulièrement bien adaptée aux qubits photoniques. On réalise un calcul en effectuant des mesures dont les effets se propagent de proche en proche grâce aux liens d'intrication.

136 Matériaux III/V ou III-V : couples associant des éléments de la colonne III et de la colonne V de la classification.

137 [High-speed thin-film lithium niobate quantum processor driven by a solid-state quantum emitter](#) by Patrick I. Sund *et al.*, NBI, CeNTech, *Science Advances*, May 2023 (9 pages).

138 [Expanding the Quantum Photonic Toolbox in AlGaAsOI](#) by Joshua E. Castro *et al.*, May 2022 (9 pages). They implement non linear elements, edge couplers, waveguide crossings, couplers, and MZIs in Aluminum gallium arsenide-on-insulator (AlGaAsOI).

139 [Roadmap on integrated quantum photonics](#) by Galan Moody, Jacqueline Romero, Eleni Diamanti *et al.*, August 2021 (108 pages) is a good review paper on integrated nanophotonics.

140 [Advances in silicon quantum photonics](#) by Jeremy C. Adcock *et al.*, July 2022 (25 pages) décrit les défis de la nanophotonique.

141 [Mitigating photon loss in linear optical quantum circuits: classical postprocessing methods outperforming postselection](#) by James Mills, and Rawad Mezher, Quandela and University of Edinburgh, *arXiv*, May 2024 (31 pages).

142 [Global calibration of large-scale photonic integrated circuits](#) by Jin-Hao Zheng, Guang-Can Guo *et al.*, Hefei National Laboratory, CAS, *arXiv*, July 2024 (9 pages).

En outre, il s'écoule peu de temps entre la création d'un qubit physique et sa mesure. L'information quantique peut être préservée par des qubits « virtuels », c'est-à-dire qu'elle se propage de proche en proche sur les qubits physiques régulièrement mesurés. En revanche, les résultats de mesure pour un ensemble de qubits à un temps donné déterminent les bases de mesure pour les qubits ultérieurs. Cela requiert que les paramètres des composants physiques puissent être reconfigurés (« *feed-forward* ») très rapidement.

Le modèle MBQC déplace une bonne part des difficultés dans la création de ces grands états intriqués de photons¹⁴³ ainsi que dans les codes de correction d'erreur qu'il faut aussi mettre en œuvre. Ceux-ci reposent sur le processus dit de foliation, qui permet de construire des codes correcteurs sur des états clusters en trois dimensions. Cela nécessite de créer des états clusters tridimensionnels avec de nombreux qubits. Pour cela, on peut fusionner de petits états intriqués, ou utiliser des stratégies hybrides telles que la percolation, le modèle *fusion-based quantum computing* (FBQC) de PsiQuantum, ou, dans le cas de Quandela, l'utilisation simultanée des spins des boîtes quantiques et des photons comme porteurs d'information. Cela nécessite d'être capable de fabriquer des boîtes quantiques avec des propriétés identiques.

143 [Multidimensional cluster states using a single spin-photon interface coupled strongly to an intrinsic nuclear register](#) by Cathryn P. Michaels *et al.*, University of Cambridge, April 2021 (11 pages).

photon qubits key takeaways

| highlights | challenges |
|---|---|
| <ul style="list-style-type: none"> • stable qubits with absence of decoherence. • ambient temperature for processing. • emerging nano-photonic manufacturing techniques enabling scalability. • easier to scale-out with inter-qubits communications and quantum telecommunications. • MBQC/FBQC circumventing the fixed gates depth computing capacity and difficulty to create multiple qubit gates. • boson sampling-based quantum advantage: starts to being programmable but a practical quantum advantage remains to be proven. | <ul style="list-style-type: none"> • need to cool photon sources and detectors: but at relatively reasonable temperatures between 2K and 10K, requiring lightweight cryogenic systems (unless also cooling the whole photonic circuit). • not yet scalable in number of operations: due to probabilistic character of quantum gates and the efficiency of photon sources in most paradigms. • non-deterministic cluster states and two-photon interactions. • needs delay lines and optical switches. • heat generated by phasers: increasing cooling budget. • photon detectors efficiency: 89% with PsiQuantum. • photon losses in nanophotonic circuits. |
| variations | path to scalability |
| <ul style="list-style-type: none"> • encoding: direct variables qubits (DV), continuous variables (CV) qubits, multimode photon encoding. • MBQC (measurement based quantum computing) and FBQC (fusion-based quantum computing). • BS/GBS: programmable Boson sampling and Gaussian boson sampling. • hybrid approach: spin-optical quantum computing (SPOQC) with quantum dots spin qubits (Quandela), hybrid atom-photon qubits. • classical photonic models: coherent Ising models, photonic waveguide arrays and interferometric systems. | <ul style="list-style-type: none"> • efficiency: improve photon sources efficiency, determinism and indistinguishability, improve photon detectors efficiency (SNSPD and PNRD). • cluster states: generate large cluster states, with or without heralding. • interactions: improve fusion efficiency in FBQC. • losses: large-scale and low-losses optical switches and wave guides, reduce photon losses in nanophotonic circuits thanks to higher precision manufacturing and new materials. • energy: create low-heating phasers to minimize power consumption. • nanophotonics: heterogeneous nanophotonic circuits (III-V + silicon). • classical control speed: particularly with FBQC models. |

Figure 12: Points forts, défis, variétés et options d'évolutivité des qubits photons.

3.3.1. AVANCÉES ET BÉNÉFICES CLÉS

Voici les points forts actuels de qubits à base de photons.

Ce sont des **qubits stables** et sans décohérence, en tout cas sur des courtes portées.

Ils permettent des **traitements à température ambiante**, notamment chez Quandela. Ce n'est pas l'approche retenue par PsiQuantum qui refroidit à 1,8K ses circuits de nanophotonique, lesquels intègrent directement des sources et des détecteurs de photons.

Une **bonne évolutivité** permise par les techniques de fabrication de nanophotonique qui permettront à terme d'assembler un grand nombre de qubits photons par circuit.

L'**interconnexion entre calculateurs quantiques photoniques** sera facilitée du fait qu'elle sera aussi réalisée à base de photons. Cependant, les longueurs d'onde du calcul quantique photonique ne sont pas forcément les mêmes que celles qui seront utilisées pour établir des liaisons quantiques distantes. Cela nécessitera donc probablement des conversions de fréquences. Celles-ci sont cependant plus faciles à réaliser que, par exemple, le passage du régime des micro-ondes à celui des photons infrarouges, qui est nécessaire pour les qubits supraconducteurs. La facilité de médiation de l'intrication par des photons est un point commun entre les qubits photons et les qubits à base d'atomes neutres et d'ions piégés.

Les **modèles de calcul à base de mesures** MBQC/FBQC permettront de contourner l'aspect probabiliste des portes à deux qubits et d'envisager la création d'ordinateurs quantiques photoniques à tolérance de pannes et qui montent en échelle.

Les **systèmes à base d'échantillonnage de bosons** commencent à être programmables, avec un avantage quantique pratique qui semble possible, notamment pour résoudre divers problèmes d'optimisation.

3.3.2. DÉFIS

Ils sont nombreux avec, notamment :

Le besoin de **refroidir les sources et détecteurs de photons**, mais à des températures relativement raisonnables situées entre 2 K et 10 K, nécessitant des systèmes cryogéniques légers, à moins de refroidir également l'ensemble du circuit photonique comme le fait PsiQuantum.

Les ordinateurs quantiques photoniques actuels ne sont **pas encore évolutifs** en nombre d'opérations en raison du caractère probabiliste des portes quantiques et de l'efficacité des sources de photons dans la plupart des paradigmes.

La création de **clusters déterministes**, ou aussi déterministes que possible de photons intriqués pour la mise en œuvre du modèle de calcul par la mesure MBQC.

Le besoin de **guides d'ondes à faibles pertes** et de commutateurs optiques qui restent à mettre au point.

La **chaleur dégagée par les phaseurs** qui génère une augmentation du budget de refroidissement, en particulier lorsque les circuits sont refroidis à la même température que les sources et les détecteurs.

L'**efficacité des détecteurs de photons** qui est encore trop faible, de 89 % chez PsiQuantum, sachant qu'il leur faut mettre au point des détecteurs de photons multiples.

3.3.3. VARIATIONS

En plus de l'encodage à variables continues et les modèles MBQC déjà évoqués, il existe d'autres technologies de calcul quantique ou semi-quantique à base de photons.

L'**échantillonnage de bosons** (*boson sampling*) correspond à une idée de Scott Aaronson and Alex Arkhipov dans un papier publié en 2010¹⁴⁴. Ils proposaient un système d'optique linéaire qui serait impossible à simuler efficacement classiquement. Il s'agit de résoudre un problème d'échantillonnage de la distribution de photons identiques et indiscernables qui sont mélangés dans un interféromètre et aboutissent ensuite dans des détecteurs de photons. La simulation classique de l'expérience coûte très cher mathématiquement, car elle repose sur l'évaluation du permanent de matrices carrées¹⁴⁵, un problème de la classe « #P difficile »¹⁴⁶. La vérification du résultat dépasserait même les capacités des ordinateurs classiques. Les premières expériences d'échantillonnage de bosons exploitaient des composants optiques passifs et non paramétrables¹⁴⁷. Puis, progressivement,

144 [The computational Complexity of Linear Optics](#) by Alex Arkhipov and Scott Aaronson, *Proceedings of the forty-third annual ACM symposium on Theory of computing* 2010 (94 pages).

145 [Lecture 3: Boson sampling](#) by Fabio Sciarrino, University of Rome, (63 slides), [Permanents and boson sampling](#) by Stefan Scheel, University of Rostock, 2018 (21 slides).

146 #P est la classe des problèmes consistant à décompter le nombre de solutions de problèmes NP.

147 [An introduction to boson-sampling](#) by Jonathan Dowling *et al.*, 2014 (13 pages) describes well the issues involved in conducting boson sampling.

notamment en Chine, des chercheurs sont parvenus à rendre ces expériences paramétrables avec des données en entrée et en sortie et la capacité à résoudre divers problèmes complexes, notamment autour de la théorie des graphes. Une variante développée en Chine est celle des échantillonneurs gaussiens de bosons (GBS, pour *Gaussian boson sampler*) avec Jiuzhang 1.0 en 2020 avec 70 modes de photons^{148,149}. Ils calculent l'équivalent de hafniens, qui évaluent le permanent de matrices carrées symétriques¹⁵⁰. Suivait Jiuzhang 2.0 en 2021 qui était paramétrable au niveau de la phase des photons entrants¹⁵¹, et avec la résolution de problèmes de graphes en 2023¹⁵². La même année, Jiuzhang 3.0 supportait la détection de 255 photons¹⁵³. En 2024, une autre équipe chinoise créait un GBS programmable qui pouvait résoudre un problème de recherche de molécule thérapeutique exploitant une technique de repliement d'ARN¹⁵⁴. En 2024, des chercheurs de l'Université du Maryland utilisaient un GBS pour résoudre un problème de machine learning¹⁵⁵. En 2022, Xanadu créait aussi un GBS programmable avec une installation plus simple, exploitant un multiplexage temporel de photons. Le système servait à résoudre des problèmes de graphes¹⁵⁶. En pratique, l'expérience de Xanadu était une première étape sur le chemin menant à la tolérance de panne dans un modèle basé sur la mesure (MBQC).

-
- 148 [Quantum computational advantage using photons](#) by Han-Sen Zhong *et al.*, December 2020 (23 pages) and the supplemental materials (64 pages).
- 149 [Benchmarking 50-Photon Gaussian Boson Sampling on the Sunway TaihuLight](#) by Yuxuan Li *et al.*, 2020 (12 pages).
- 150 [The Second Moment of Hafnians in Gaussian Boson Sampling](#) by Adam Ehrenberg *et al.*, *arXiv*, March 2024 (34 pages).
- 151 [Phase-Programmable Gaussian Boson Sampling Using Stimulated Squeezed Light](#) by Han-Sen Zhong, Chao-Yang Lu, Jian-Wei Pan *et al.*, June 2021 (9 pages).
- 152 [Solving Graph Problems Using Gaussian Boson Sampling](#) by Yu-Hao Deng *et al.*, February 2023 (7 pages).
- 153 [Gaussian Boson Sampling with Pseudo-Photon-Number Resolving Detectors and Quantum Computational Advantage](#) by Yu-Hao Deng *et al.*, China, *PRL*, April-October 2023 (6 pages).
- 154 [A universal programmable Gaussian Boson Sampler for drug discovery](#) by Shang Yu, Ian A. Walmsley, Guang-Can Guo *et al.*, *arXiv*, October 2022-March 2024 (11 pages).
- 155 [Biclustering a dataset using photonic quantum computing](#) by Ajinkya Borle, and Ameya Bhawe, University of Maryland, *arXiv*, May 2024 (32 pages).
- 156 [Using Gaussian Boson Sampling to Find Dense Subgraphs](#) by Juan Miguel Arrazola and Thomas R. Bromley, March-July 2018 (6 pages).

Les **modèles d'Ising¹⁵⁷ cohérents** (*Coherent Ising Machines* ou CIM) reposent sur des réseaux de guides d'ondes photoniques et systèmes interférométriques. La technique permet d'utiliser des réseaux de neurones optiques pour résoudre des problèmes de combinatoire qui sont convertis en modèles d'Ising NP-difficiles¹⁵⁸. L'un des plus grands CIM a été créé au Japon en 2021 avec des problèmes à résoudre comportant 100 000 spins¹⁵⁹. Ce genre de solution concurrence les systèmes de recuit quantique de D-Wave et de recuit simulé classiquement de Fujitsu¹⁶⁰.

Les **simulations à base de marches quantiques** qui fonctionnent avec des photons à variables discrètes ou continues^{161, 162}. Une équipe chinoise créait en 2022 une marche quantique à variables continues générant un espace de Hilbert de dimension 400¹⁶³. Les marches quantiques pourraient être réalisées avec des matrices de guides d'ondes programmables^{164, 165}.

Des **approches hybrides diverses** existent comme la proposition de calcul quantique spin-optique (SPOQC) de Quandela qui associe des qubits de spin

157 Voir par exemple <https://www.bing.com/search?q=Ising%20&qs=n&form=QBRE&sp=-1&ghc=2&lq=0&pq=ising%20&sc=11-6&sk=&cvid=566E3737143A46EC9B64666E40F84401>

158 [Coherent Ising Machines: non-von Neumann computing using networks of optical parametric oscillators](#) by Peter McMahon, Cornell University, October 2020 (100 slides).

159 [100,000-spin coherent Ising machine](#) by Toshimori Honjo *et al.*, September 2021 (8 pages).

160 [Coherent Ising machines - optical neural networks operating at the quantum limit](#) by Y. Yamamoto *et al.*, *npj Quantum*, December 2017 (16 pages).

161 [Quantum walks of two correlated photons in a 2D synthetic lattice](#) by Chiara Esposito, Fabio Sciarrino *et al.*, April 2022 (18 pages).

162 [Probing quantum walks through coherent control of high-dimensionally entangled photons](#) by Poolad Imany *et al.*, July 2020 (9 pages).

163 [Large-scale full-programmable quantum walk and its applications](#) by Yizhi Wang *et al.*, August 2022 (73 pages)

164 [Programmable high-dimensional Hamiltonian in a photonic waveguide array](#) by Yang Yang, Robert J. Chapman, Alberto Peruzzo *et al.*, ETH Zurich, Griffith University, Purdue University, University of Trento, Heriot-Watt University and Qubit Pharmaceuticals, *Nature Communications*, January 2024 (7 pages).

165 [Programmable quantum circuits in a large-scale photonic waveguide array](#) by Yang Yang, Alberto Peruzzo *et al.*, ETH Zurich, RMIT University, University of Muenster, Heriot-Watt University, University of Trento, Qubit Pharmaceuticals, *arXiv*, May 2024 (15 pages).

de boîtes quantiques exploitant l'intermédiation de photons pour les intriquer, et les mesurer, ou des approches associant atomes neutres et photons¹⁶⁶.

3.3.4. CHEMINS VERS L'ÉVOLUTIVITÉ

Le développement d'ordinateurs quantiques à tolérance de pannes à base de photons passe par la résolution de nombreux défis technologiques que voici :

L'amélioration des sources de photons en ce qui concerne leur efficacité, leur déterminisme, l'indiscernabilité et, surtout, dans la capacité à générer des états de cluster de grande taille.

L'amélioration de l'efficacité des détecteurs de photons au-delà de 90%.

L'amélioration de l'efficacité de la fusion dans le modèle FBQC proposé par PsiQuantum.

La **réduction des pertes de photons** dans les circuits de nanophotonique passant par une fabrication de plus grande précision et l'usage de nouveaux matériaux.

La **création de commutateurs optiques** pour le routage des photons entre les différents circuits et pour la mise en œuvre du «*feed-forward*» dans le modèle FBQC.

La **réduction de la consommation d'énergie** qui passe par la création de phaseurs à faible consommation d'énergie.

Développer des **composants de nanophotonique hétérogènes** associant par collage des briques III-V sur du silicium.

Architecturer le **contrôle classique des circuits** de manière à suivre le rythme des photons, en particulier avec les modèles FBQC et MBQC.

¹⁶⁶ [Deterministic photonic quantum computation in a synthetic time dimension](#) by Ben Bartlett, Avik Dutt and Shanhui Fan, Optica, November 2021 (9 pages).

3.3.5. FEUILLES DE ROUTE

Nous allons ici examiner les feuilles de route des principaux acteurs industriels des qubits photons, en vue de créer des ordinateurs quantiques à tolérance de pannes.

PsiQuantum (USA/UK/Australie) a fait le pari de créer un ordinateur quantique à tolérance de panne sans passer par l'intermédiaire d'une machine NISQ en mode KLM comme Quandela. Elle vise d'emblée la création de 100 qubits logiques d'ici le début des années 2030 et à partir d'un million de qubits physiques, les photons.

L'architecture de PsiQuantum repose sur une variante du modèle MBQC dénommée FBQC (*Fusion-based quantum computation*). Le MBQC repose sur la création de clusters de photons intriqués géants qui sont très difficiles à créer. Le modèle FBQC contourne le problème en créant des clusters de taille limitée, de l'ordre de 4 photons intriqués, et en les reliant par des mesures conjointes probabilistes. Les qubits sont encodés « en chemin » avec la technique du double rail (*dual rail*). La technique est délicate à évaluer, car elle fait appel à des processus probabilistes à différents niveaux : la génération des « *cluster states* », les fusions entre ces « *cluster states* », et la détection des photons.

L'autre choix de PsiQuantum consiste à intégrer dans des puces silicium l'intégralité de la photonique : les sources de photons, les guides d'ondes et opérations de calcul, le routage des photons et les détecteurs de photons, le tout opérant à 1,8K. Ces puces sont fabriquées sur des *wafers* 300 mm en technologie FD-SOI 22 nm chez GlobalFoundries dans l'état de New York. La machine à 100 qubits logiques reposera sur des milliers de ces puces reliées entre elles par des photons.

En avril 2024, la société décrivait où elle en était dans la mise au point de cette puce¹⁶⁷. Elle affiche de très bonnes fidélités d'opérations pour la génération

¹⁶⁷ [A manufacturable platform for photonic quantum computing](#) by Koen Alexander *et al.*, PsiQuantum, *arXiv*, April 2024 (8 pages).

de photons et pour les portes à un et deux qubits¹⁶⁸. Les écueils résident dans l'efficacité de la détection des photons qui est de seulement 89% et dans les pertes de photons dans les circuits. De nombreux autres défis restent à relever dans la génération des photons, dans la création de guides d'onde à faibles pertes en nitrure de silicium, avec des déphaseurs plus efficaces, la création d'un système de routage de photons matriciel, des coupleurs directionnels, des couplages entre circuits et fibres optiques et enfin, la création de détecteurs de photons multiples exploitant un multiplexage spatial de détecteurs de photons uniques de type SNSPD¹⁶⁹. Leur feuille de route prévoit de résoudre tous ces problèmes en six ans, ce qui semble plutôt optimiste.

Enfin, une première estimation de la puissance nécessaire pour alimenter cette machine est d'environ 10 MW juste pour la cryogénie, ce qui serait prohibitif si la puissance nécessaire pour générer les milliers de qubits logiques nécessaires pour de nombreux algorithmes croissait linéairement avec leur nombre.

Xanadu Quantum Technologies (Canada) développe aussi un ordinateur quantique photonique à tolérance de panne, à base de photons à variables continues, mais sur un modèle MBQC^{170, 171, 172}. Celui-ci est documenté dans un papier de 2021¹⁷³. Ses puces à nitrure de silicium étaient fabriquées par IMEC en Belgique, mais en 2022, la société a annoncé un partenariat

168 With: 99.98% \pm 0.01% state preparation and measurement fidelity, Hong-Ou-Mandel quantum interference between independent photon sources with 99.50% \pm 0.25% visibility, two-qubit fusion with 99.22% \pm 0.12% fidelity, and a chip-to-chip qubit interconnect with 99.72% \pm 0.04% fidelity.

169 "The performance of the baseline technology described above is still not sufficient for useful photonic quantum computing. In particular, silicon waveguides incur too much propagation loss for fault tolerance, photon sources require complex and power-hungry tuning, and high-speed optical switching is unavoidably necessary to overcome the intrinsic nondeterminism of the spontaneous single photon sources".

170 [The power of one qumode for quantum computation](#), 2016 (10 pages), [Continuous-variable gate decomposition for the Bose-Hubbard model](#), 2018 (9 pages).

171 [Optical hybrid approaches to quantum information](#) by Peter van Loock, 2010 (35 pages).

172 [Quantum computing with multidimensional continuous-variable cluster states in a scalable photonic platform](#) by Bo-Han Wu *et al.*, 2020 (22 pages).

173 [Blueprint for a Scalable Photonic Fault-Tolerant Quantum Computer](#) by J. Eli Bourassa *et al.*, February 2021 (38 pages).

avec GlobalFoundries. Elle prévoit d'atteindre 1000 qubits logiques, qui demanderaient 10 000 racks de data center, ce qui est quelque peu inquiétant. En 2022, Xanadu démontrait un avantage quantique réalisé avec un échantillonneur gaussien de bosons (GBS) dans son QPU Borealis, atteignant un record de 216 modes de photons s'appuyant sur du multiplexage en fréquence et des lignes à retard. Son système est paramétrable au niveau des phases des photons entrant dans l'échantillonneur¹⁷⁴.

Quandela (France) prévoit d'adopter une déclinaison du modèle FBQC pour créer un ordinateur à tolérance de pannes. Ses travaux de recherche sont multiples, à commencer par la génération de *cluster states* de photons intriqués très efficaces¹⁷⁵, la polarisation des photons générés étant contrôlée par le champ magnétique auquel est exposée la boîte quantique les générant¹⁷⁶. Elle en est pour l'instant à des clusters de 4 photons¹⁷⁷. En novembre 2023, Quandela publiait une feuille de route détaillant son modèle SPOQC (*spin-optical quantum computing*) qui associe des qubits de données qui sont supportés par les boîtes quantiques sources de photons, et les photons qu'ils émettent comme qubits auxiliaires permettant notamment de gérer des portes à deux qubits entre les boîtes quantiques¹⁷⁸. Ces portes utilisent la technique de la répétition jusqu'au succès (*repeat until success*, ou RUS) ainsi qu'un routage de photons permettant de relier toutes les boîtes quantiques entre elles, un défi voisin du routage de photons envisagé par PsiQuantum. L'architecture repose en effet sur des codes de correction d'erreur de type qLDPC qui nécessitent une telle connectivité. Un autre défi à relever consiste à rallonger la durée de cohérence des boîtes quantiques

174 [The hardness of quantum spin dynamics](#) by Chae-Yeun Park *et al.*, Xanadu, Sungkyunkwan University, December 2023 (30 pages).

175 [High-rate entanglement between a semiconductor spin and indistinguishable photons](#) by Nathan Coste, Sophia Economou, Niccolo Somaschi, Alexia Auffèves, Loic Lanco, Pascale Senellart *et al.*, *Nature Photonics*, July 2022 (17 pages).

176 [Controlling photon polarisation with a single quantum dot spin](#) by Elham Mehdi, Pascale Senellart, Loic Lanco *et al.*, December 2022 (9 pages).

177 [Quantifying n-photon indistinguishability with a cyclic integrated interferometer](#) by Mathias Pont, Fabio Sciarrino, Pascale Senellart, Andrea Crespi *et al.*, PRX, January-September 2022 (21 pages).

178 [A Spin-Optical Quantum Computing Architecture](#) by Grégoire de Gliniasty, Paul Hilaire, Pierre-Emmanuel Emeriau, Stephen C. Wein, Alexia Salavrakos, Shane Mansfield, Quandela and LIP6, November 2023 (20 pages).

qui est actuellement bien trop faible pour supporter ce modèle. Le record dans le domaine provient de l'Université de Cambridge, avec une cohérence de 0,11 ms^{179, 180}. Quandela a aussi établi un partenariat technologique avec Welinq (France) pour le développement d'une solution d'interconnexion entre processeurs quantiques exploitant les mémoires quantiques à base d'atomes neutres de ce dernier.

ORCA Computing (UK) développe une plateforme de calcul photonique quantique à base de photons à variables continues de type qumodes et d'une technologie de mémoire quantique exploitant des lignes à retard et des séparateurs de faisceaux^{181,182}. Ses puces sont fabriquées par Ligentec en Suisse, comme pour Quandela. Elle planche aussi sur la création de *cluster states* et sur un modèle FBQC voisin de celui de PsiQuantum^{183,184}.

QuiX Quantum (Pays-Bas) développe des circuits de calcul photonique quantique à base de nitrures de silicium (Si_3N_4) à faible perte qui utilisent des déphaseurs thermo-optiques et des séparateurs de faisceaux optiques programmables¹⁸⁵. En 2022, ils supportaient 20 «qumodes»¹⁸⁶ à l'aide de 380 déphaseurs et d'une source de photons exploitant un laser Ti:Sapphire et un cristal. La société prévoit des réalisations capables de supporter 10 000 qumodes après 2030, mais n'a pas publié de véritable *roadmap* FTQC.

179 [Researchers find ways to improve the storage time of quantum information in a spin rich material](#) by the Cavendish Laboratory of the Department of Physics of the University of Cambridge, January 2023.

180 [Ideal refocusing of an optically active spin qubit under strong hyperfine interactions](#) by Leon Zaporski, Claire Le Gall (who now is VP of the quantum management team at Nu Quantum) *et al.*, University of Cambridge, University of Sheffield, University of Oxford, *Nature Nanotechnology*, January 2023 (23 pages).

181 [One-Way Quantum Computing in the Optical Frequency Comb](#) by Nicolas C. Menicucci, Steven T. Flammia and Olivier Pfister, April 2018 (4 pages).

182 [High-speed noise-free optical quantum memory](#) by K. T. Kaczmarek *et al.*, April 2018 (12 pages).

183 [High photon-loss threshold quantum computing using GHZ-state measurements](#) by Brendan Pankovich *et al.*, Orca Computing, August 2023 (15 pages).

184 [Flexible entangled state generation in linear optics](#) by Brendan Pankovich *et al.*, Orca Computing, October 2023 (20 pages).

185 [Quantum simulation of thermodynamics in an integrated quantum photonic processor](#) by Frank H. B. Somhorst *et al.*, December 2021 – March 2023 (20 pages).

186 [20-Mode Universal Quantum Photonic Processor](#) by Caterina Taballione, June 2022 (9 pages).

3.3.6. CONCLUSION

La filière des qubits photons est originale par rapport à toutes les autres filières évaluées dans ce rapport. Elle présente autant d'avantages que de défis de taille. Ils tournent presque tous autour du côté très probabiliste des opérations quantiques avec des photons. Les enjeux sont de créer des états intriqués de photons aussi déterministes que possible, de perdre le moins de photons possible dans les circuits de calcul et de bien les détecter en bout de course. Il est très difficile de se prononcer sur la faisabilité d'ensemble tant les paramètres en jeu sont nombreux.

On peut poser la question de la possibilité de réaliser des portes déterministes entre photons dans le domaine optique, ce qui est envisageable en utilisant des techniques d'électrodynamique en cavité (*cavity* QED, comme dans les expériences de Gerhard Rempe au MPQ de Munich ou avec des super-atomes de Rydberg comme dans les expériences d'Alexei Ourjoumtev au Collège de France). Ces expériences fonctionnent entre deux qubits photoniques, mais sont très complexes et actuellement très éloignées d'une possible mise à l'échelle. Remarquons enfin que les interactions entre photons dans le domaine micro-onde fonctionnent très bien, et sont à la base des « qubits de chat » discutés par ailleurs.

3.4. SPINS DANS LE SILICIUM

Les qubits de spins d'électrons constituent une technologie prometteuse et, comme les autres, sujette à de nombreuses variations. Ses développements sont plus récents que pour les qubits à base d'ions piégés et de supraconducteurs à effet Josephson.

Les qubits de ce type utilisent l'orientation de spin d'électrons piégés dans des puits de potentiel selon une direction donnée, ou de trous de spin correspondant à un électron manquant dans une structure, le tout sous un champ magnétique statique.

L'idée de créer des qubits de spin vient de Daniel Loss (Université de Bâle) et David DiVincenzo (alors chez IBM Research) dans un papier datant de 1997¹⁸⁷. Ils proposaient une porte à deux qubits utilisant un contrôle électrique de la barrière de tunnel entre des boîtes quantiques voisines. Une faible tension de déclenchement crée un couplage entre les qubits voisins. La conception proposait aussi des portes à un qubit. Le concept a ensuite été étendu à l'utilisation de paires de spins d'électrons de boîtes quantiques, l'un étant le qubit lui-même, et l'autre, couplé capacitivement avec le premier et utilisé pour la lecture du premier qubit. Cette lecture implique une conversion de spin en charge utilisant une mesure de conductance, généralement avec une réflectométrie radiofréquence utilisant une impulsion micro-ondes, un peu comme avec la lecture de qubits supraconducteurs.

Les premières démonstrations de qubit de spin dans le silicium ont été réalisées en Australie en 2012 dans le groupe d'Andrew Dzurak d'UNSW. En 2016, ils étaient réalisés en utilisant un processus de fabrication semi-industriel par une équipe du CEA-Leti et du CEA-IRIG à Grenoble¹⁸⁸. Cette technique dite Si-MOS est dérivée des MOS planaires et FDSOI.

Les portes à un qubit sont générées par l'exposition des boîtes quantiques à un champ magnétique oscillant. Les portes à deux qubits sont générées en abaissant la barrière de potentiel entre deux boîtes adjacentes avec une tension électrique. La mesure du qubit peut se faire de différentes manières, la plus courante étant à base de conversion de spin en charge, en passant souvent par un second électron apparié à celui qu'il faut mesurer et dont le spin est inversé du fait du blocage de Pauli^{189,190}.

187 [Quantum computation with quantum dots](#) by Daniel Loss and David DiVincenzo, 1997 (20 pages).

188 [A CMOS silicon spin qubit](#) by Romain Maurand, Maud Vinet, Marc Sanquer, Silvano De Franceschi *et al.*, 2016 (12 pages).

189 [Rapid single-shot parity spin readout in a silicon double quantum dot with fidelity exceeding 99 %](#) by Kenta Takeda *et al.*, RIKEN and QuTech, npj Quantum Information, February 2024 (6 pages).

190 [Modeling and Experimental Validation of the Intrinsic SNR in Spin Qubit Gate-Based Readout and Its Impacts on Readout Electronics](#) by Bagas Prabowo, Lieven M. K. Vandersypen *et al.*, QuTech, December 2023 (16 pages).

quantum dots spin qubits key takeaways

| | |
|--|---|
| <p style="text-align: center; margin: 0;">highlights</p> <ul style="list-style-type: none"> qubits fidelity: reaching 99.5% for two-qubit gates in labs for a small number of qubits (RIKEN, 2022). simpler qubit drive than with superconducting qubits. good quantum gates times: 75 ns for two-qubit gates. operating temperature: around 100 mK - 1K => larger cooling budget for control electronics vs superconducting qubits. 2D architectures: usable with surface codes or color codes QEC. manufacturing: can leverage existing semiconductor fabs. cryo-CMOS developments: for scalable qubit drive. scalability potential: could reach millions of qubits, thanks to their size of 100x100 nm. | <p style="text-align: center; margin: 0;">challenges</p> <ul style="list-style-type: none"> research in the field: started later than with other qubit technologies and spread over several technologies (full Si, SiGe, atom spin donors). lesser funded startups: and Intel relatively modest investment. qubit addressing and unsettled qubit drive techniques (ESR, ...). high fabs costs and long test cycles: 18 months average. only 4 to 15 entangled qubits (QuTech, UNSW, Princeton, University of Tokyo). long-distance coupling between qubits, which enables more efficient QEC like qLDPC. high qubits variability: requires calibration. charge noise and other sources of noise to address, and scalability that remains to be demonstrated. |
| <p style="text-align: center; margin: 0;">variations</p> <ul style="list-style-type: none"> SiGe qubits: spins or holes, more complicated to manufacture but better gate fidelities. donor spins: phosphorus atom nucleus, more complicated to scale. carbon nanotubes : with better spin stability but harder to manufacture and drive, with only one startup (C12). spin on superfluid helium or neon with only one startup in the domain (EeroQ). | <p style="text-align: center; margin: 0;">path to scalability</p> <ul style="list-style-type: none"> materials purity improvements: isotopic and element impurities. manufacturing: improvements, faster cycling and characterization. full-stack EDA for digital simulation. long range qubit coupling within chips: to enable efficient qLDPC QEC. SFQ electronics for qubit drive. cryo-CMOS integration with qubits: for better integration. inter-QPU connectivity: electron spin shuttling, hole-microwave photons coupling, color centers. |

Figure 13: Points forts, défis, variétés et options d'évolutivité des qubits à base de spins dans des boîtes quantiques.

3.4.1. AVANCÉES

Voici quelques avancées récentes ou points forts des qubits de spin.

La **fidélité des portes quantiques** peut atteindre 99,5 % pour des portes à deux qubits en laboratoire pour un petit nombre de qubits, selon une expérience de 2022 réalisée par RIKEN au Japon¹⁹¹. Cette fidélité est cependant sujette à caution, car elle n'a jamais été obtenue à l'échelle de plusieurs dizaines de qubits et mesurée avec des *benchmarks* de type « *randomized benchmarks* ».

Le **contrôle des qubits** est plus simple qu'avec des qubits supraconducteurs. On a toujours besoin de pulsations micro-ondes pour générer des portes à

¹⁹¹ [Fast universal quantum control above the fault-tolerance threshold in silicon](#) by Akito Noiri, Giordano Scappucci *et al.*, 2022 (27 pages).

un qubit et pour la lecture des qubits, mais les portes à deux qubits sont plus simples à mettre en œuvre avec des contrôles par tensions.

La **durée des portes quantiques** est compétitive, comparée à celle des autres types de qubits, avec par exemple 75 ns pour une porte à deux qubits en SiGe « à trous »¹⁹².

Un **fonctionnement à une température plus élevée** que celle des qubits supraconducteurs, comprise entre 100 mK et 1,5 K¹⁹³, notamment du fait des énergies utilisées dans les signaux de contrôle des qubits. Cela procure un plus grand budget de refroidissement à consommation électrique équivalente en cryogénie, permettant d'avoir une quantité plus grande d'électronique de contrôle basse température et donc, d'avoir le contrôle d'un plus grand nombre de qubits physiques.

L'**architecture 2D** des circuits les rend utilisables avec des codes de surface. C'est une caractéristique voisine de celle des qubits supraconducteurs. Elle n'a cependant pas encore été validée expérimentalement.

La **capitalisation sur l'expérience** de fabrication de l'industrie de la nanoélectronique autour des composants CMOS qui sont voisins de ceux de ces qubits de spins. Elle est mise en avant par tous les acteurs industriels, mais est toutefois à prendre avec du recul. Cette expérience n'a pas encore porté ses fruits pour permettre la production de qubits de qualité suffisante pour rivaliser, par exemple, avec les qubits supraconducteurs.

Les **développements d'électronique basse température** de type cryo-CMOS et SFQ permet d'envisager une bonne montée en échelle à moindre coût, ce d'autant plus que le budget de cryogénie disponible est plus élevé pour faire fonctionner ces composants, notamment de type cryo-CMOS, du fait d'une température de fonctionnement plus élevée que pour les qubits supraconducteurs.

192 [Fast two-qubit logic with holes in germanium](#) by N.W. Hendrickx, Menno Veldhorst, Giordano Scappucci *et al.*, January 2020 in *Nature* et on *arXiv* in April 2019 (6 pages).

193 [Hotter is easier: unexpected temperature dependence of spin qubit frequencies](#) by Brennan Undseth, Lieven M. K. Vandersypen *et al.*, April 2023 (17 pages).

La **capacité de miniaturisation** plus grande du fait d'une taille de qubit de l'ordre de 100×100 nm permettant en théorie de supporter l'intégration de millions de qubits physiques sur une seule puce^{194, 195}. C'est un point clé pour la tolérance de pannes pour retarder autant que possible le besoin de faire appel à des technologies d'interconnexions entre puces quantiques. Cette miniaturisation pourrait avoir à terme une incidence économique positive, permettant le développement d'ordinateurs quantiques extensibles à l'échelle, à moindre coût. C'est d'autant plus important que les solutions opérationnelles de calcul à tolérance de pannes pour résoudre des problèmes complexes, par exemple en chimie quantique, nécessiteront d'exécuter les mêmes circuits quantiques sur plusieurs processeurs quantiques similaires et en parallèle.

3.4.2. DÉFIS

La **recherche** dans les qubits de spin a démarré plus tard qu'avec les autres technologies de qubits (atomes froids, ions piégés, supraconducteurs), et s'étend sur plusieurs voies concurrentes industrielles (Si, SiGe, donneurs de spin atomique) avec relativement peu d'acteurs.

Les **startups** sont moins nombreuses et moins bien financées que pour les autres types de qubits, et Intel, le plus grand acteur du domaine, y consacre un investissement relativement modeste, en tout cas au regard des investissements correspondants d'IBM et Google dans les qubits supraconducteurs, ou même des startups telles que IonQ et Quantinuum dans les ions piégés ainsi que PsiQuantum et Xanadu dans les photons.

Les **techniques d'adressage et de pilotage des qubits** ne sont pas encore bien sédimentées, surtout pour opérer à grande échelle¹⁹⁶.

194 [The path to scalable quantum computing with silicon spin qubits](#) by Maud Vinet, *Nature Nanotechnology*, December 2021.

195 [Scaling silicon-based quantum computing using CMOS technology: State-of-the-art, Challenges and Perspectives](#) by M. F. Gonzalez-Zalba, Silvano de Franceschi, Tristan Meunier, Maud Vinet, Andrew S. Dzurak *et al.*, *Nature Electronics*, November 2020-April 2023 (21 pages).

196 [A Crossbar Network for Silicon Quantum Dot Qubits](#) by R Li *et al.*, 2017 (24 pages).

Les **coûts de fabrication des wafers** sont élevés et les cycles de test sont assez longs, de l'ordre de 18 mois en moyenne. C'est la technologie pour laquelle ces cycles de conception, fabrication et tests sont les plus longs. Cela a un impact indirect sur la vitesse de maturation de la technologie, malgré ses promesses. Les acteurs industriels font appel à différentes méthodes pour raccourcir ces cycles : fabrication internalisée dans des salles blanches de recherche avec du personnel dédié (SemiQon chez VTT), recourt à des lignes de fabrication industrielle (Diraq, Quobly, Quantum Motion et Equal chez GlobalFoundries et ARQUE chez Infineon), des tests de plusieurs designs sur les mêmes wafers et la création de jumeaux numériques pour simuler les circuits.

Le **nombre de qubits** contrôlés et intriqués est pour l'instant limité à 4 à 15 qubits (QuTech, UNSW, Princeton, Université de Tokyo). La montée à l'échelle n'a pas encore été démontrée d'un point de vue expérimental.

La **variabilité élevée des qubits** qui nécessite un étalonnage, à l'instar des qubits supraconducteurs. Par ailleurs, la fidélité de la lecture des qubits, qui est située actuellement autour de 99 %, devrait être améliorée.

Le **bruit de charge** et d'autres sources de bruits affectent la performance des qubits. Le travail sur le design, les matériaux et la fabrication continue pour les réduire¹⁹⁷.

3.4.3. VARIATIONS

Voici les principales variations technologiques de qubits de spin dans du silicium et par extension dans des structures exotiques de graphène et autres.

Silicium-germanium. Il s'agit d'hétérostructures en silicium, germanium et silicium-germanium où le germanium est utilisé pour la stabilité des spins de

197 [Decoherence of solid-state spin qubits: a computational perspective](#) by Mykyta Onizhuk, and Giulia Galli, University of Chicago, *arXiv*, May 2024 (25 pages).

trous^{198, 199}, de larges bandes interdites, une meilleure mobilité des électrons, un meilleur couplage de moments cinétiques spin-orbite, et de longs temps de cohérence. Les spins de trou sont gérés avec des boîtes quantiques en germanium entre deux couches de SiGe tandis que les qubits de spins utilisent une boîte en silicium entre les mêmes couches de SiGe. Ces qubits sont cependant plus difficiles à fabriquer, avec des portes qui se contrôlent à distance des qubits²⁰⁰, et avec diverses sources de bruit qui restent à contenir^{201, 202}.

Atomes de phosphore donneurs de spin. Il s'agit de la technique proposée par Bruce Kane (UNSW) en Australie en 1998. Il s'agit d'utiliser des atomes de phosphore (³¹P) dans une structure cristalline de silicium²⁰³. Cette approche hybride exploite la résonance magnétique nucléaire pour contrôler le spin du noyau de ces atomes et les coupler au spin d'un des électrons de la couche de valence du phosphore qui n'est pas relié aux atomes de silicium avoisinants. Les qubits sont contrôlés par des champs électriques et magnétiques²⁰⁴. Le principal bénéfice réside dans la longue durée de cohérence des spins de noyau du phosphore qui constituent les qubits, qui peut atteindre plusieurs secondes²⁰⁵. Les défis relèvent du placement des atomes sur le *wafers* en silicium, une technique maintenant maîtrisée par la startup australienne SQC qui exploite un microscope à balayage par effet tunnel et la mise en œuvre des portes quantiques à un et deux qubits.

198 [Recent advances in hole-spin qubits](#) by Yinan Fang *et al.*, October 2022 (46 pages).

199 [Coherent control of a high-orbital hole in a semiconductor quantum dot with near-unity fidelity](#) by Junyong Yan *et al.*, December 2022 (27 pages).

200 [The germanium quantum information route](#) by Giordano Scappucci, Silvano De Franceschi *et al.*, 2020 (18 pages).

201 [Simulation of 1/f charge noise affecting a quantum dot in a Si/SiGe structure](#) by Marcin Kępa *et al.*, March 2023 (7 pages).

202 [Spatial noise correlations beyond nearest-neighbor in 28Si/SiGe spin qubits](#) by Juan S. Rojas-Arias, Daniel Loss *et al.*, February 2023 (11 pages).

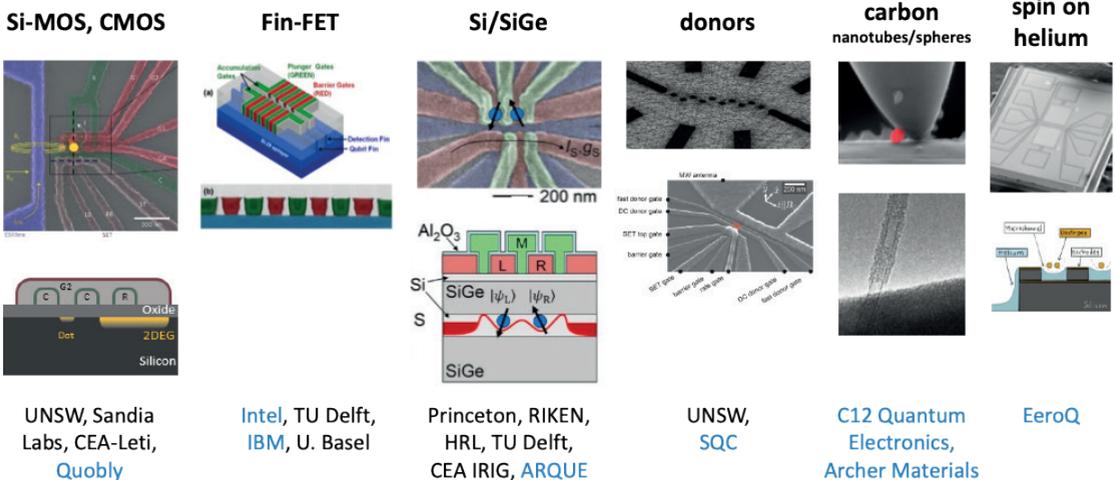
203 [A silicon-based nuclear spin quantum computer by Bruce Kane, Nature, 1998 and Silicon-based Quantum Computation](#) by Bruce E. Kane, 2000 (14 pages).

204 [The Race To Make Better Qubits](#) by Katherine Derbyshire, Semiconductor Engineering, November 2021.

205 [Toward a Silicon-Based Nuclear-Spin Quantum Computer](#) by Robert G. Clark, P. Chris Hammel, Andrew S. Dzurak, Alexander Hamilton, Lloyd Hollenberg, David Jamieson, and Christopher Paves, Los Alamos Science, 2022 (18 pages).

Nanotubes de carbone, la technique proposée par la startup française C12, qui permet d'obtenir une meilleure stabilité de spin, au prix d'un contrôle un peu plus complexe des qubits et des portes à deux qubits^{206, 207}. La startup australienne Archer Materials proposait depuis plusieurs années le développement de qubits à base de nanosphères de carbone. Elle semble avoir abandonné cette filière pour le calcul quantique et se focalise maintenant sur la création de capteurs quantiques pour des applications médicales.

Spin sur hélium superfluide²⁰⁸ ou sur néon²⁰⁹, une technique relativement exotique explorée par des laboratoires tels que RIKEN au Japon et par la startup EeroQ aux USA.



206 [Carbon Nanotube Devices for Quantum Technology](#) by Andrey Baydin *et al.*, MDPI, February 2022 (26 pages).

207 [Long-lived electronic spin qubits in single-walled carbon nanotubes](#) by Jia-Shiang Chen *et al.*, *Nature communications*, February 2023 (8 pages).

208 [Blueprint for quantum computing using electrons on helium](#) by Erika Kawakami *et al.*, RIKEN, QunaSys, OIST, and DLR, March 2023-September 2023 (28 pages).

209 [Single electrons on solid neon as a solid-state qubit platform](#) by Xianjing Zhou, Kater W. Murch, David I. Schuster *et al.*, *Nature*, May 2022 (16 pages).

Figure 14: Différents types de qubit de spins à boîtes quantiques. (cc) Olivier Ezratty, 2022-2023.

3.4.4. CHEMINS VERS L'ÉVOLUTIVITÉ

Voici les voies envisagées par les acteurs académiques et industriels des qubits de spin pour monter en échelle :

L'amélioration de la pureté des matériaux qui commence par l'usage, maintenant consacré, de l'isotope 28 du silicium en FD-SOI pour créer les boîtes quantiques. D'autres travaux portent sur la pureté des matériaux utilisés²¹⁰ qui permet notamment de réduire le bruit de charge^{211, 212}.

Le développement de techniques de fabrication industrielles avec l'apport des salles blanches de GlobalFoundries, Intel, STMicroelectronics et à terme, potentiellement, de TSMC, qui a créé une équipe exploratoire sur le sujet en 2023.

La création de solutions de conception et simulation électronique « full-stack » pour les circuits. C'est une approche notamment retenue par Quobly.

Le couplage de qubits à longue portée pour permettre l'utilisation de codes de correction d'erreur de type qLDPC qui sont plus efficaces et nécessitent moins de qubits physiques par qubit logique²¹³.

L'intégration de composants de contrôle cryo-CMOS à proximité de la puce des qubits, avec des solutions de type chiplet, le tout en optimisant la consommation d'énergie et la capacité de cryostats adaptés à des températures opérationnelles comprises entre 100 mK et 1K.

210 [Materials for Silicon Quantum Dots and their Impact on Electron Spin Qubits](#) by Andre Saraiva, Wee Han Lim, Chih Hwan Yang, Christopher C. Escott, Arne Laucht and Andrew S. Dzurak, December 2021 (22 pages).

211 [Low charge noise quantum dots with industrial CMOS manufacturing](#) by Asser Elsayed *et al.*, IMEC, December 2022 (22 pages).

212 [Stabilizing an individual charge fluctuator in a Si/SiGe quantum dot](#) by Feiyang Ye, Ammar Ellaboudy, and John M. Nichol, University of Rochester, *arXiv*, July 2024 (6 pages).

213 [Coherent Spin-Spin Coupling Mediated by Virtual Microwave Photons](#) by Patrick Harvey-Collard, Jurgen Dijkema, Guoji Zheng, Amir Sammak, Giordano Scappucci, and Lieven M. K. Vandersypen, QuTech, Physical Review X, May 2022 (16 pages).

Le **développement d'électronique SFQ** supraconductrice pour le pilotage des qubits, qui est pour l'instant l'apanage d'une seule société, SeeQC (USA). Ceci pourrait permettre une montée en échelle des qubits de spin avec un budget de cryogénie limité. Cette électronique n'est cependant pas encore au point.

Le **développement de techniques d'interconnexion** entre processeurs quantiques, avec des électrons volants²¹⁴, des couplages de photons trou-micro-ondes, des couplages de spins avec des centres colorés (type NVcenter) et enfin, l'usage de photons optiques. Des tests d'électrons volants ont été réalisés en 2024 sur une distance de 10 μm en <200 ns avec une fidélité moyenne de 99%²¹⁵.

3.4.5. FEUILLES DE ROUTE

À ce stade, la grande majorité des acteurs industriels de ces types de qubits ont publié des *roadmaps* qui sont surtout NISQ, avec des évolutions prudentes et peu chiffrées envisagées vers le FTQC :

Intel (USA) fait le pari des qubits silicium-germanium, qu'il met au point avec l'aide de QuTech aux Pays-Bas. Leur dernière puce de 12 qubits, Tunnel Falls, date de juin 2023. Elle a été fournie à des universités principalement américaines pour intégration et tests, reflétant une stratégie OEM d'Intel à l'instar de celle de ses processeurs classiques²¹⁶. La puce était gravée sur *wafers* de 300 mm sur son site d'Hillsboro dans l'Oregon, avec une lithographie EUV ASML. Intel a fait plusieurs présentations à l'APS March meeting 2024 de Minneapolis où elle a dévoilé que les fidélités des portes à deux qubits

214 [Coherent shuttle of electron-spin states](#) by Lieven Vandersypen *et al.*, 2017 (21 pages).

215 [High-fidelity single-spin shuttling in silicon](#) by Maxim De Smet, Lieven M.K. Vandersypen *et al.*, QuTech and TU Delft, *arXiv*, June 2024 (15 pages).

216 [Characterization of individual charge fluctuators in Si/SiGe quantum dots](#) by Feiyang Ye, John M. Nichol *et al.*, University of Rochester and Sandia Labs, *arXiv*, January 2024 (37 pages) is about characterizing a 4-quantum dot circuit, seemingly not coming from Intel, or at least, not being Tunnel Falls.

de cette puce étaient de 92 %, ce qui est peu satisfaisant²¹⁷. Intel développe aussi des puces cryo-CMOS de contrôle avec, notamment, Horse Ridge 2 en 2021, qui opère à 4 K et génère tous les signaux de contrôle et les fonctions de lecture de l'état des qubits silicium. En 2024, elle complétait cette puce avec Pando Tree, qui fonctionne à la température des qubits et permet de démultiplexer des signaux de contrôle provenant de Horse Ridge 2, avec un gain important en lignes de contrôle. Intel n'a pas publié de *roadmap* FTQC.

Quantum Motion (UK) travaille en parallèle sur ses qubits de spin et sur des composants de contrôle cryo-CMOS. En 2021, elle présentait avec Hitachi Cambridge, l'Université de Cambridge et l'EPFL un chip opérant à 50 mK comprenant à la fois des qubits et une électronique de routage des signaux de contrôle²¹⁸. Elle complétait cela en 2024 avec une architecture modulaire de chip de qubits et un amplificateur bas-bruit cryo-CMOS pour la lecture de l'état des qubits²¹⁹. Elle a dévoilé son architecture en août 2022²²⁰ suivie de sa puce Bloomsbury de $3 \times 3 \text{ mm}^2$ fabriquée chez Global Foundries avec 1024 *quantum dots*²²¹. En juin 2023, elle a expliqué comment elle pourrait exécuter un même circuit quantique plusieurs fois en parallèle de manière efficace²²². Au lieu d'arranger N qubits dans une matrice de $\sqrt{N} \times \sqrt{N}$ qubits, elle prévoit de créer une matrice de $N \times D$, D étant le nombre de fois qu'un circuit doit être exécuté. Cela augmente évidemment la taille du circuit. elle prévoit de créer un ordinateur FTQC de 100 qubits logique d'ici 2029.

217 [Intel Presents 12 Quantum Research Papers at APS March Meeting 2024](#) by Intel, March 2024. Probably in "High-fidelity Operation of Encoded Spin Qubits on Intel Tunnel Falls" by Felix F Borjans but its content is not public.

218 [Integrated multiplexed microwave readout of silicon quantum dots in a cryogenic CMOS chip](#) by A. Ruffino, Edoardo Charbon *et al.*, Quantum Motion, Hitachi and EPFL, January 2021 (14 pages).

219 [A multi-module silicon-on-insulator chip assembly containing quantum dots and cryogenic radio-frequency readout electronics](#) by David J. Ibberson, James Kirkman, John J. L. Morton, M. Fernando Gonzalez-Zalba, and Alberto Gomez-Saiz, Quantum Motion and UCL, *arXiv*, May 2024 (3 pages).

220 [Silicon edge-dot architecture for quantum computing with global control and integrated trimming](#) by Michael A. Fogarty, August 2022 (13 pages).

221 [Rapid cryogenic characterisation of 1024 integrated silicon quantum dots](#) by Edward J. Thomas *et al.*, Quantum Motion and UCL, October 2023 (22 pages).

222 [Pipeline quantum processor architecture for silicon spin qubits](#) by S. M. Patomäki, Simon Benjamin *et al*, *npj Quantum Information*, March 2024 (10 pages).

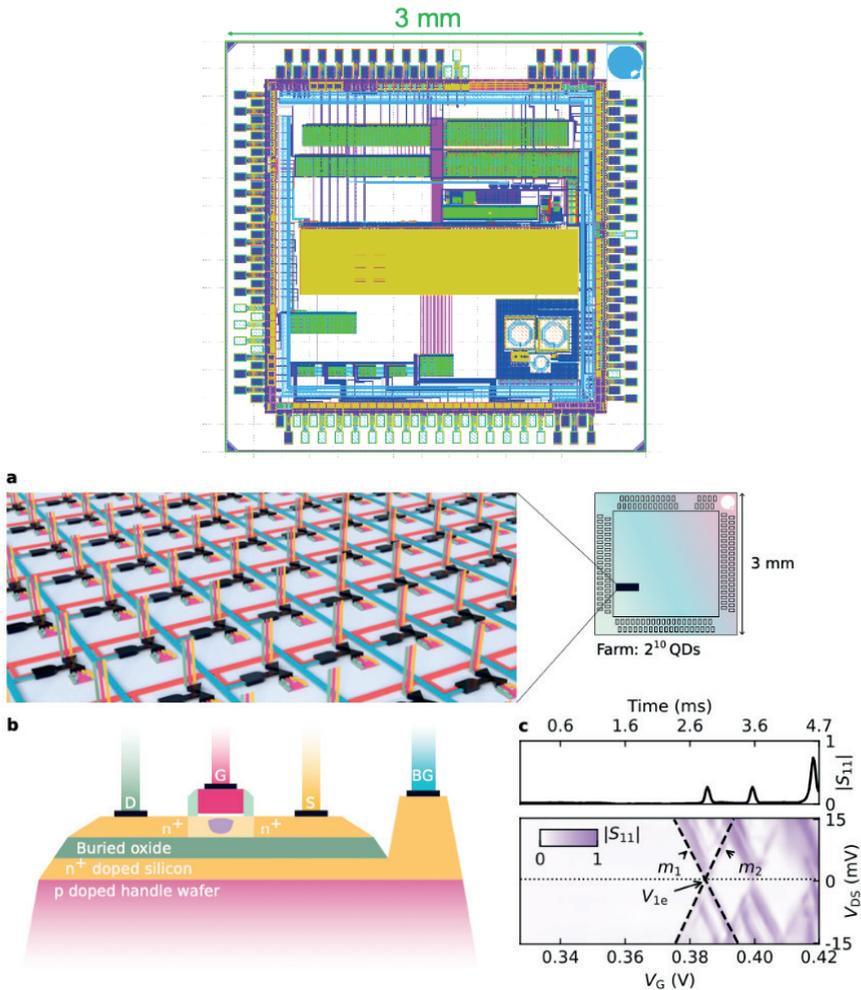


Figure 15: La puce Bloomsbury de Quantum Motion fabriquée par GlobalFoundries.
Source: Quantum Motion, Q2B Santa Clara, décembre 2023.

Qobly (France) a une stratégie consistant à créer en parallèle ses puces de qubits et d'électronique de contrôle basse température de type cryo-CMOS, co-développées avec le CEA/LIST. Les puces de qubits seront d'abord 1D, avant de passer au 2D. Trois phases de développement sont prévues: 100 qubits physiques d'ici 2026, 100 000 qubits physiques d'ici 2029 puis 1000 qubits logiques d'ici 2032.

Diraq (Australie) affiche l'objectif ambitieux de créer un ordinateur quantique avec un milliard de qubits physiques, en procédant par étape avec d'abord 9 puis 256 qubits. Elle envisage d'adopter la technique SiMOS voisine de celle de Quobly, mais explore en parallèle d'autres voies comme celle des qubits multiélectrons²²³, voire des qubits à donneur de spin exploitant des atomes d'antimoine (¹²³Sb)²²⁴. Elle a publié plusieurs avancées sur la fidélité de l'initialisation des qubits²²⁵, sur la variabilité de la fidélité des portes quantiques²²⁶, sur le *benchmarking*²²⁷, sur le contrôle des qubits^{228, 229, 230}, sur la lecture des qubits avec un amplificateur paramétrique^{231, 232} et sur une technique de suppression d'erreur²³³. En décembre 2022, elle affichait des fidélités de 99,96 % pour des portes à un qubit²³⁴ et de 98,92 % pour des portes à deux qubits, sur un nombre de qubits non précisé, donc très faible²³⁵.

-
- 223 [Electronic Correlations in Multielectron Silicon Quantum Dots](#) by Dylan H. Liang, MengKe Feng, Philip Y. Mai, Jesus D. Cifuentes, Andrew S. Dzurak, and Andre Saraiva, Diraq and UNSW, *arXiv*, July 2024 (6 pages).
- 224 [Creation and manipulation of Schrödinger cat states of a nuclear spin qubit in silicon](#) by Xi Yu, Andrew S. Dzurak, Andrea Morello *et al.*, Diraq *et al.*, *arXiv*, May 2024 (40 pages).
- 225 [Beating the Thermal Limit of Qubit Initialization with a Bayesian Maxwell's Demon](#) by Mark A. I. Johnson, Kohei M. Itoh, Andrew S. Dzurak, Andrea Morello *et al.*, *PRX*, October 2022 (15 pages).
- 226 [Bounds to electron spin qubit variability for scalable CMOS architectures](#) by Jesús D. Cifuentes, Andrew S. Dzurak *et al.*, March 2023 (20 pages).
- 227 [Stability of high-fidelity two-qubit operations in silicon](#) by Tuomo Tantt, Kohei M. Itoh, Robin Blume-Kohout, Andrea Morello, Andrew S. Dzurak, March 2023 (13 pages).
- 228 [On-demand electrical control of spin qubits](#) by Will Gilbert, Kohei M. Itoh, Andrea Morello, Andrew S. Dzurak *et al.*, *Nature Nanotechnology*, January 2023 (21 pages).
- 229 [Implementation of an advanced dressing protocol for global qubit control in silicon](#) by I. Hansen, Kohei M. Itoh, Andrew S. Dzurak *et al.*, *Applied Physics Reviews*, September 2022 (9 pages).
- 230 [Implementation of the SMART protocol for global qubit control in silicon](#) by Ingvild Hansen, Andrew S. Dzurak *et al.*, August-September 2021 (9 pages).
- 231 [Direct detection of spin resonance with a microwave parametric amplifier](#) by Wyatt Vine, Andrea Morello *et al.*, November 2022 (28 pages).
- 232 [Gate-based spin readout of hole quantum dots with site-dependent g-factors](#) by Angus Russell, Andrew S. Dzurak, Alessandro Rossi *et al.*, June 2022-April 2023 (16 pages).
- 233 [Real-time feedback protocols for optimizing fault-tolerant two-qubit gate fidelities in a silicon spin system](#) by Nard Dumoulin Stuyck, Andrew S. Dzurak *et al.*, September 2023 (6 pages).
- 234 [Diraq achieves record accuracy for device manufactured by existing semiconductor infrastructure](#) by Diraq, June 2024.
- 235 [High-fidelity spin qubit operation and algorithmic initialization above 1K](#) by Jonathan Y. Huang, Natalia Ares, Andrew S. Dzurak, Chih Hwan Yang *et al.*, *Nature*, August 2023-March 2024 (20 pages).

Equal 1 (Irlande-USA) planche sur la création d'une puce de qubits silicium-germanium qui comprendra à terme des millions de qubits, ainsi que l'électronique de contrôle associée, correction d'erreurs comprise. Son Quantum System-on-chip (QSoC) sera en pratique un composant intégrant d'un côté une puce pour les qubits^{236, 237} et, de l'autre, une puce cryo-CMOS pour le contrôle des qubits. Elle s'appuie pour l'instant sur la ligne de fabrication de recherche de TNO aux Pays-Bas pour les qubits et sur celle de GlobalFoundries à Dresde en Allemagne pour la puce cryo-CMOS. L'ordinateur quantique qui intégrera ce composant tient dans un format serveur 4U. Ses figures de mérite cible sont des fidélités de portes à deux qubits de 98 % et de portes à un qubit de 99 %, des portes durant 50 à 100 ns et un temps de lecture de 10 µs pouvant descendre ensuite à 500 ns.

SemiQon (Finlande) est installé dans les locaux de VTT à Espoo, près d'Helsinki. Elle vise la création d'une puce d'un million de qubits de spin intégrant l'électronique de contrôle cryo-CMOS des qubits²³⁸. Son prototype d'avril 2023 comprenait 48 qubits avec l'électronique de contrôle associée²³⁹.

Arque (Allemagne) a une *roadmap* comprenant 2-4, 50, 200, 10 000 puis 1 million de qubits de type ASGa puis SiGe. elle prévoit d'obtenir des fidélités de portes à deux qubits de 99,9 %^{240, 241}.

236 [A Single-Electron Injection Device for CMOS Charge Qubits Implemented in 22-nm FD-SOI](#) by Imran Bashir, Elena Blokhina *et al.*, 2020 (4 pages).

237 [Nanoscale single-electron box with a floating lead for quantum sensing: modelling and device characterization](#) by Nikolaos Petropoulos, Elena Blokhina *et al.*, *arXiv*, April 2024 (7 pages).

238 [Scalable on-chip multiplexing of silicon single and double quantum dots](#) by Heorhii Bohuslavskyi, Alberto Ronzani, Joel Häätinen, Arto Rantala, Andrey Shchepetov, Panu Koppinen, Mika Prunnila, and Janne S. Lehtinen, *arXiv*, August 2022-December 2023 (30 pages).

239 [SemiQon's quantum processor testing and measurement facilities at the VTT MIKES premises up and running](#), SemiQon, April 2024. The first tested chip has 4 qubits, but no specific gate set at this point.

240 [The SpinBus Architecture: Scaling Spin Qubits with Electron Shuttling](#) by Matthias Künne *et al.*, JARA and ARQUE, June 2023 (15 pages).

241 [Scalable Parity Architecture With a Shuttling-Based Spin Qubit Processor](#) by Florian Ginzl, Michael Fellner, Christian Ertler, Lars R. Schreiber, Hendrik Bluhm, and Wolfgang Lechner, *arXiv*, March 2024 (17 pages).

SQC (Australie) utilise la technique des atomes donneurs de spin, exploitant des atomes de phosphore implantés dans un substrat de silicium ^{28}Si ²⁴² et dont le noyau est couplé au spin de celui des cinq électrons de la couche de valence de l'atome qui n'est pas relié aux atomes de silicium avoisinants par des liaisons covalentes. Elle crée des portes à deux qubits avec deux atomes de phosphore éloignés de 17,5 nm²⁴³. Elle a obtenu en 2020 des fidélités de portes à un qubit de 99,99%²⁴⁴. En 2022, elle a présenté un processeur de 10 qubits en 1D. En 2024, elle exécutait un algorithme de Grover avec 4 qubits, organisés avec trois atomes de phosphore et un spin d'électron avec une fidélité de portes à deux qubits de 99%²⁴⁵. La société n'a pas publié de *roadmap* FTQC.

C12 (France) planche sur l'usage de nanotubes de carbone pour piéger en 1D des spins d'électrons. La technique présente l'intérêt de protéger les qubits des interférences extérieures et d'améliorer leur temps de cohérence. Les nanotubes de carbone sont réalisés avec du carbone ^{12}C à spin entier, n'interférant pas avec celui de l'électron piégé dedans. Ils sont intégrés sur un circuit en silicium avec des agrafeuses automatisées²⁴⁶. Les qubits sont reliés entre eux par des cavités micro-ondes. La société dispose de ses propres infrastructures à Paris pour la fabrication de ses nanotubes de carbone et pour le circuit en silicium les accueillant.

EeroQ (USA) développe un processeur piégeant des électrons sur un lit d'hélium superfluide au-dessus d'un circuit en silicium contenant

242 [Highly \$^{28}\text{Si}\$ enriched silicon by localised focused ion beam implantation](#) by Ravi Acharya, David N. Jamieson, Richard J. Curry *et al.*, University of Melbourne and University of Manchester, *Communications Materials*, May 2024 (7 pages) shows a ^{28}Si purification technique on a silicon substrate that is localized on the implanted phosphorus atom location.

243 [Measurement of enhanced spin-orbit coupling strength for donor-bound electron spins in silicon](#) by Radha Krishnan, Michelle Y. Simmons, Bent Weber *et al.*, NTU Singapore, UNSW, *arXiv*, April 2024 (8 pages).

244 [Exploiting a Single-Crystal Environment to Minimize the Charge Noise on Qubits in Silicon](#) by Ludwik Kranz, Michelle Simmons *et al.*, 2020 and [A two-qubit gate between phosphorus donor electrons in silicon](#) by Y. He, Michelle Simmons *et al.*, 2019.

245 [Grover's algorithm in a four-qubit silicon processor above the fault-tolerant threshold](#) by Ian Thorvaldson, Michelle Y. Simmons *et al.*, *arXiv*, April 2024 (16 pages).

246 [Nanoassembly technique of carbon nanotubes for hybrid circuit-QED](#) by Tino Cubaynes, Matthieu Desjardin, Audrey Cottet, Taki Kontos *et al.*, September 2021 (6 pages).

l'électronique de contrôle de l'ensemble²⁴⁷. L'idée vient de l'Université du Michigan et des Bell Labs en 1999^{248, 249, 250}. Elle a ensuite été développée entre 2003 et 2006 pour exploiter des spins d'électrons avec des circuits ressemblant aux pièges d'ions et exploitant des électrons navettes pour créer des portes à deux qubits²⁵¹. Sa première puce de test en 2023 supportait théoriquement 2432 qubits, le tout ne nécessitant que 30 lignes de contrôle. Les électrons survolent l'hélium superfluide à une altitude d'environ 10 nm. Ils sont contrôlés par des électrodes situées dans une puce CMOS. EeroQ prévoit d'obtenir des temps de cohérence de 10s, et des portes de deux qubits avec des fidélités de 99,9%²⁵². Le tout avec la capacité à atteindre 10 000 qubits par puce.

3.4.6. CONCLUSION

Les qubits de spin d'électrons présentent autant de promesses que de défis. Leur niveau de maturité est bien plus faible que celle des qubits supraconducteurs, à atomes froids et ions piégés. L'appui sur la filière de la microélectronique qui est souvent mise en avant par les acteurs de ce marché est un plus, mais pas suffisant. De nombreuses difficultés sont à surmonter, relevant de la physique quantique et des matériaux. Leur résolution, qui prendra certainement du temps, pourrait ouvrir des voies intéressantes en termes de montée en échelle.

247 [Electron-on-helium qubit](#) page sur Wikipedia.

248 [Quantum Computing with Electrons Floating on Liquid Helium](#) by P. M. Platzman and M. I. Dykman, Science, June 1999 (3 pages).

249 [Quantum computing using floating electrons on cryogenic substrates: Potential And Challenges](#) by Ash Jennings *et al.*, RIKEN, October 2023 (25 pages).

250 [Integrating superfluids with superconducting qubit systems](#) by Johannes Pollanen, Kater Murch *et al.*, Michigan State University, Washington University in Saint Louis, 2019 (11 pages).

251 [Spin-based quantum computing using electrons on liquid helium](#) by Steve Lyon, PRA, 2003–2006 (12 pages).

252 [Coulomb interaction-driven entanglement of electrons on helium](#) by Niyaz R. Beysengulov, Johannes Pollanen *et al.*, October 2023 (19 pages).

3.5. IONS PIÉGÉS

Les qubits à base d'ions piégés sont parmi les plus anciens qui soient, les premières expériences les concernant remontant au milieu des années 1990. La communauté scientifique du domaine est très large et couvre tous les continents, avec notamment les USA, l'Europe, Taïwan et la Chine. Les entreprises du secteur sont toutes des startups, telles que IonQ, Quantinuum pour les USA, mais aussi Universal Quantum et Oxford Ionics pour le Royaume-Uni, eleQtron pour l'Allemagne, AQT pour l'Autriche et Crystal Quantum Computing pour la France.

Les ions de ces ordinateurs quantiques sont piégés au-dessus de circuits électroniques qui contiennent des électrodes permettant leur positionnement précis grâce à des champs électriques, en complément de lasers qui ont servi à les refroidir initialement. Ils sont organisés en structures à une ou deux dimensions selon les cas. Les états $|0\rangle$ et $|1\rangle$ de ces ions correspondent à des niveaux d'énergie séparés par des fréquences qui vont conditionner leur mode de contrôle. Les plus courants sont les ions à structure hyperfine contrôlés par des micro-ondes de quelques GHz et des transitions à effet Raman à base de lasers²⁵³. Viennent ensuite les ions contrôlés par des fréquences optiques de quelques centaines de THz et enfin, plus rarement, les ions excités vers des états de Rydberg, par des lasers émettant dans le domaine ultraviolet.

Les ions sont choisis en fonction de leur configuration électronique et de leurs transitions énergétiques. Ce sont généralement des métaux alcalins du groupe 2 ou IIA du tableau de Mendeleïev avec le béryllium, le magnésium, le calcium, le strontium, le baryum ainsi que certaines terres rares comme l'ytterbium^{254, 255}. Certains systèmes exploitent deux éléments comme le calcium et le strontium, ou le baryum et l'ytterbium, l'un servant au refroidissement et l'autre aux qubits.

253 [Robust and resource-efficient microwave near-field entangling \$^9\text{Be}^+\$ gate](#) by G. Zarantonello, November 2019 (6 pages).

254 [Introduction to Trapped Ion Quantum Computing](#) by Gabriel Mintzer from MIT, February 2020.

255 [Ion-Based Quantum Computing Hardware: Performance and End-User Perspective](#) by Thomas Strohm, Sebastian Lubner *et al.*, Bosch, *arXiv*, May 2024 (44 pages).

Les ions procurent de longs temps de cohérence pouvant être de plusieurs dizaines de secondes, des portes quantiques ayant les meilleures fidélités connues, dépassant 99,9% pour des portes à deux qubits, ainsi qu'une meilleure connectivité entre qubits, des portes à deux qubits pouvant être créées entre n'importe quel qubit d'un ensemble d'ions. Leurs inconvénients principaux sont la lenteur de leurs portes et diverses difficultés de montée en échelle.

La stabilisation spatiale des ions est assurée par des pièges à ions. Ils sont de deux principaux types: les pièges de Penning qui utilisent un champ magnétique et un quadripôle électrique et les pièges de Paul qui exploitent un champ électrique oscillant. Le positionnement et le contrôle des ions associent couramment des courants continus et des champs micro-ondes. Des lasers complètent l'ensemble pour refroidir au préalable les ions par effet Doppler et par bande latérale (*sideband cooling*), pour limiter les effets phononiques de vibration des ions ainsi que pour la lecture par fluorescence de l'état des qubits. Les portes quantiques sont réalisées à partir de champs micro-ondes ou lasers selon les cas^{256, 257}.

Les pièges à ions les plus courants sont maintenant les QCCD (*Quantum Charge-Coupled Device*). Ils permettent de distribuer les ions et leurs champs de contrôle dans différentes zones en 1D et 2D²⁵⁸. Les zones sont reliées entre elles avec des ions qui circulent d'une zone à l'autre (*shuttling ions*)²⁵⁹. Les acteurs de ce marché s'appuient généralement sur des salles blanches commerciales comme celles de GlobalFoundries et d'Infineon. Ils utilisent ainsi le même argumentaire que les acteurs des qubits silicium: l'exploitation de salles blanches professionnelles de l'industrie de la microélectronique.

256 [Individually Addressed Quantum Gate Interactions Using Dynamical Decoupling](#) by M.C. Smith, A.D. Leu, M.F. Gely, and D.M. Lucas, *PRX Quantum*, August 2024 (9 pages).

257 [Quantum information processing with trapped ions](#) by Christian Roos, 2012 (53 slides).

258 [Architecture for a large-scale ion-trap quantum computer](#) by D. Kielpinski, C. Monroe, D. J. Wineland, *Nature*, June 2002 (3 pages).

259 [Multi-zone trapped-ion qubit control in an integrated photonics QCCD device](#) by Carmelo Mordini, Jonathan P. Home *et al.*, ETH Zurich, *arXiv*, January 2024 (13 pages).

trapped ions qubits key takeaways

| highlights | challenges |
|--|--|
| <ul style="list-style-type: none"> • first two-qubit gate fidelities reaching 99.9% (Quantinuum, Oxford Ionics). • first logical qubits above break-even. • high ratio between coherence time and gate time: supports deep algorithms in number of gate cycles. • low qubits variability given the ions are all the same. • entanglement possible between all qubits on 1D architecture which speeds up computing, avoiding SWAP gates. • requires some cryogeny at 4K to 10K. • QPU interconnect can directly use photon entangled resources. | <ul style="list-style-type: none"> • unproven scalability options beyond 60 qubits (ions shuttling, 2D architectures, photon interconnect, micro-Penning traps). • slow computing: due to long quantum gate times and ions shuttling which may be problematic for deep algorithms in a FTQC regime despite better qubit many-to-many connectivity at small scale. • two-qubit gate times increase with ion distance in some laser-driven 1D and 2D settings. • many-to-many connectivity demonstrated only at small scale. • control signals variability: microwave, lasers, etc. • ions heating phenomenon: it is not yet explained yet and really contained. |
| variations | path to scalability |
| <ul style="list-style-type: none"> • microwave/DC drive instead of laser drive. • connectivity: many-to-many within zones and ions shuttling between zones. • dual species like ytterbium + barium for computing and cooling. • Rydberg ion qubits for avoiding phonon and heating effect. • hybrid neutral atoms-ions platforms. | <ul style="list-style-type: none"> • 2D QCCD and ions shuttling. • QCCD tiling (Universal Quantum). • multi modules ion traps with intermodules ions shuttling. • multi-layer ion traps to enable long-range microwave based entanglement. • photonic interconnect to entangle qubits from different QPUs. |

Figure 16: Points forts, défis, variétés et options d'évolutivité des qubits à base d'ions piégés.

3.5.1. AVANCÉES

Les qubits à base d'ions piégés existent depuis près de trois décennies. Les pionniers en sont le NIST à Boulder, l'Université d'Innsbruck, puis celle de Maryland.

Les fidélités des portes quantiques à base d'ions piégés sont les meilleures de toutes les modalités de qubits. Elles atteignent 87% pour les portes à un qubit et 99,9% pour les portes à deux qubits, notamment chez Quantinuum et pour 20 qubits. Quantinuum a atteint en juin 2024 un record de 99,84% de fidélité pour les portes à deux qubits sur 56 qubits²⁶⁰. Cela permet d'exécuter des algorithmes NISQ relativement profonds en cycles de portes quantiques.

Les ions piégés sont les premiers avec lesquels des qubits logiques ont été créés au-dessus du seuil de rentabilité (*break-even*), à savoir avec des fidélités

260 [The computational power of random quantum circuits in arbitrary geometries](#) by Matthew DeCross, Marco Pistoia, et al., *arXiv*, June 2024 (36 pages).

de qubits logiques meilleures que celle des qubits physiques sous-jacents. C'est notamment le cas chez Quantinuum qui est le plus avancé de ce point de vue²⁶¹. Elle réalisait en 2024 la téléportation de qubits logiques avec une fidélité de 97%²⁶². Elle a créé trois qubits logiques avec une fidélité de portes à deux qubits de 99,91% sur son QPU H1-1 de 20 qubits et de 99,8% sur le H2-1 avec 32 qubits²⁶³.

Les ions ont un rapport élevé entre leur temps de cohérence et la durée des portes quantiques. Il est situé autour de 10^6 alors qu'il est plutôt de l'ordre de 10^3 pour les qubits supraconducteurs et de 200 pour les atomes froids. Cela permet aux ions de supporter des algorithmes de plus grande profondeur en nombre de cycles de porte, et ce, sans correction d'erreur, en régime NISQ.

Comme les atomes, les ions ont une faible variabilité. Celle-ci dépend essentiellement du circuit de contrôle.

Les ions piégés permettent la création de portes quantiques arbitraires entre paires de qubits, évitant les nombreuses portes SWAP qui sont nécessaires autrement comme dans les architectures de qubits où ceux-ci ne sont reliés qu'à leur proche voisin, comme les qubits supraconducteurs. Cette technique fonctionne cependant uniquement à petite échelle de quelques dizaines de qubits, comme chez IonQ (39) et Quantinuum (56). Par ailleurs, plus les qubits sont éloignés, plus les portes quantiques les reliant sont lentes et de mauvaise qualité. Au-delà, cette connectivité n'est rendue possible que par des « ions navette » qui sont déplacés d'un bloc de qubits à l'autre et permettent de relier ces blocs entre eux par des portes à deux qubits. La connectivité de pair-à-pair n'est donc pas généralisée à l'ensemble des ions d'un processeur.

261 [Benchmarking logical three-qubit quantum Fourier transform encoded in the Steane code on a trapped-ion quantum computer](#) by Karl Mayer, Russell Stutz *et al.*, Quantinuum, *arXiv*, April 2024 (13 pages).

262 [High-fidelity and Fault-tolerant Teleportation of a Logical Qubit using Transversal Gates and Lattice Surgery on a Trapped-ion Quantum Computer](#) by C. Ryan-Anderson, D. Hayes *et al.*, Quantinuum, *arXiv*, April 2024 (13 pages).

263 [Benchmarking logical three-qubit quantum Fourier transform encoded in the Steane code on a trapped-ion quantum computer](#) by Karl Mayer, Russell Stutz *et al.*, Quantinuum, *arXiv*, April 2024 (13 pages).

Les ions nécessitent une cryogénie à 4K qui est plus simple à mettre en œuvre que celle des qubits supraconducteurs à 15 mK. Comme pour les atomes neutres, ce refroidissement de la chambre à vide qui contient les ions permet d'améliorer la qualité de l'ultravide qui y règne et d'éviter les effets de photons thermiques.

Enfin, les ions présentent l'avantage d'être relativement faciles à intriquer avec des photons pour assurer l'interconnexion entre processeurs, une partie de leur contrôle reposant sur des photons dans le visible ou l'infrarouge, à base de lasers.

3.5.2. DÉFIS

Voici les défis à surmonter pour faire progresser ces qubits dans le cadre d'architectures à tolérance de pannes.

Les **options d'évolutivité** ne sont pas encore éprouvées au-delà d'une cinquantaine de qubits. Elles reposent toutes sur des circuits QCCD 2D intégrant des blocs d'ions avec des ions flottants d'un bloc à l'autre. Les « *blueprints* » pour ce faire existent depuis plus de deux décennies, mais n'ont toujours pas été mis en œuvre en pratique.

La **lenteur des portes quantiques** porte préjudice à la rapidité des calculs, surtout en régime de tolérance de pannes où les circuits sont profonds avec un grand nombre de cycles de portes quantiques. Elle est de l'ordre d'une à quelques centaines de microsecondes. Cette lenteur est accrue avec l'usage d'ions flottants qui sont déplacés physiquement d'un endroit à l'autre des circuits pour établir des intrications entre blocs de qubits. Les portes quantiques des ions piégés sont environ 1000 fois plus lentes que celle des qubits supraconducteurs. C'est un énorme handicap en vitesse de calcul qui n'est pas forcément compensé par la bonne connectivité entre qubits.

La **connectivité *many-to-many*** opère de manière limitée dans des blocs de qubits comprenant entre 4 et 12 qubits physiques. Dans certains types de circuits de contrôle à base de micro-ondes comme chez Oxford Ionics, la connectivité est limitée au voisin le plus proche et en 1D. Elle n'est donc pas meilleure qu'avec les qubits supraconducteurs.

La **durée des portes à deux qubits** augmente avec la distance entre les ions dans les circuits 1D et 2D et le contrôle d'ions par laser, comme chez IonQ.

Les **erreurs résiduelles** proviennent principalement des variations de tension ou d'intensité des circuits de contrôle des ions, des variations des fréquences des lasers de contrôle, des effets de diaphonie optique dans les circuits de contrôle^{264, 265}, des imprécisions des pinces optiques²⁶⁶, et enfin, de l'effet de réchauffement des ions qui reste encore partiellement inexpliqué. Les ions sont aussi sensibles aux variations de champ magnétique, créant des bruits de phase ainsi que de collisions entre ions et gaz résiduels.

3.5.3. VARIATIONS

Voici quelques-unes des variantes technologiques principales concernant les ordinateurs quantiques à base d'ions piégés.

Le **pilotage des qubits** peut se faire par lasers ou par micro-ondes, radiofréquences et courants continus. Le pilotage par laser est la solution historique retenue par exemple par IonQ. Elle fonctionne bien à petite échelle, permet un contrôle précis des ions, est adaptée aux transitions à haute énergie, ainsi qu'à la génération d'intrications à longue distance, mais elle est plus difficile à faire fonctionner à grande échelle. C'est la solution pour l'instant retenue par IonQ. La plupart des autres acteurs tels que Quantinuum, Universal Quantum ou Oxford Ionics préfèrent piloter leurs portes quantiques avec des micro-ondes²⁶⁷ ou des tensions continues qui sont dirigées vers les ions via les circuits QCCD. La solution permet de se passer d'une partie des circuits optiques nécessaires au pilotage par lasers,

264 [Low-Crosstalk, Silicon-Fabricated Optical Waveguides for Laser Delivery to Matter Qubits](#) by Clayton L. Craft, David Hucul *et al.*, AFRL, HRL Laboratories, *arXiv*, June 2024 (9 pages).

265 [Physical coherent cancellation of optical addressing crosstalk in a trapped-ion experiment](#) by Jeremy Flannery, Roland Matt, Luca Huber, Kaizhao Wang, Christopher Axline, Robin Oswald, and Jonathan P. Home, ETH Zurich, *arXiv*, June 2024 (11 pages).

266 [Alignment and Optimisation of Optical Tweezers on Trapped Ions](#) by M. Mazzanti, R. X. Schüssler *et al.*, QuSoft, *arXiv*, June 2024 (8 pages).

267 [Robust and fast microwave-driven quantum logic for trapped-ion qubits](#) by M. A. Weber, D. M. Lucas *et al.*, University of Oxford, *arXiv*, February 2024 (6 pages).

ceux-ci restant cantonnés aux fonctions de refroidissement des ions et de lecture de leur état. L'adressage des ions est plus facile à grande échelle et consomme moins d'énergie.

La **connectivité entre qubits** pour l'exécution de portes à deux qubits varie d'une technologie à l'autre. Le pilotage des portes par lasers et micro-ondes permet généralement de construire des portes à deux qubits arbitraires entre toutes les paires de qubits d'un processeur. En pratique, cette connectivité est limitée à des grappes d'ions allant de quelques-uns à une cinquantaine. Au-delà, la connectivité entre grappes est prévue avec des ions navettes qui se déplacent d'une grappe à l'autre pour établir des relations d'intrication entre une grappe d'ions et une grappe adjacente. Ces grappes peuvent être organisées en une dimension (IonQ) ou en deux dimensions sur des rails orthogonaux (Quantinuum). La connectivité arbitraire entre ions est donc locale à ces grappes et non pas globale à l'ensemble d'un ordinateur gérant plusieurs grappes d'ions.

L'**usage de deux éléments** comme l'ytterbium et le baryum, le premier pour le calcul et le second pour le refroidissement. C'est la technique utilisée par Quantinuum. IonQ est de son côté en train de migrer de l'ytterbium au baryum, car celui-ci est pilotable avec des photons dans la bande télécom de 1550 nm ce qui facilite l'interconnexion photonique entre processeurs quantiques.

L'**usage d'ions en états de Rydberg** pour éviter l'usage des phonons et les effets de réchauffement des ions. C'est la technique adoptée par la startup française Crystal Quantum Computing. Le prix à payer est l'absence de connectivité *many-to-many*, les états de Rydberg ne permettant de relier les ions qu'à leurs voisins immédiats. Sauf à les déplacer, comme le fait QuEra.

Des **plates-formes hybrides d'atomes neutres et d'ions** qui sont à l'état de recherche en Allemagne²⁶⁸.

268 [Emulating Solid-State Physics with a Hybrid System of Ultracold Ions and Atoms](#) by U. Bissbort, R. Gerritsma *et al.*, PRL, August 2013 (8 pages)

3.5.4. CHEMINS VERS L'ÉVOLUTIVITÉ

Voici les voies technologiques retenues par les différents acteurs du marché pour monter en échelle avec les ions piégés.

Les **circuits QCCD 2D et ions navettes** sont la première voie envisagée pour monter en échelle en nombre de qubits physiques^{269, 270}.

Les **ordinateurs multimodules** avec le transfert d'ions entre modules. C'est l'approche retenue par Universal Quantum. Ce transfert se ferait avec une très grande fidélité²⁷¹. Cela nécessite des techniques de compilation optimisées de code quantique²⁷².

Les **pièges à ions multicouches** pour permettre l'intrication à longue portée par micro-ondes. Les difficultés à surmonter sont voisines de la conception de circuits supraconducteurs. Une solution envisagée, réduisant les effets de réchauffement, consiste à utiliser des circuits supraconducteurs pour la délivrance des micro-ondes de pilotage des qubits, comme RIKEN l'étudie au Japon²⁷³.

269 [Blueprint for a microwave trapped ion quantum computer](#) by Bjoern Lekitsch *et al.*, *Science Advances*, February 2017 (11 pages). See also [A Shuttle-Efficient Qubit Mapper for Trapped Ion Quantum Computers](#) by Suryansh Upadhyay *et al.*, April 2022 (7 pages).

270 [High-Fidelity Transport of Trapped-Ion Qubits in a Multi-Layer Array](#) by Deviprasath Palani, Tobias Schaetz *et al.*, University of Freiburg, May 2023 (8 pages).

271 [TITAN: À Distributed Large-Scale Trapped-Ion NISQ Computer](#) by Cheng Chu *et al.*, Lawrence Berkeley National Laboratory, *arXiv*, February 2024 (6 pages) transporte des ions d'un circuit QCCD à l'autre en 0,4 ms et avec une fidélité de 99,999 993 %. Il exploite des ions ytterbium ¹⁷¹Yb+ pour le calcul et baryum ¹³⁸Ba+ pour les transferts.

272 [Shuttling for Scalable Trapped-Ion Quantum Computers](#) by Daniel Schoenberger, Stefan Hillmich, Matthias Brandl, and Robert Wille, Infineon, *arXiv*, February 2024 (7 pages).

273 [Superconducting surface trap chips for microwave-driven trapped ions](#) by Yuta Tsuchimoto *et al.*, University of Tokyo, RIKEN, Inamori Research Institute for Science, *arXiv*, July 2024 (27 pages).

L'interconnexion photonique pour intriquer les qubits de différents QPU. C'est la stratégie d'IonQ^{274, 275}. Des liens allant jusqu'à 400 mètres ont été testés à l'Université d'Innsbruck en Autriche, avec des ions calcium séparés de 230 mètres par une fibre de 520 m de long, pouvant être étendue à 50 km^{276, 277}. Il reste encore de gros travaux de recherche pour y arriver, du fait du taux de succès encore faible de la création de ces liaisons photoniques intriquées, avec des paires de Bell obtenues à un taux d'erreur très faible de $2,18 \times 10^{-4}$ ^{278, 279}.

3.5.5. FEUILLES DE ROUTE

Les acteurs du marché des ions piégés ont presque tous communiqué leur feuille de route allant vers les ordinateurs quantiques à tolérance de pannes. En général, ils prévoient une transition continue du régime NISQ vers le régime FTQC du fait d'ions qui ont de bonnes fidélités et permettent d'envisager d'exploiter la mitigation d'erreurs dans des régimes plus développés que dans les autres modalités de qubits.

IonQ a publié sa *roadmap* en 2020. Elle a aussi adopté un *benchmark* maison de « qubits algorithmiques » (AQ = *Algorithmic Qubits*), utilisant le \log_2 du volume quantique d'IBM et en s'appuyant sur un ensemble de *benchmarks* applicatifs de niveau intermédiaire du consortium QED-C²⁸⁰. Elle a atteint successivement un niveau de 22 qubits algorithmiques en 2022, puis 29 et 35 en 2023²⁸¹. Elle prévoit ensuite d'atteindre 64 AQ en 2025 en exploitant des

274 [Large Scale Modular Quantum Computer Architecture with Atomic Memory and Photonic Interconnects](#) by Christopher Monroe *et al.*, 2014 (16 pages).

275 [Integrated photonic structures for photon-mediated entanglement of trapped ions](#) by F. W. Knollmann *et al.*, MIT and Sandia National Laboratories, *arXiv*, January 2024 (17 pages).

276 [Entanglement of Trapped-Ion Qubits Separated by 230 Meters](#) by V. Krutyanskiy, Maria Galli, Nicolas Sangouard, Tracy Northup *et al.*, PRL, February 2023 (22 pages).

277 [Atom-photon coupling with trapped ions](#) by Tracy Northup, 2022 (40 slides).

278 [High-Rate, High-Fidelity Entanglement of Qubits Across an Elementary Quantum Network](#) by L. J. Stephenson *et al.*, University of Oxford, PRL, 2020 (6 pages).

279 [Ion Trap with In-Vacuum High Numerical Aperture Imaging for a Dual-Species Modular Quantum Computer](#) by Allison L. Carter, Christopher Monroe *et al.*, UMD, October 2023 (8 pages).

280 Quantum Economic Development Consortium - <https://quantumconsortium.org/>

281 [How We Achieved Our 2024 Performance Target of #AQ 35](#) by IonQ, January 2024.

qubits logiques à 16 qubits physiques, puis 256 et 1024 entre 2026 et 2028. Ceci ne sera possible qu'en interconnectant des processeurs quantiques de 64 ions avec des photons^{282, 283, 284, 285}. Cela a amené la société à faire en 2023 l'acquisition de la startup canadienne Entangled Networks qui est spécialisée dans le domaine.

Quantinuum a une *roadmap* qui a démarré en 2020 avec des circuits 1D (H1), puis est passée en 2023 aux circuits « *racetrack* » H2 (à l'image d'hippodromes), supportant 56 qubits. Au-delà, la société prévoit de passer par un circuit avec un croisement (Helios) avec 96 qubits, puis à des circuits 2D en rails orthogonaux et à base d'ions navettes passant de bloc en bloc de qubits pour les relier par des portes à deux qubits²⁸⁶. Elle ne communique cependant pas avec précision sur le nombre de qubits physiques et logiques qu'elle envisage d'atteindre avec ses QPUs H3, H4 et H5²⁸⁷. La société a mis à jour sa *roadmap* avec quelques détails chiffrés supplémentaires en septembre 2024. Elle prévoit d'assembler plusieurs milliers de qubits physiques et des centaines de qubits logiques d'ici 2030 avec des taux d'erreurs logiques de 10^{-16} . Deux questions restent en suspens dans sa *roadmap*: ses circuits QCCD en deux dimensions à partir de 2027 permettront-ils de mettre en œuvre des portes quantiques entre tous les qubits du système ou seulement par grappes locales et comment vont-ils supporter un jeu de portes universelles ?

De son côté, **AQT** (Autriche) prévoit aussi de mettre en place une architecture FTQC. Elle a réalisé sa première porte logique CNOT en mai 2022 avec 16 qubits physiques et en exploitant un code de correction de type code de

282 [Scaling the ion trap quantum processor](#) by Christopher Monroe and J. Kim, *Science*, 2013 (7 pages).

283 [Large-scale modular quantum-computer architecture with atomic memory and photonic interconnects](#) by Christopher Monroe, Robert Raussendorf *et al.*, *PRA*, 2013 (16 pages).

284 [IonQ Achieves Critical First Step Towards Developing Future Quantum Networks](#) by IonQ, February 2024.

285 [Enabling Networked Quantum Computing with Ion-Photon Entanglement](#) by IonQ, February 2024.

286 [Transport of multispecies ion crystals through a junction in an RF Paul trap](#) by William Cody Burton *et al.*, June 2022 (6 pages) where they describe how they can transport ytterbium and barium in 2D structures.

287 [Scalable Multispecies Ion Transport in a Grid Based Surface-Electrode Trap](#) by Robert D. Delaney *et al.*, Quantinuum, *arXiv*, March 2024 (11 pages).

couleur de 7 qubits. Elle a aussi réalisé une porte-T à tolérance de panne à l'aide de 16 qubits²⁸⁸. En 2023, elle publiait un *blueprint* pour mettre en œuvre une architecture FTQC²⁸⁹.

Au Royaume-Uni, **Universal Quantum** planche sur l'interconnexion de plusieurs modules de contrôle d'ions piégés de type QCCD avec des ions ytterbium exploités au niveau hyperfin de l'orbitale 2S²⁹⁰. La mesure non destructive des qubits s'appuie sur des ions auxiliaires de type baryum. En 2022, elle a annoncé vouloir atteindre un million de qubits grâce à son approche modulaire²⁹¹ (figure 17). Ses modules conduisent bien la chaleur, ce qui leur permet de l'évacuer efficacement. En juillet 2024, elle a annoncé la création d'une puce ASIC supportant sa plateforme d'interconnexion UQConnect²⁹². Elle supporte le transfert d'ions entre modules avec une fidélité de 99,999 993 %. Le tout opère à 70 K.

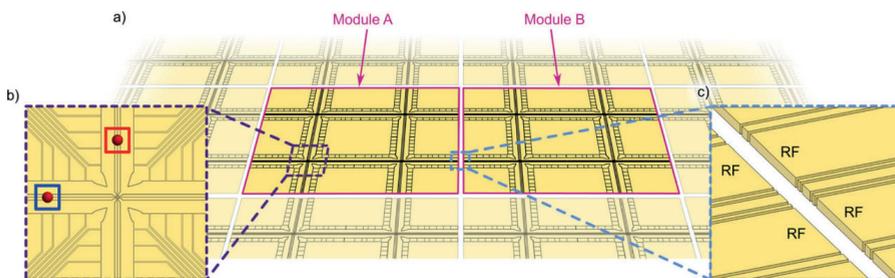


Figure 17: L'approche d'Universal Quantum pour interconnecter des modules de piégeage d'ions, les ions pouvant se déplacer d'un module à l'autre. Chaque module a une taille de 20 mm dans leur première génération. Source: [A high-fidelity quantum matter-link between ion-trap microchip modules](#) par M. Akhtar, W. K. Hensinger *et al.*, Nature Communications, février 2023.

288 [Demonstration of fault-tolerant universal quantum gate operations](#) by Lukas Postler, Rainer Blatt, Thomas Monz *et al.*, *Nature*, November 2021 and May 2022 (14 pages).

289 [Strategies for practical advantage of fault-tolerant circuit design in noisy trapped-ion quantum computers](#) by Sascha Heußen *et al.*, January 2023 (36 pages).

290 [Microfabricated Ion Traps](#) by Winfried Hensinger *et al.*, 2011 (28 pages).

291 [How Universal Quantum is rising to the million-qubit challenge](#), Universal Quantum, February 2022.

292 [Universal Quantum develops key enabler of million-qubit quantum computer](#) by Universal Quantum, July 2024.

Oxford Ionics s'appuie sur le principe WISE (*Wiring using Integrated Switching Electronics*), un module supportant jusqu'à 1000 ions dans un arrangement en matrice 2D (figure 18). Les puces sont optimisées pour le routage des signaux de contrôle des qubits. En juillet 2024, la société publiait ses premiers résultats exploitant un contrôle des qubits avec de simples électrodes et tensions²⁹³. Elle a obtenu des portes à deux qubits avec des fidélités de 99,97%, mais à petite échelle, sur 10 ions et 7 zones de 2 ions. Ses puces sont fabriquées par Infineon en Allemagne. Elle ambitionne d'ici quelques années d'atteindre 256 qubits avec cette technologie²⁹⁴.

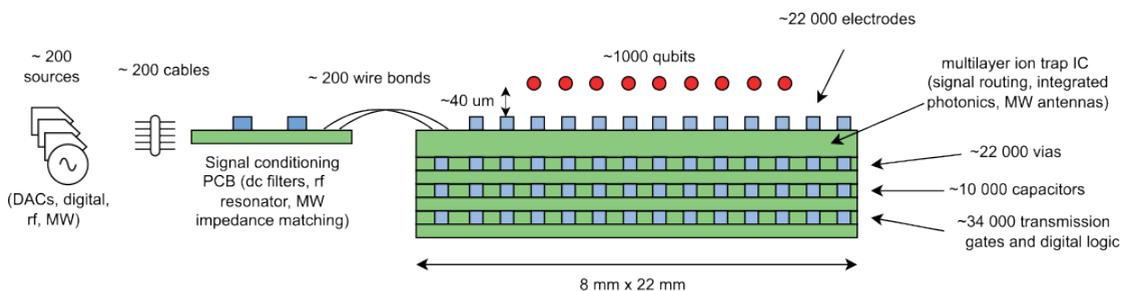


Figure 18 : schéma de câblage multicouche de la puce de contrôle des ions d'Oxford Ionics pouvant aller jusqu'à supporter 1000 qubits. La puce comprend des capacités et des circuits de routage, alimentés par 200 fils, et sur une surface de 8 mm x 22 mm. Source : [How to wire a 1000-qubit trapped ion quantum computer](#) par M. Malinowski *et al.*, Oxford Ionics, *PRX Quantum*, October 2023.

En France, **Crystal Quantum Computing** ambitionne de créer un ordinateur quantique à base d'ions strontium avec des ions excités dans des états de Rydberg. Leur contrôle nécessite des lasers UV opérants à 243 nm, à partir de lasers infrarouges suivis d'un doublement de fréquence et d'antennes micro-ondes THz directives²⁹⁵. Elle n'a pas encore démontré ces qubits ni publié de *roadmap* FTQC.

293 [Scalable, high-fidelity all-electronic control of trapped-ion qubits](#) by C. M. Löschnauer, C. J. Ballance, C. Matthiesen, M. Malinowski, T. P. Harty *et al.*, *arXiv*, July 2024 (12 pages).

294 [Oxford Ionics breaks global quantum performance records](#) by Oxford Ionics, July 2024.

295 [A microwave dressed Rydberg ion](#) by Fabian Pokorny, Stockholm University, 2020 (146 pages).

3.5.6. CONCLUSION

Les ions piégés présentent de beaux potentiels avec les meilleures fidélités actuellement disponibles. Ils permettent d'envisager la création d'ordinateurs à tolérance de pannes avec des ratios de qubits physiques par qubits logiques raisonnables. Leur montée en échelle doit relever plusieurs défis de taille: la capacité à contrôler le placement et le mouvement d'ions en 2D sur des puces interconnectées, d'interconnecter ensuite ces puces avec des ressources de photons intriqués ou de *ion shuttling* et enfin, de contourner d'une manière ou d'une autre la lenteur de leurs portes quantiques.

Chapitre 4

LE PASSAGE À L'ÉCHELLE DES CALCULATEURS QUANTIQUES

Au cours des trois décennies passées, on peut distinguer trois phases concernant les démonstrations expérimentales pour le calcul quantique. Dans un premier temps, des groupes de recherche travaillant sur différentes technologies ont démontré que l'on pouvait réaliser et contrôler un, puis quelques qubits, avec une fidélité croissante. Ensuite, lorsqu'il a été possible de contrôler plus de 50 qubits, même de manière imparfaite, des démonstrations d'avantage quantique calculatoire ont été réalisées : il s'agit de tâches d'échantillonnage (de bosons ou de circuits) difficiles à réaliser pour un supercalculateur classique, mais faciles pour un processeur quantique, même petit et non universel^{296, 297, 298, 299, 300}. Enfin, à partir de 2023, quelques laboratoires ont réussi à contrôler plusieurs centaines de qubits de manière suffisamment précise pour réaliser un qubit logique (voir chapitre 2). La prochaine étape consistera à proposer une architecture de calcul permettant le passage à l'échelle au-delà de 1000 qubits et à en réaliser les briques élémentaires. Pour passer à l'échelle et contrôler des millions de qubits, il sera indispensable de combiner des modules de taille physique plus

296 F. Arute *et al.* "Quantum supremacy using a programmable superconducting processor", *Nature* **574**, 505–510 (2019)

297 H.-S. Zhong *et al.* "Quantum computational advantage using photons", *Science* **370**, 1460–1463 (2020)

298 Y. Wu *et al.* "Strong Quantum Computational Advantage Using a Superconducting Quantum Processor", *Physical Review Letters* **127**, 180501 (2021)

299 L.S. Madsen *et al.* "Quantum computational advantage with a programmable photonic processor", *Nature* **606**, 75–81 (2022)

300 La comparaison précise de la performance pour réaliser ces tâches d'échantillonnage, lorsqu'on prend en compte le bruit, entre un calculateur classique et un calculateur quantique, est l'objet de discussions régulières, au gré des progrès en informatique classique et quantique, que nous ne reprenons pas ici, car elles ne rentrent pas dans le cadre de ce rapport.

modeste, interconnectés par des liens quantiques, comme nous l'expliquons dans ce chapitre.

4.1. LA SCALABILITÉ PAR LA MODULARITÉ

4.1.1. LIMITE À L'INTÉGRATION MONOLITHIQUE

Un ordinateur quantique tolérant aux fautes capables d'exécuter des algorithmes utiles, notamment dans les cas d'usage de simulation chimique, nécessitera des millions de qubits physiques. Or, les processeurs quantiques actuels ne peuvent pas croître tels quels jusqu'à atteindre ce nombre. En effet, d'une part, certaines de leurs propriétés physiques dépendent de leur taille et se dégradent lorsqu'on ajoute des qubits. Par exemple, la diaphonie (*crosstalk*) entre des qubits correspond à l'apparition d'un signal parasite dans le composant correspondant à un qubit causé par un signal appliqué à un composant d'un autre qubit, et peut causer des erreurs corrélées sur plusieurs qubits. Lorsque la diaphonie augmente avec la taille du système, ce qui peut être le cas pour les qubits supraconducteurs ou les atomes neutres, le taux d'erreur augmente à son tour, et il devient impossible de rester sous le seuil de la correction d'erreur. Pour les qubits supraconducteurs, un deuxième exemple est l'impact de rayons cosmiques, qui peut causer une erreur catastrophique détruisant la cohérence à l'échelle de la puce entière, et dont la probabilité augmente avec la taille de la puce. Les pertes photoniques constituent un troisième exemple: les processeurs quantiques photoniques souffrent des pertes de photon, et si la manipulation d'un nombre croissant de qubits photoniques passe par l'utilisation d'un interféromètre de profondeur croissante, le taux de pertes par photon augmentera avec le nombre de qubits. Par ailleurs, certaines contraintes de fabrication existent pour les circuits, notamment supraconducteurs, dont les qubits occupent une place importante, de l'ordre d'un quart de millimètre carré par qubit, et un peu plus pour des qubits de chats, notamment du fait de la taille du résonateur utilisé pour la lecture de leur état. La taille des puces est limitée par les systèmes de lithographie et celle des *wafers* utilisés, en général de 8 pouces. Ces contraintes pourraient être en partie levées dans le futur avec l'usage de techniques de fabrication sur des *wafers* des 12 pouces (300 mm) et grâce à la réduction de la taille des résonateurs.

D'autre part, ces processeurs comptent un certain nombre de composants proportionnels au nombre de qubits, qu'il serait physiquement impossible de multiplier par plusieurs millions. Il peut s'agir du câblage lié à l'électronique de contrôle et à la connexion entre les qubits, de la cryogénie, ou de la taille des qubits, qui, lorsque le facteur d'encombrement est trop important, rend impossible l'intégration monolithique de millions de qubits (voir chapitre 3 pour le détail des propriétés physiques limitant le passage à l'échelle par technologie de qubit).

Il existe des voies d'amélioration matérielle qui permettront d'intégrer plus de qubits malgré ces facteurs limitants, comme l'électronique intégrée de type cryo-CMOS classique ou supraconductrice (SFQ ou SQUID) et le multiplexage des signaux de contrôle. Les circuits cryo-CMOS semblent être viables pour piloter des qubits silicium qui fonctionnent à des températures situées entre 100 mK et 1K, là où le budget de cryogénie est le plus important. Il est plus difficile de les utiliser à proximité des puces supraconductrices qui opèrent à 15 mK. Dans ce cas, la solution envisagée est l'électronique supraconductrice, qui fonctionne avec une très faible déperdition d'énergie compatible avec la charge que le cryostat peut supporter à cette température. Ces circuits envoient cependant des signaux différents à base de pulsations, et génèrent des effets parasites sur les qubits (*back action*). La technique est notamment poussée par la startup américaine SeeQC.

Il se pose toutefois toujours la question du câblage. Chaque qubit supraconducteur nécessite de 2 à 5 lignes de contrôle selon les cas. Cela fait autant de lignes à créer entre la puce du processeur et son environnement de pilotage, y compris dans le cas d'une puce supraconductrice avoisinante. À moins d'utiliser des solutions de multiplexage/démultiplexage intégrées dans ces puces, il subsistera une difficulté de câblage bloquante pour augmenter le nombre de qubits par puce. C'est encore plus délicat dans le cas où les signaux de contrôle sont créés à température ambiante. Ils requièrent l'usage de câbles souples et coaxiaux qui sont reliés à la puce. Aujourd'hui, on ne sait pas produire de câbles souples supraconducteurs donc à faible dissipation thermique et ceux-ci ne sont donc généralement installés que dans les niveaux supérieurs à 4K dans les cryostats, là où le budget de refroidissement est plus important qu'à 15 mK. En dessous, il faut toujours utiliser des câbles coaxiaux.

Il existe en outre des méthodes logicielles, dites de tricotage de circuits (*circuit knitting*)³⁰¹ qui permettent de tirer parti de plusieurs circuits quantiques séparés pour simuler un seul circuit quantique plus grand, et dépasser ainsi la taille maximale des processeurs actuels au prix d'un surcoût en calcul classique. Bien qu'intéressantes pour aller au-delà de la capacité des processeurs actuels et exécuter des algorithmes NISQ sur des instances plus grandes, ces techniques ne sont pas *scalables*, car le surcoût en simulation est, dans le cas général, exponentiel.

4.1.2. LIEN ENTRE LA CONNECTIVITÉ DES QUBITS PHYSIQUES ET LA CORRECTION D'ERREURS

Pour qu'une architecture de calcul soit *scalable* en toute généralité, et ainsi compatible avec les techniques de correction d'erreur et de tolérance aux fautes, il faut qu'elle consiste en un assemblage de modules dont les caractéristiques sont constantes, indépendamment du nombre de modules assemblés. Ainsi, et seulement ainsi, le principe de base de la correction d'erreur, qui consiste à ajouter des qubits physiques pour réduire l'erreur logique autant que nécessaire lorsque les taux d'erreur physique se trouvent sous le seuil, peut s'appliquer.

Ces caractéristiques sont liées à la technologie de qubit considérée, ainsi qu'à l'architecture qui dicte comment ces qubits sont exploités ensemble. Un élément clef est la connectivité requise entre les qubits physiques pour réaliser un qubit logique à l'aide d'un code correcteur donné. À ce titre, le code de surface (voir chapitre 2) est un outil précieux, car il repose sur une connectivité 2D entre plus proches voisins : chaque qubit est placé sur une grille en deux dimensions et ne doit être connecté qu'à ses 4 plus proches voisins, quelle que soit la taille du code considéré, c'est-à-dire, quel que soit le nombre de qubits physiques utilisés. Ce type de code local ne peut cependant pas atteindre les performances des meilleurs codes en termes de surcoût en qubits physiques et de distance, et il est intéressant de considérer des interactions non locales. Dans ce cas, pour que l'architecture soit *scalable*,

301 C. Piveteau, D. Sutter. "Circuit Knitting With Classical Communication", IEEE Transactions on Information Theory, 70 (4) 2734-2745 (2024)],

il faut que le nombre de connexions entre les qubits soit borné, pour éviter que la connectivité n'explode avec le nombre de qubits. Cela correspond à la famille des codes de parité à faible densité, dits LDPC (*low-density parity check*).

4.1.3. COUPLAGE DE QPU PAR OPÉRATION ENTRE QUBITS DISTANTS

Pour dépasser les limites de l'intégration monolithique, il faut donc non seulement assembler des modules dont les propriétés physiques se comportent bien lors du passage à l'échelle, mais il faut également assurer une interconnexion quantique entre ces modules qui soit compatible avec les codes correcteurs et les protocoles de calcul tolérant aux fautes considérés. En effet, de seuls échanges d'information classique entre les processeurs ne permettent pas d'exécuter un calcul quantique général tolérant aux fautes sur l'ensemble de qubits logiques que comptent ces processeurs. Dit autrement, deux processeurs quantiques comptant chacun N qubits et liés par des communications classiques ne constituent pas un processeur quantique de $2N$ qubits.

Une première possibilité est basée sur la téléportation quantique, qui consiste à utiliser l'intrication pour transférer un état ou pour réaliser une porte sur des qubits distants.

On peut distribuer les qubits A et B d'une paire de Bell

$$|\Psi_{AB}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

à chacun des deux processeurs, puis implémenter des portes CNOT locales, puis mesurer les qubits distribués, réalisant ainsi, après correction par des portes à un qubit, une porte CNOT sur les qubits distants³⁰². Le circuit correspondant est donné en (figure 19).

³⁰² Nous donnons l'exemple de la porte CNOT, car celle-ci additionnée de quelques portes à un qubit constituent un ensemble de portes quantiques universel.

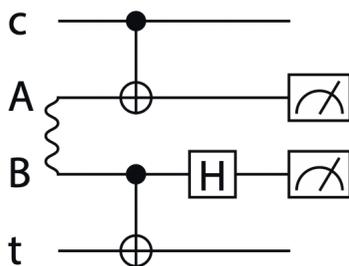


Figure 19 : Téléportation d'une porte CNOT. Une porte CNOT est implémentée entre deux qubits distants c et t à l'aide d'une paire de Bell sur les qubits A et B (représentée par une ligne ondulée), dont le qubit A (resp. B) est distribué à proximité du qubit c (resp. t). Des portes CNOT sont ensuite appliquées localement sur les qubits A et c, d'une part, et B et t, d'autre part. Les qubits A et B sont ensuite mesurés. Par simplicité, les corrections locales sont omises.

Une variante consiste à créer, pour chacun des deux qubits sur lesquels on souhaite réaliser l'opération, un qubit additionnel intriqué avec le qubit initial, puis à réunir ces deux qubits additionnels afin de réaliser une mesure d'état de Bell sur ceux-ci. À nouveau, à des corrections à un qubit près, cela est équivalent à appliquer une porte CNOT entre les qubits distants. Cela est possible, par exemple, lorsque les qubits sont encodés dans un degré de liberté d'un émetteur de photons uniques, ou lorsqu'une transduction permet de convertir les qubits servant au calcul en information encodée sur des photons.

Une deuxième possibilité pour réaliser des portes à deux qubits entre deux modules différents, lorsque les qubits servant au calcul sont mobiles, consiste à déplacer les qubits de chacun des deux modules, pour les placer dans une zone où on les fait interagir directement. Cette approche est, par exemple, compatible avec des processeurs à base d'atomes neutres³⁰³, ainsi qu'avec les ions piégés, en utilisant la technique de « *ion shuttling* ». Elle est notamment promue par la startup britannique Universal Quantum qui a démontré en 2024 une grande efficacité de cette technique pour déplacer un ion d'une puce de contrôle à une autre.

303 Q. Xu *et al.* "Constant-overhead fault-tolerant quantum computation with reconfigurable atom arrays", *Nature Physics* (2024)

Une troisième approche consiste à utiliser un bus quantique basé sur un résonateur micro-onde. Les deux qubits distants sur lesquels l'opération doit être réalisée sont couplés avec le bus, et la porte quantique entre les deux qubits est réalisée de manière globale grâce à cette interaction avec le bus. Cette méthode est particulièrement adaptée aux qubits supraconducteurs.

4.1.4. OPÉRATIONS LOGIQUES INTER-QPU

Afin de pouvoir implémenter le circuit correcteur d'erreur et les protocoles de tolérance aux fautes choisis, l'architecture proposée doit permettre d'exécuter ce type de primitive entre un certain nombre de qubits physiques. L'orchestration précise des opérations logiques entre les modules en un ensemble d'interactions entre qubits physiques intra- et intermodules est déterminée par l'architecture, le code correcteur et le protocole de tolérance aux fautes considéré. Par exemple, si l'on envisage d'encoder les qubits logiques à l'aide d'un code de surface et de réaliser les opérations logiques par des techniques de chirurgie de maille (*lattice surgery*)³⁰⁴ qui permettent d'implémenter de manière efficace un ensemble universel de portes sur des codes topologiques 2D en préservant la connectivité locale, il faudra pouvoir réaliser des portes à 2 qubits entre tous les qubits situés à la frontière de chacune des grilles correspondant aux qubits logiques. Cela est illustré avec l'exemple d'une porte CNOT entre deux qubits logiques en figure 20³⁰⁵.

304 D. Horsman *et al.* "Surface code quantum computing by lattice surgery", *New Journal of Physics* 14 123011 (2012)

305 D'autres techniques permettent de réaliser une porte CNOT logique en préservant la connectivité réduite aux plus proches voisins, comme celle dite du tissage (*braiding*) ou celle de la déformation de nœuds (*twist deformation*). Nous ne les détaillons pas ici, l'idée n'étant pas de passer en revue les façons de réaliser des portes sur des qubits encodés, mais de montrer comment elles sont compatibles avec l'assemblage modulaire nécessaire pour le passage à l'échelle.

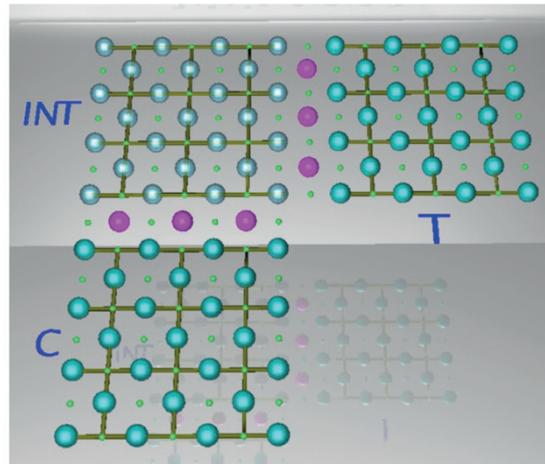


Figure 20: Réalisation d'une porte CNOT logique par chirurgie de maille (in D. Horsman *et al.* 2012 *New J. Phys.* 14 123 011, CC BY-NC-SA 3.0). Les qubits physiques correspondent aux grands cercles, et chacune des trois grilles est un qubit logique encodé par le code de surface. Ces trois qubits peuvent correspondre à trois modules physiques distincts. Pour réaliser une porte CNOT entre les qubits C et T à l'aide du qubit intermédiaire INT, il suffit de pouvoir réaliser des portes CNOT entre les qubits situés à la frontière des grilles et une ligne de qubits physiques intermédiaires, en rose.

Lorsqu'elles ne sont pas limitées à une connectivité entre plus proches voisins, d'autres architectures peuvent permettre de réaliser une porte logique à deux qubits de manière transversale: la porte logique est implémentée en exécutant la même porte entre tous les qubits physiques composant les deux qubits logiques, voir figure 21. Pour cela, il faut pouvoir déplacer les qubits afin de les faire interagir deux à deux. À nouveau, cette approche est donc compatible avec les plateformes de qubits mobiles, tels que les atomes neutres ou les photons³⁰⁶.

306 Il est en revanche impossible de réaliser toutes les portes d'un ensemble de portes universel de manière transversale (théorème d'Eastin-Knill). La manière la plus répandue d'atteindre l'universalité est alors la distillation et l'injection d'état magique.

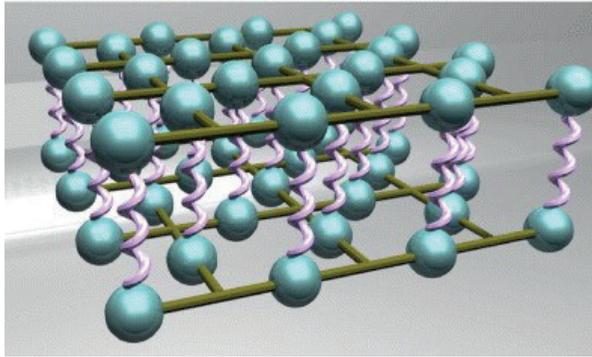


Figure 21: Réalisation d'une porte CNOT logique transversale (in D. Horsman *et al.* 2012 New J. Phys. 14 123 011, CC BY-NC-SA 3.0). Les deux grilles correspondent aux deux qubits logiques encodés à l'aide du code de surface. La porte logique est réalisée en implémentant une porte CNOT physique entre chaque qubit physique (lignes roses).

4.2. INTERCONNEXION PHOTONIQUE

Les efforts dans le domaine du calcul quantique ces dernières années se sont naturellement focalisés sur le développement des processeurs quantiques (QPU, pour *Quantum Processing Unit*) de taille de plus en plus grande afin de permettre l'exécution d'algorithmes démontrant un avantage exponentiel en temps de calcul par rapport à un processeur classique. Un tel avantage, cependant, nécessite des dizaines de milliers ou des centaines de milliers de qubits selon l'algorithme^{307, 308}. Les défis technologiques associés au développement d'une machine de cette taille sont nombreux: limitations techniques, en terme par exemple de besoins en cryogénie ou en densité du circuit selon la modalité du qubit, mais aussi capacité à réduire le bruit, elle-même liée au code correcteur d'erreur utilisé et aux ressources supplémentaires requises.

Dans ce contexte, la solution consistant à interconnecter des QPU dans une architecture de calcul modulaire suscite actuellement un très grand intérêt, car elle ouvre une voie réaliste vers le passage à l'échelle du calcul quantique

307 E. Gouzien *et al.* "Factoring 2048-bit RSA Integers in 177 Days with 13 436 Qubits and a Multimode Memory", *Phys. Rev. Lett.* 127 140503 (2021).

308 L. Clinton *et al.* "Towards near-term quantum simulation of materials", *Nature Communications*, 15: 211 (2023)

dans un horizon de quelques années. Cette interconnexion consiste à intriquer des qubits appartenant à des QPUs distincts faisant en sorte qu'un nombre de qubits bien plus grand que ceux d'un seul QPU soit disponible pour le calcul. Il s'agit ensuite d'effectuer un algorithme distribué sur l'ensemble de ces QPUs interconnectés qui est ainsi équivalent à un ordinateur quantique de taille supérieure (figure 22).

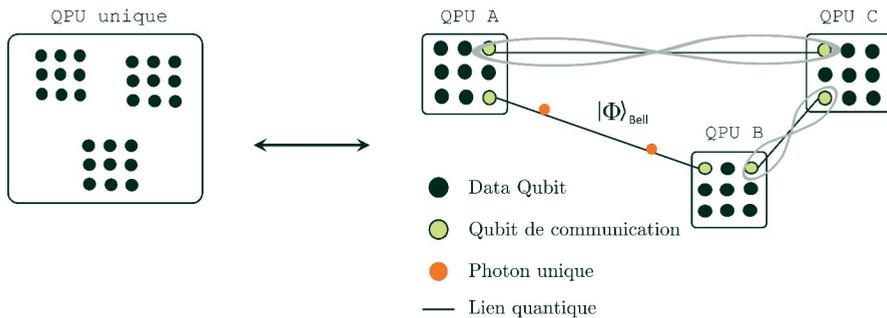


Figure 22: Principe de l'interconnexion de QPUs à l'aide de liens quantiques. Les QPUs A et C, ainsi que les QPUs B et C sont interconnectés. Une paire de Bell est sur le point d'intriquer des qubits de communication des QPU A et C.

Nous nous intéressons ici au modèle de calcul basé sur des circuits quantiques. Dans ce modèle, un algorithme est donné sous forme d'un circuit quantique abstrait, impliquant un certain nombre de qubits sur lesquels agissent des opérateurs unitaires à un ou plusieurs qubits, représentés par des portes logiques quantiques.

Afin de réaliser de telles portes entre des qubits appartenant à des QPUs distincts, deux protocoles sont principalement utilisés, appelés TeleData et TeleGate (voir paragraphes ci-dessous)³⁰⁹. Ces protocoles reposent tous deux sur l'intrication quantique. Leur utilisation conduit à définir deux catégories de qubits contenus dans chaque QPU à interconnecter : (1) les data qubits qui sont utilisés pour réaliser les opérations au sein du QPU lui-même et (2) les qubits de communication qui sont utilisés pour établir l'intrication entre

309 Van Meter, "Arithmetic on a Distributed-Memory Quantum Multicomputer", *ACM Journal on Emerging Technologies in Computing Systems*, 3 4 1-23 (2008)

QPUs. Établir l'intrication entre deux qubits de communication nécessite l'intermédiaire d'une paire de Bell dont chaque membre sera intriqué avec un des qubits de communication (figure 22). On nomme lien quantique le système matériel qui réalise l'interconnexion. Établir une interconnexion entre deux QPUs avec un lien quantique mobilise donc, dans un cas idéal, un qubit local dans chaque QPU et consomme une paire de Bell.

4.2.1. PARTITION DES ALGORITHMES QUANTIQUES

La partition d'un algorithme quantique est un problème inhérent au modèle du calcul quantique distribué. La capacité à partitionner un circuit est dans ce sens un enjeu majeur du passage à l'échelle du calcul quantique, et ce quelle que soit la taille d'un QPU (*Quantum Processing Unit*) qu'il sera possible d'atteindre dans l'avenir, car l'augmentation continue de besoins en ressources de calcul amènera le besoin d'interconnexion entre QPUs.

4.2.1.1. PARTITION CLASSIQUE

Les premières approches ont consisté à découper de façon classique le circuit quantique initial en un ensemble de sous-circuits indépendants les uns des autres. L'idée générale, compte tenu de la disponibilité d'un QPU de taille limitée et d'un circuit quantique nécessitant plus de qubits que ceux dont dispose le QPU, est de diviser le circuit en sous-circuits dont la taille correspond au nombre de qubits du QPU à disposition, remplaçant les opérations rendues non locales lors du découpage par des opérations locales. Les sous-circuits sont activés un à un sur le QPU, et les résultats sont recombinaés par des techniques de post-traitement classique afin de reproduire le résultat du circuit initial³¹⁰.

Cette technique de partition, et en particulier l'optimisation des coupes, est actuellement un sujet de recherche actif³¹¹. Cependant, tenter de reconstruire le résultat quantique à partir des résultats intermédiaires classiques conduit à

310 Piveteau *et al.*, "Circuit knitting with classical communication", *IEEE Transactions on Information Theory*, 70 4 (2023)

311 *Ibid.*

un surcoût significatif en termes de ressource de calcul classique. Ce surcoût évolue de façon exponentielle avec le nombre de coupes³¹², empêchant une implémentation réaliste au-delà de quelques dizaines de coupes. Le fait de préserver l'intrication lors de la coupe d'un circuit et de permettre des opérations non locales promet une partition davantage utilisable et plus optimale. C'est tout l'enjeu de l'interconnexion quantique de QPUs.

4.2.1.2. PARTITIONNEMENT QUANTIQUE PRÉSERVANT L'INTRICATION

L'interconnexion quantique de QPUs fournit la possibilité d'établir l'intrication entre différents QPUs et permet ainsi de réaliser des opérations logiques entre QPUs distincts, en exploitant les deux protocoles mentionnés auparavant qui sont les briques de base du calcul quantique distribué : TeleData et TeleGate.

a) Teledata

On souhaite réaliser le transfert de l'état quantique d'un qubit d'un QPU vers un qubit contenu dans un autre QPU (figure 31). Ce protocole est constitué d'une séquence de quatre phases :

1. dénération de l'intrication de deux qubits de communication appartenant aux deux QPUs distincts ;
2. opérations logiques sur les qubits du QPU initial (porte CNOT et porte à un qubit contrôle-rotation et Hadamard) ;
3. mesures intermédiaires de l'état des qubits impliqués dans le QPU initial et communication classique du résultat de ces mesures au second QPU ;
4. opérations conditionnelles locales dans le second QPU (porte à un qubit contrôle-rotation).

³¹² Harada *et al.* "Doubly optimal parallel wire cutting without ancilla qubits" *arXiv*: 2303.07340 (2023).

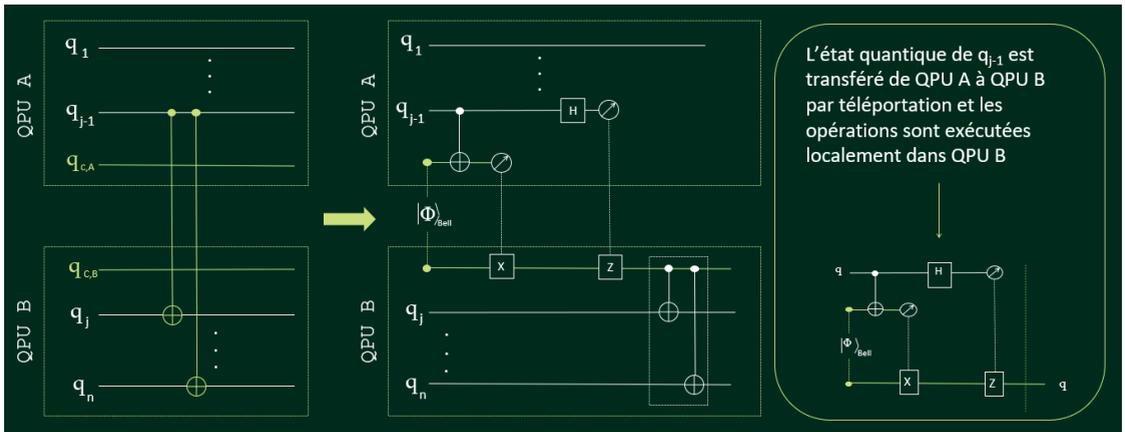


Figure 23 : Schéma de principe du protocole TeleData utilisé pour réaliser une porte à deux qubits non locale de type contrôle-rotation entre QPU A et QPU B. Une paire de Bell Φ est consommée par des qubits de communication pour établir l'intrication entre QPU A et QPU B. L'état quantique du qubit q_{j-1} est ensuite téléporté vers QPU B. Les portes logiques sont alors exécutées localement dans QPU B entre le qubit de communication et q_j . À la fin, l'information n'est plus contenue dans QPU A.

Avec ce protocole, à l'instar d'un protocole de téléportation quantique, l'état quantique d'un qubit appartenant au QPU A est transféré à un qubit appartenant au QPU B, et la suite des opérations est menée localement dans ce dernier. Le premier QPU ne possède plus l'information concernant le qubit initial.

b) TeleGate

On souhaite réaliser une porte à deux qubits entre les QPUs A et B (figure 24). Le protocole TeleGate peut être décomposé en trois grandes phases et a la particularité d'exploiter un état quantique intermédiaire qui partage une copie de l'état initial avec le QPU cible, sans téléporter l'état quantique. En prenant l'exemple d'une porte à deux qubits contrôle-rotation (CX par exemple), les trois étapes sont :

1. intrication de l'état quantique du qubit de contrôle avec un qubit de communication du deuxième QPU. À cette étape, une copie du qubit de contrôle est partagée en local sur le deuxième QPU, transformant le qubit de communication du QPU-B en un qubit de contrôle intermédiaire;

2. opérations locales entre le qubit de contrôle intermédiaire et les qubits cibles ;
3. restauration de l'état quantique initial qui peut être utilisé par la suite.

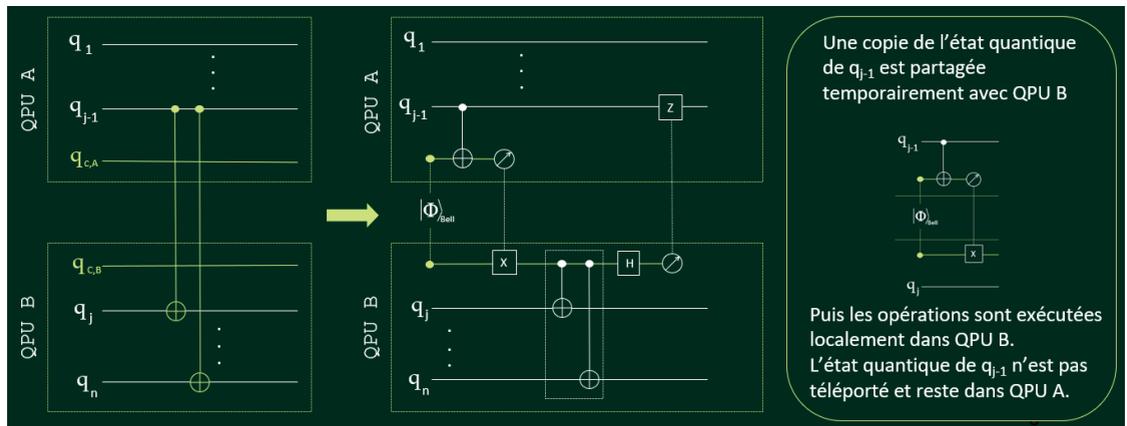


Figure 24: Schéma de principe du protocole TeleGate utilisé pour réaliser une porte à deux qubits non locale de type contrôle-rotation entre QPU A et QPU B. Une paire de Bell Φ est consommée par des qubits de communication pour établir l'intrication entre QPU A et QPU B. L'état quantique du qubit q_{j-1} est alors momentanément partagé avec QPU B et les portes logiques sont exécutées localement dans QPU B entre le qubit de communication et q_j . À la fin, l'état quantique intermédiaire est réinitialisé et l'information n'est plus contenue dans QPU B.

Avec ce protocole, l'état quantique du qubit de contrôle du QPU A n'a été que temporairement partagé avec le QPU B, durant le temps de réaliser les portes distribuées concernées, sans être téléporté. À la fin, l'information quantique reste dans le QPU A et n'est pas présente dans QPU B.

On note également que dans un contexte d'interconnexion d'un grand nombre de QPUs, une voie alternative à l'utilisation des protocoles TeleData et TeleGate passe par le développement de protocoles impliquant des états quantiques intriqués multipartites (par exemple, états maximale-ment intriqués GHZ, pour *Greenberger-Horne-Zeilinger*). Ceci pourrait optimiser le coût de la distribution d'intrication lorsqu'augmenteront le nombre

de liens d'interconnexion et le nombre de QPUs à interconnecter^{313, 314}. Ce cas nécessite cependant une investigation approfondie prenant en compte toutes les ressources nécessaires.

4.2.1.3. PARTITION OPTIMALE D'UN CIRCUIT QUANTIQUE

Le critère d'optimisation de partition que nous utilisons est de minimiser le nombre de liens quantiques d'interconnexion pour ne pas introduire un surcoût matériel trop important.

Pour cette optimisation, il est nécessaire de disposer d'un compilateur de distribution adapté à l'interconnexion des QPUs³¹⁵. Cette brique logicielle prend en entrée le circuit quantique à distribuer ainsi que les caractéristiques du réseau de QPUs (nombre de QPUs, nombre de qubits par QPU, nombre de liens quantiques, nombre de qubits de communication par QPUs, connectivité au sein du QPU, topologie du réseau...). Elle fournit en sortie la partition du circuit quantique initial en un ensemble de sous-circuits liés entre eux par un certain nombre d'opérations TeleData et TeleGate, qui minimise le nombre de paires de Bell nécessaires.

Comme présenté sur la figure 25, la première étape du compilateur de distribution consiste à mettre en correspondance les données du circuit quantique initial avec une structure de graphe dans laquelle les qubits deviennent les sommets, et les portes à deux qubits deviennent les arêtes.

Lors d'une deuxième étape, le graphe représentant le circuit quantique est partitionné à l'aide de techniques de partitionnement de graphe. Chaque partition correspond à un sous-circuit, fragment de l'algorithme initial, à exécuter sur un des QPUs interconnectés.

313 Meignant *et al.* "Distributing graph states over arbitrary quantum networks", *Phys. Rev.* À **100** 052333 (2018).

314 Barral *et al.* "Review of Distributed Quantum Computing. From single QPU to High Performance Quantum Computing", *arXiv*: 2404.01265 (2024)

315 Tomesh *et al.* "Divide and Conquer for Combinatorial Optimization and Distributed Quantum Computation", *IEEE International Conference on Quantum Computing and Engineering (QCE)* 11-12 (2023).

La troisième étape consiste à identifier les opérations multiqubits qui, après la partition, impliquent des qubits appartenant à différents sous-circuits. Il s'agit d'opérations distribuées qui doivent être effectuées à l'aide de protocoles qui ont été présentés plus haut.

Le compilateur de distribution itère ces étapes pour minimiser le nombre de paires de Bell utilisées. Il fournit alors la partition du graphe optimale. Lors d'une dernière étape, les sous-graphes sont alors retransformés en sous-circuits mettant en jeu des opérations distribuées. Chacun de ces sous-circuits sera envoyé à un QPU et les liens quantiques d'interconnexion effectueront les opérations nécessaires selon la partition optimale.

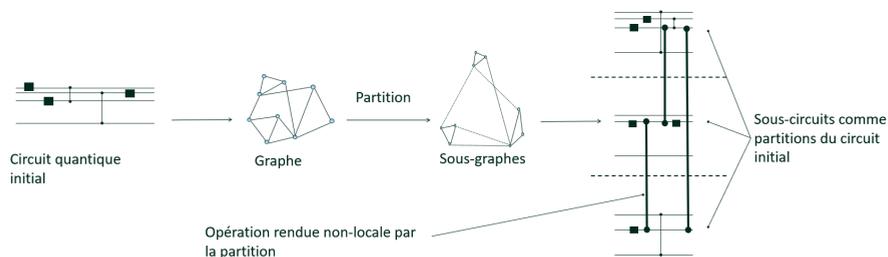


Figure 25 : Schéma de principe du compilateur de distribution. La partition est réalisée sur le graphe équivalent au circuit quantique initial. À la suite de cette partition, certaines opérations sont rendues non locales. Elles pourront être exécutées grâce aux protocoles TeleData ou TeleGate, en minimisant le nombre de paires de Bell consommées.

4.2.1.4. LIEN AVEC LA CORRECTION D'ERREUR

Un aspect important du calcul quantique distribué est la prise en compte de la correction d'erreur qui est une étape incontournable pour la pleine adoption du calcul quantique. Il est en effet nécessaire d'anticiper en entrée du compilateur de distribution les algorithmes dans leur version tolérante aux fautes. Ceci conduira à une étape d'optimisation supplémentaire par rapport à celle présentée précédemment, prenant en compte le surcoût des mesures intermédiaires qui doivent être réalisées en cours de circuit selon les codes correcteurs d'erreur choisis.

La possibilité d'intriquer des qubits à une distance arbitraire, y compris entre QPUs distincts, ouvre par ailleurs la voie à de nouvelles architectures de codes correcteurs d'erreur qui promettent de diminuer drastiquement le rapport entre le nombre de qubits physiques sur le nombre de qubits logiques^{316, 317}. Ce domaine explorant la correction d'erreur facilitée par l'interconnexion quantique est encore dans une phase préliminaire, mais présente un potentiel intéressant.

4.2.2. MISE EN ŒUVRE AU NIVEAU MATÉRIEL

D'un point de vue physique, la voie la plus adaptée pour réaliser des liens d'interconnexion quantique consiste à utiliser des paires de photons intriqués. En effet, on bénéficie alors de la grande maturité des technologies photoniques.

Le calcul quantique distribué sur un réseau de QPUs interconnectés nécessitera des liens quantiques permettant des architectures variées et flexibles. Ces liens devront créer l'intrication à la demande, suffisamment rapidement pour ne pas limiter l'exécution des algorithmes quantiques, et préservant la fidélité des opérations logiques du calcul.

4.2.2.1. LIENS QUANTIQUES D'INTERCONNEXION

Un lien quantique est un système qui permet de créer de l'intrication photonique pour établir l'interconnexion entre les qubits de communication des QPUs. En fonction de la technologie des QPUs, il est intéressant de disposer d'un lien quantique qui absorbe une paire de Bell émise par les registres quantiques à interconnecter ou d'un lien quantique qui produit à la demande et met à disposition une paire de Bell. Dans les deux cas, la vitesse à laquelle on établit l'intrication et la fidélité des protocoles TeleData et TeleGate qui en résulte sont les deux paramètres principaux du lien.

316 Cohen *et al.* "Low-overhead fault-tolerant quantum computing using long-range connectivity", *Science Advances* 8 20 (2022)

317 Pecorari *et al.* "High-rate quantum LDPC codes for long-range-connected neutral atom registers", *arXiv*: 2404.13010 (2024)

a) Lien quantique absorptif

Pour certains types de QPU, comme ceux à qubits supraconducteurs, l'émission d'un photon unique par le qubit de communication est l'approche la plus simple. Dans ce cas, lors de l'émission, ce photon est intriqué avec le qubit de communication qui l'a émis. Comme présenté par la figure 26, le lien quantique va collecter les photons émis par chacun des QPUs à interconnecter, et les faire interférer en réalisant une mesure de Bell. Le fait que ces photons interfèrent au même moment sur le module de Bell crée l'intrication entre ces photons, ce qui résulte par transitivité en l'intrication des qubits de communication appartenant aux QPUs.

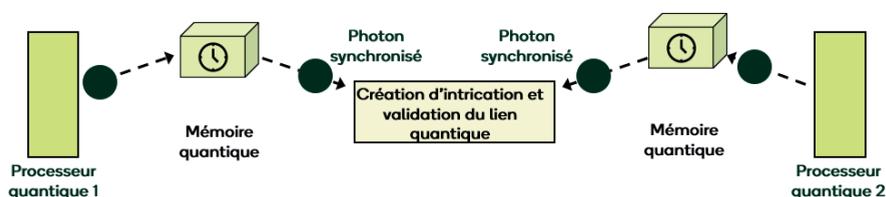


Figure 26 : Schéma de principe d'un lien quantique absorptif. Le lien quantique collecte les photons uniques émis par les qubits de communication des QPU à interconnecter et les fait interférer pour établir l'intrication entre les qubits de communication. À l'issue du processus, la paire de Bell est consommée.

L'émission du photon intriqué par les QPUs est probabiliste, et il est nécessaire d'utiliser une mémoire quantique pour synchroniser l'arrivée des photons collectés sur le module de mesure.

b) Lien quantique émissif

Dans certaines situations, il est plus avantageux de disposer d'un lien quantique qui produit des paires de Bell à la demande. Dans ce cas, le lien quantique produit une ressource d'intrication photonique qui est mise à disposition des QPUs à un instant arbitraire ajustable par l'ordonnanceur du calcul. Une paire de photons uniques intriqués est créée à l'intérieur du lien. Chacun de ces photons est ensuite stocké dans une mémoire quantique, qui réémet de façon synchronisée un photon vers les QPUs à interconnecter. Cette paire de photons intriqués constitue la paire de Bell qui sera absorbée

par les qubits de communication des QPUs, ce qui établira l'interconnexion entre QPUs (figure 27).

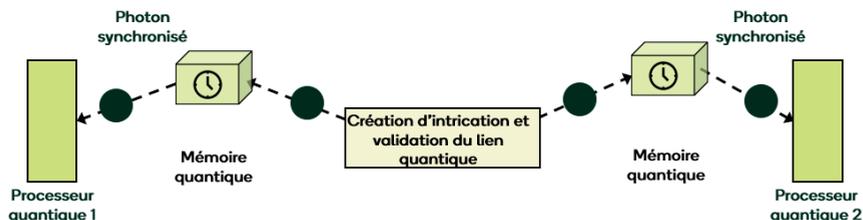


Figure 27 : Schéma de principe d'un lien quantique émissif. Le lien quantique prépare une paire de photons intriqués (paire de Bell) qui est mise à disposition des QPUs à interconnecter. Chacun de ces photons sera ensuite absorbé par un qubit de communication. Grâce aux mémoires quantiques, ce type de lien d'interconnexion peut fournir à la demande une ressource d'intrication photonique.

Dans cette situation, le rôle des mémoires quantiques à la demande est essentiel. En effet, ce sont elles qui stockent la ressource d'intrication qui a été créée à l'avance, jusqu'au moment où la paire de Bell est prête à être consommée par les QPUs pour réaliser un protocole TeleData ou TeleGate. Il est ainsi possible d'ajuster les délais temporels entre l'arrivée des paires de Bell et l'exécution des portes logiques afin de minimiser la durée des protocoles et maximiser ainsi le temps de calcul effectif.

Par exemple dans le cas de l'interconnexion de QPUs à atomes neutres, on veut pouvoir fournir une ressource d'intrication photonique au moins à chaque cycle de QPU juste avant le début de la phase de calcul, c'est-à-dire à un temps de cycle de l'ordre de 100 ms³¹⁸.

4.2.2.2. MÉMOIRE QUANTIQUE À LA DEMANDE EFFICACE

Une mémoire optique quantique à la demande est un système qui accepte en entrée un état quantique photonique, le stocke pendant un certain temps et le réémet plus tard sur ordre d'un signal extérieur de déclenchement.

318 L. Henriet *et al.*, "Quantum computing with neutral atoms", *Quantum* 4 327 (2020)

Dans un lien quantique, la mémoire joue le rôle de tampon et permet d'ajuster dans le temps l'émission de photons uniques, ce qui est une caractéristique essentielle pour une interconnexion optimale.

Une mémoire quantique est caractérisée par quatre paramètres physiques principaux :

- l'efficacité de la mémoire, qui correspond à la probabilité de récupérer un photon en sortie. Ce paramètre est essentiel pour obtenir une interconnexion efficace. L'état de l'art des efficacités est aujourd'hui de l'ordre de 90 %³¹⁹. Ce niveau de performance permet des liens quantiques pouvant établir l'intrication avec des fidélités supérieures à 99,5 % et des temps de cycle de l'ordre de 50 ms ;
- le temps de stockage, qui correspond à la durée pendant laquelle le photon peut être stocké avant de voir l'efficacité de la mémoire diminuée d'un facteur 1/e. Pour l'interconnexion locale, un temps de stockage de quelques dizaines de microsecondes est suffisant ;
- la fidélité de la mémoire, qui compare l'état quantique du photon en sortie avec l'état quantique du photon en entrée. Aujourd'hui, les mémoires quantiques présentent des fidélités de plus de 99,5 % ;
- le multiplexage, qui indique combien de photons une mémoire quantique peut stocker à la fois.

Il existe plusieurs plateformes physiques pour réaliser une mémoire quantique (atomes froids, atomes en vapeur, cristaux dopés...). La mémoire quantique à atomes froids présente des caractéristiques favorables pour l'interconnexion locale de QPUs et bénéficie de la maturité de la technologie des atomes froids pour en faire un produit au standard industriel qui puisse être exploité en dehors des laboratoires.

319 Cao *et al.* "Efficient reversible entanglement transfer between light and quantum memories", *Optica* 7 10 (2020)

À l'heure actuelle, les mémoires quantiques à atomes froids démontrent le record du monde d'efficacité à un niveau de 90 %, rendant possible l'interconnexion de QPUs à l'aide de liens quantiques.

4.2.2.3. INTERFACE ENTRE LE LIEN QUANTIQUE ET LES QPUs

La technologie de qubit des QPUs à interconnecter (atomes neutres, ions piégés, photons...) va déterminer les caractéristiques physiques des photons des paires de Bell qui seront utilisés pour créer l'intrication. En particulier, leur longueur d'onde et leur étalement temporel sont déterminants. Afin d'obtenir des protocoles TeleData et TeleGate performants, il est nécessaire d'ajuster l'interface entre la mémoire quantique et ces photons.

Il est possible d'ajuster la longueur d'onde optique avec un étage de conversion de fréquence. Pour cette brique technologique mature basée sur l'utilisation de cristaux non linéaires, il sera nécessaire de maximiser les efficacités de conversion. Dans le cas de qubits supraconducteurs, il est nécessaire d'ajouter un étage de transduction, qui permet de convertir un qubit du domaine micro-onde en un qubit dans le domaine optique. Plusieurs acteurs travaillent actuellement à développer ce type de transducteur, qui sera disponible comme sous-système³²⁰.

Pour ce qui est de l'étalement temporel des photons, il est possible d'ajuster les paramètres physiques de la mémoire quantique pour qu'elle accepte de photons plus ou moins courts. Les mémoires à atomes froids présentent en particulier la versatilité nécessaire pour s'adapter aux différentes modalités de qubits.

4.2.2.4. CAS NON IDÉAL

En pratique, les paires de Bell produites pour établir l'intrication ne sont pas parfaites. Par ailleurs, les pertes introduites lors du couplage entre les photons uniques et les qubits de communication doivent être prises en compte.

³²⁰ Weaver *et al.* "An integrated microwave-to-optics interface for scalable quantum computing", *Nat. Nanotechnol.* **19** 166-172 (2024).

Il sera donc nécessaire d'ajouter une étape de purification de l'intrication³²¹ et de la redondance au niveau du lien quantique. Ceci indique qu'il sera utile d'allouer plusieurs qubits de communication par QPU pour un protocole TeleData ou TeleGate ainsi que de disposer de liens quantiques multiplexés.

4.2.3. CONCLUSION

L'interconnexion de QPUs à l'aide de liens quantiques photoniques basés sur des mémoires quantiques efficaces est une voie prometteuse pour le passage à l'échelle du calcul quantique. En mettant en réseau des QPUs de taille intermédiaire, elle permettra d'envisager un ordinateur quantique effectif présentant un nombre de qubits, une qualité de qubits et un temps de cohérence suffisant pour exécuter des algorithmes quantiques non triviaux.

Le développement actuel de mémoires quantiques multiplexées permettra des topologies de réseaux quantiques plus complexes, la mise en œuvre de schémas de redondance des liens quantiques pour améliorer la fidélité des portes quantiques distribuées, et ouvre la voie à la distribution efficace d'intrication multipartite.

Pour assurer le passage à l'échelle du calcul quantique grâce à l'interconnexion de QPUs ainsi que la pleine adoption du calcul quantique distribué tolérant aux fautes, il est nécessaire d'anticiper l'intégration des technologies de liens quantiques en environnement de calcul intensif, tant sur les aspects logiciels que matériels. Ces technologies d'interconnexion constituent une ressource quantique à part entière au même titre que les QPUs, et permettront la mise en service de grappes de processeurs quantiques interconnectés.

4.3. SCALABILITÉ ET CONNECTIVITÉ DES QUBITS SUPRACONDUCTEURS

La fidélité des portes à un ou deux qubits augmente régulièrement dans les plateformes à qubits supraconducteurs. Dans l'architecture la plus utilisée au niveau mondial (qubits de type transmon), la fidélité de la porte CNOT est

321 Bennett *et al.* "Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels", *Phys. Rev. Lett.* **76** 722 (1996)

désormais comprise entre 99,3% et 99,7% (chez IBM dans ses processeurs Heron r1 et r2 lancés en 2023 et 2024). Par ailleurs, les facteurs limitant les fidélités de mesure sont en passe d'être compris. Nous arrivons donc sous les seuils théoriques de codes de correction d'erreur (*surface code*, codes LDPC...).

Dans cette section, nous donnons un panorama des problèmes potentiels lors de la mise à l'échelle des architectures supra (pour des processeurs à 1000 voire 1 million de qubits) et des efforts réalisés pour résoudre ces problèmes. Nous évoquons aussi des pistes permettant d'augmenter la connectivité (nombre de qubits avec lesquels chaque qubit peut réaliser une porte logique) de ces architectures.

4.3.1. INTÉGRATION 3D ET SUPPRESSION DES COUPLAGES PARASITES LORS DE LA MISE À L'ÉCHELLE

La plupart des processeurs à petit nombre de qubits sont fabriqués selon une architecture planaire. Lorsqu'on augmente le nombre de qubits, deux problèmes se posent :

- si on arrange les qubits selon un quadrillage, il est plus difficile, mais pas impossible de contrôler tous les qubits indépendamment sans que les lignes de contrôle se croisent ou ne croisent les interconnexions entre qubits (lorsque ces lignes se croisent, un signal a tendance à fuiter d'une ligne à l'autre). En augmentant la taille de la puce pour incorporer plus de qubits, on abaisse la fréquence de modes électromagnétiques définis par le porte-échantillon métallique contenant la puce (dont le champ est principalement contenu dans le substrat). Ces modes sont responsables de *cross talks* entre qubits non nominalement connectés. Une solution à ces deux problèmes est d'utiliser des vias. Une via est un tunnel perçant la puce et dont les bords sont métallisés (TSV: *Through Silicon Vias*). Ils permettent de faire passer des lignes de contrôle orthogonales à la puce ;
- définir des frontières conductrices évitant l'apparition de modes résonants à basse fréquence.

Les TSV doivent être réalisés avec des matériaux supraconducteurs, ce que l'on ne sait pas encore faire actuellement. Un exemple est donné en figure 28. Une technologie similaire est développée dans^{322, 323}. Cette technologie permet de diminuer les *cross talks* entre qubits non nominalement connectés de \sim -40 dB (pour les qubits physiquement les plus proches, cette isolation est censée augmenter exponentiellement avec la distance). Elle permet en principe également de connecter des qubits distants sur la puce, et pas seulement des plus proches voisins.

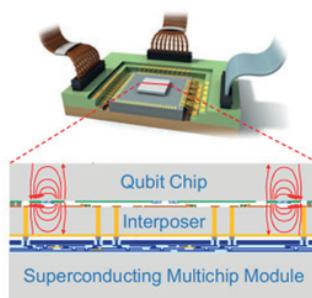


Figure 28

Source : Yost, Donna-Ruth W., *et al.* "Solid-state qubits integrated with superconducting through-silicon vias." *npj Quantum Information* 6.1 (2020): 59.

Il est à noter que :

- avec un grand nombre de qubits, on s'expose au phénomène de *spectral crowding* : il devient de plus en plus probable que deux qubits aient une fréquence très proche. Si le couplage résiduel est de l'ordre du désaccord de fréquence, les deux qubits s'hybrident et on obtient une interaction (porte) non voulue entre qubits non nominalement connectés. Pour éviter ces « collisions de fréquence » sur une puce à grand nombre de qubits, il faudra effectivement que les *cross talks* soient fortement supprimés à longue distance, la fréquence des qubits étant difficilement prévisible à

322 Acharya, Narendra, *et al.* "Integration of through-sapphire substrate machining with superconducting quantum processors." *arXiv preprint arXiv: 2406.09930* (2024).

323 Spring, Peter A., *et al.* "High coherence and low cross-talk in a tileable 3D integrated superconducting circuit architecture." *Science Advances* 8.16 (2022): eabl6698.

mieux que ~1% au moment de la fabrication, du fait du manque de reproductibilité du courant critique des jonctions Josephson (malgré des progrès récents pour ajuster ce courant critique par des méthodes de recuit local);

- pour éteindre ou allumer des interactions entre qubits nominalement connectés, les principaux acteurs du domaine utilisent des coupleurs ajustables: un circuit ajustable en flux est placé entre les deux qubits à connecter. Ce circuit médie une interaction qui s'ajoute à l'interaction nativement présente. Lorsqu'on veut éteindre l'interaction, on choisit un flux pour lequel ces deux contributions s'annulent exactement^{324, 325}. Ce circuit occupe une place équivalente à celle d'un qubit et il en faut environ deux par qubit (121 coupleurs dans la puce Sycamore de 72 qubits de Google), ce qui multiplie au passage par presque trois la surface de la puce à nombre égal de qubits utiles.

4.3.2. EMPREINTE ET RESSOURCES D'ENVIRONNEMENT

4.3.2.1. EMPREINTE DES CIRCUITS

Si les problèmes de *cross talks* et d'adressage en 3D sont réglés, il n'y a, *a priori*, pas d'obstacle à l'augmentation de la taille des puces et le nombre de qubits. En termes d'ordre de grandeur, un transmon a une empreinte typique inférieure à 0,5 mm × 0,5 mm, ce qui permet d'assembler 300 000 qubits sur un *wafer* de 12 pouces de diamètre. L'empreinte par transmon pourrait être drastiquement réduite en utilisant des technologies de «*parallel plate capacitors*».

324 Arute, Frank, *et al.* "Quantum supremacy using a programmable superconducting processor." *Nature* 574.7779 (2019): 505-510.

325 Zhang, Helin, *et al.* "Tunable Inductive Coupler for High-Fidelity Gates Between Fluxonium Qubits." *PRX Quantum* 5.2 (2024): 020326.

4.3.2.2. EMPREINTE DES COMPOSANTS MICRO-ONDES

Dans un système quantique « *full-stack* » une contribution importante vient des composants « d'environnement » utilisés pour générer et détecter les signaux de contrôle et les router vers chaque qubit. En particulier, les signaux d'entrée (atténués) doivent être séparés physiquement des signaux de sortie (amplifiés) par des composants non réciproques (circulateurs). La plupart des composants disponibles commercialement (circulateurs, amplificateurs, atténuateurs...) sont volumineux ($\sim \text{cm}^3$) et coûteux. Des efforts importants sont réalisés par la communauté pour miniaturiser et intégrer ces composants sur puce^{326, 327}.

4.3.2.3. RESSOURCES EN ÉLECTRONIQUE CLASSIQUE

Une autre composante *hardware* dont l'empreinte peut poser un problème est l'électronique permettant de générer les pulses de contrôle, détecter les pulses de mesure et effectuer des opérations mathématiques plus ou moins complexes pour la correction d'erreur. Le coût de ces systèmes est pour l'instant élevé (de l'ordre de 10 000 euros pour contrôler un qubit), mais appelé à baisser sous l'effet de la concurrence, avec des systèmes programmables *open source* (Qubic, Qick...). La possibilité récente de générer numériquement des pulsations micro-onde arbitraires (par opposition à un traitement analogique d'un signal monochromatique mixé avec des pulses basse fréquence) ouvre également la possibilité d'un multiplexage important pour partager une seule ligne de contrôle entre plusieurs qubits. Les systèmes de routage de micro-ondes reconfigurables sur puce pourraient encore augmenter les capacités de multiplexage. Enfin, à terme, il sera peut-être possible d'effectuer les opérations de traitement de l'information classique à basse température dans un système intégré à l'architecture quantique (technologie RSFQ à basse consommation énergétique)³²⁸.

326 Macklin, Chris, *et al.* "A near - quantum-limited Josephson traveling-wave parametric amplifier." *Science* 350.6258 (2015): 307-310.

327 Chapman, Benjamin J., *et al.* "Widely tunable on-chip microwave circulator for superconducting quantum circuits." *Physical Review X* 7.4 (2017): 041043.

328 Liu, Chuan-Hong, *et al.* "Single flux quantum-based digital control of superconducting qubits in a multichip module." *PRX Quantum* 4.3 (2023): 030310.

4.3.2.4. RESSOURCES EN CRYOGÉNIE

Des annonces récentes ont montré qu'il était possible d'augmenter significativement la taille et puissance des cryostats à dilution d'hélium servant à refroidir les qubits supraconducteurs à 10 mK. Citons en particulier la connexion de deux cryostats par un lien supraconducteur³²⁹ et un cryostat pouvant accueillir plusieurs milliers de qubits avec des composants micro-ondes actuels (Bluefors KIDE). Si l'intégration sur puce des composants se poursuit, la cryogénie ne devrait pas être un facteur limitant.

À l'opposé du spectre, on note l'apparition de cryostats de petites dimensions, moins coûteux, nécessitant moins d'hélium3 et consommant moins d'énergie, portés par de nouveaux acteurs (Maybell, Qinu) comme par les leaders du marché (Bluefors). D'autres approches industrielles telles que celles proposées par Air Liquide permettent d'envisager la création de cryostats de très forte puissance pour supporter un grand nombre de qubits physiques.

4.3.3. CONNECTIVITÉ

La connectivité d'une architecture dénote le nombre de qubits avec lesquels chaque qubit peut réaliser une porte logique. On peut en donner une définition plus large comme étant le nombre de portes logiques élémentaires pour intriquer deux qubits arbitraires.

Le *surface code*, qui est le code correcteur d'erreur le plus étudié, a l'avantage d'avoir une structure de faible connectivité (4) avec des interactions entre plus proches voisins uniquement selon une géométrie plane. D'autres codes permettent d'avoir des performances meilleures (en termes de seuil de correction ou de nombre de qubits logiques encodés par qubit physique) avec une connectivité plus grande et/ou une topologie plus élaborée (structure à plus de deux dimensions). Les codes LDPC sont un exemple prometteur de code à haute densité en qubits logiques.

329 <https://bluefors.com/products/kide-cryogenic-platform/>

Un autre élément à prendre en compte est la chaîne de lecture qui repose aujourd'hui sur l'usage de circulateurs, d'amplificateurs bas bruit fonctionnant à 15 mK (notamment les TWPA de *Silent Waves*), d'amplificateurs HEMT opérant à 4K et d'amplificateurs fonctionnant à température ambiante. L'ensemble de ces dispositifs permet de multiplexer en fréquence les signaux de lecture d'environ 8 à 10 qubits lorsque l'amplification bas bruit s'appuie sur un TWPA. Mais chacun des éléments évoqués occupe une place significative, avec des parallélépipèdes d'environ 2 cm de côté et moins de 1 cm d'épaisseur. Des techniques visant à miniaturiser ces composants sont développées. Les circulateurs peuvent notamment être remplacés par des circuits supraconducteurs occupant beaucoup moins de place.

4.3.3.1. CONNECTIVITÉ SUR PUCE UNIQUE

Par rapport à d'autres plateformes où les systèmes physiques encodant l'information quantique peuvent être déplacés, une connectivité « *all-to-all* » semble irréaliste pour les circuits supraconducteurs au stade actuel. Cependant, il paraît possible d'établir quelques connexions « longue distance » sur la puce (par exemple selon le schéma décrit en figure 29 pour enrichir une architecture à connexions entre proches voisins. Cela permet de diminuer drastiquement le nombre de portes élémentaires pour effectuer une opération sur 2 qubits arbitraires, ou d'implémenter efficacement un code précis³³⁰.

À terme, une architecture de routage des micro-ondes sur puce reconfigurable *in situ* permettrait d'augmenter la connectivité de manière arbitraire.

4.3.3.2. CONNECTIVITÉ INTERPUCE OU À LONGUE DISTANCE

La connexion de plusieurs puces permettant d'effectuer des portes logiques entre qubits distants de l'ordre du mètre a été démontrée, avec des fidélités de porte s'approchant des fidélités sur puce unique³³¹. Bien que ces

330 Bravyi, Sergey, *et al.* "High-threshold and low-overhead fault-tolerant quantum memory." *Nature* 627.8005 (2024): 778-782.

331 Niu, Jingjing, *et al.* "Low-loss interconnects for modular superconducting quantum processors." *Nature Electronics* 6.3 (2023): 235-241.

démonstrations soient pour l'instant de faible taille et avec une empreinte en matériel importante, ce type d'architecture dite *modulaire* pourrait à terme présenter des avantages décisifs: remplacement de modules défectueux ou hors spécification, correction des « *chip-scale failures* », suppression des *cross talks*...

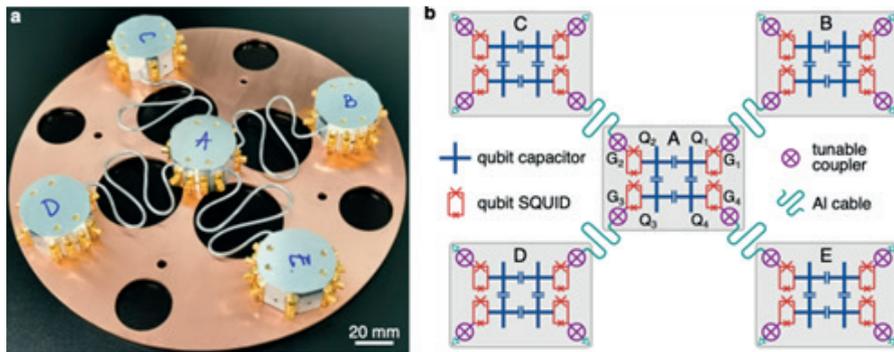


Figure 29

Source : Niu, Jingjing, *et al.* "Low-loss interconnects for modular superconducting quantum processors." *Nature Electronics* 6.3 (2023): 235–241.

Vu les pertes micro-ondes importantes dans les lignes de transmission micro-onde (atténuation par mètre très supérieure au domaine optique même pour des lignes supraconductrices), l'intrication à longue distance nécessitera sûrement de passer par la transduction vers le domaine optique. L'efficacité quantique et la rapidité des systèmes transducteurs augmentent régulièrement, mais ces systèmes ne sont pas encore matures.

4.3.4. AUTRES DÉFIS POUR L'OPÉRATION D'ARCHITECTURES À GRAND NOMBRE DE QUBITS

4.3.4.1. EMPOISONNEMENT AUX QUASI-PARTICULES ET CHIP-SCALE FAILURE

La défaillance généralisée de tous les qubits sur une puce (ou du moins une dégradation significative du temps de cohérence de la majorité des qubits) est un phénomène observé sur tous les grands processeurs actuels sur une échelle de temps typique de 1s à 1 min. Ces erreurs ne peuvent pas être corrigées. Elles sont attribuées à des impacts de haute énergie par des rayons cosmiques ou provenant de la radioactivité naturelle des matériaux. Ces impacts génèrent des cascades de phonons, eux-mêmes générant un grand nombre de quasi-particules qui peuvent faire relaxer les qubits lorsqu'elles passent par effet tunnel au travers des jonctions Josephson. L'écrantage contre les impacts de haute énergie paraît utile, mais insuffisant (même dans des laboratoires enfouis sous une montagne). Le piégeage des phonons³³² ou des quasi-particules elles-mêmes³³³ semble être une voie prometteuse, mais pour l'instant très insuffisante au vu du temps d'exécution des algorithmes quantiques. Une architecture modulaire pourrait régler ce problème (éventuellement avec des modules de taille intermédiaire [100-1000 qubits] pour limiter l'empreinte totale).

4.3.4.2. TWO-LEVEL SYSTEMS

L'appellation *Two-Level System* (TLS) désigne un bain de systèmes parasites se couplant aux qubits supraconducteurs. Leur origine est méconnue et probablement multiple (fluctuateurs électriques piégés aux interfaces substrats/air, substrat/métal ou métal/air, fluctuateurs magnétiques basse fréquence...). Lorsqu'un TLS est résonant ou quasi résonant avec un qubit, il peut dégrader son temps de relaxation T1 et modifier sa fréquence de résonance. Par ailleurs, il est observé que ce « bain de TLS » se reconfigure de manière imprédictible sur des échelles de temps variant de la seconde au

332 Henriques, Fabio, *et al.* "Phonon traps reduce the quasiparticle density in superconducting circuits." *Applied physics letters* 115.21 (2019).

333 McEwen, Matt, *et al.* "Resisting high-energy impact events through gap engineering in superconducting qubit arrays." *arXiv preprint arXiv: 2402.15644* (2024).

jour, probablement du fait de l'interaction de TLS résonant dans la gamme GHz avec des TLS basse fréquence³³⁴.

Les TLS sont un défi majeur pour les architectures à grand nombre de qubits, car leur reconfiguration oblige à une recalibration fréquente de la puce pour compiler un algorithme en évitant les qubits dégradés, réajuster les coupleurs permettant d'éteindre les interactions non voulues (voir 1 b) et généralement en limitant la fidélité des portes logiques.

Les axes d'effort de la communauté portent sur :

- l'ingénierie des matériaux pour limiter le nombre de TLS;
- la recalibration rapide des paramètres du système, éventuellement par apprentissage machine;
- le design de nouveaux qubits moins sensibles aux fluctuateurs électriques.

4.3.5. CONCLUSION

Il n'existe pas d'obstacle majeur identifié à l'avènement de circuits supraconducteurs de grande taille si les technologies continuent leur progression rapide. Les défis actuels les plus sérieux sont probablement ceux de l'empoisonnement aux quasi-particules et aux bains de TLS. Il est à noter que ce sont aussi les défis dont la communauté a pris conscience le plus récemment et pour y répondre les architectures n'ont pas encore été autant optimisées que pour d'autres sources d'erreurs.

Nous avons focalisé le propos sur les qubits de type transmon qui sont les plus largement utilisés actuellement, mais les autres types de qubits à maturité (fluxoniums, qubits bosoniques...) font face aux mêmes défis. Nous terminons un aperçu des acteurs. Au niveau mondial, l'écosystème

334 Faoro, Lara, and Lev B. Ioffe. "Interacting tunneling model for two-level systems in amorphous materials and its predictions for their dephasing and noise in superconducting microresonators." *Physical Review B* 91.1 (2015): 014201.

américain et (dans une moindre mesure) européen (incluant Israël) se sont considérablement développés ces dernières années avec des acteurs industriels importants (IBM, Google, Amazon, Northrop Grumman), des startups de taille intermédiaire (Rigetti computing, IQM, Alice&Bob...), des compagnies proposant des services de fonderie (Quantware, Imec), de l'électronique dédiée (Keysight, Zurich Instruments, QBlox, Quantum Machines), des composants micro-ondes (LNF, *Silent Waves* pour les amplificateurs bas-bruit)... Les groupes académiques leaders du domaine sont plutôt situés aux États-Unis (MIT, Yale, Stanford, Berkeley...) ainsi que des instituts publics (National Labs) fournissant aux groupes académiques américains des services de technologie d'environnement (amplificateurs TWPA des Lincoln Labs notamment). Le Japon possède un groupe académique de premier plan (Riken) ainsi que des industries de composants électroniques de haut niveau. L'écosystème chinois, en partie découplé, est mal connu. Citons la *Chinese Academy of Science* et *Tsinghua University* comme acteurs académiques de premier plan, et au moins une entreprise, Origin Quantum, qui semble se placer sur le même créneau que les grands groupes américains. En France, les principaux groupes académiques sont situés à Saclay, Paris et Grenoble, mais n'ont pas fortement investi la mise à l'échelle des qubits supraconducteurs. Alice&Bob est la principale startup du domaine et devrait s'attaquer prochainement à la mise à l'échelle de ses qubits de chat. À noter la startup *Silent Waves* à Grenoble proposant des amplificateurs TWPA pour les mesures quantiques.

Chapitre 5

ÉLÉMENTS COMPLÉMENTAIRES

5.1. INTRODUCTION

Le raisonnement économique-politique concernant le développement d'une technologie radicalement innovante comme le FTQC peut être articulé autour d'un certain nombre de questions. Nous en passons un certain nombre en revue. Au-delà de l'analyse technique des applications particulières envisagées pour la FTQC, il s'agit d'esquisser sur quelles bases l'investissement considérable en cours pourrait être justifié.

Nous abordons aussi dans ce chapitre le lien avec le Calcul haute performance, la nécessité de disposer de *benchmarks*, et les besoins en capital humain.

5.2. ANALYSE TECHNICO-ÉCONOMIQUE DE L'ÉCOSYSTÈME - COMPARAISONS HISTORIQUES

Il n'est pas vraiment pertinent de comparer le projet FTQC aux étapes de développements de technologies matures comme les filières nucléaires ou les générations de microcircuits intégrés. À cette étape, on peut se référer à d'autres projets à composantes techno-scientifiques représentant des défis totalement nouveaux à leur époque ou actuellement.

5.2.1. LA FUSION NUCLÉAIRE

L'impact du succès éventuel est très important, tant sur le plan stratégique qu'universel. Deux filières techniques sont possibles et l'incertitude est grande sur la faisabilité des deux. Le coût du projet ITER de fusion par confinement magnétique est révisé à 25 milliards d'euros (Wikipédia). Le coût cumulé des projets Mégajoule et NIF par confinement inertiel (à visée initiale surtout en

stratégie de défense) est de l'ordre de dix milliards de dollars pour un TRL similaire.

5.2.2. LA RECHERCHE SPATIALE (VOLS HABITÉS)

Dans le domaine spatial, la comparaison la plus pertinente concerne les vols habités et plus particulièrement les programmes Apollo, navette et station spatiale internationale, dont les coûts cumulés respectifs sont (source Wikipédia): Apollo (19 milliards de dollars jusqu'en 1970 soit 150 milliards actualisés), navette spatiale (190 milliards actualisés), station spatiale internationale (115 milliards en cours). Un discours sur les justifications par des applications concrètes, comme la croissance de cristaux ou la production de médicaments en microgravité, a été tenu à l'époque. Indépendamment du fait que les avantages n'ont pas été démontrés. Il est clair que l'investissement était sans commune mesure avec l'apport potentiel de tels objectifs. La justification réelle est géostratégique. C'est vrai bien sûr du point de vue de la défense, mais de manière générale l'exploration spatiale est une nouvelle frontière et les perspectives au-delà de l'horizon sont indéterminées et potentiellement immenses. Les grands acteurs mondiaux sont tenus de ne pas se laisser dépasser par leurs concurrents, indépendamment de toute considération économique.

5.2.3. LE GÉNOME PROJECT

Les impacts scientifiques, sociétaux et médicaux étaient prévisibles et se sont concrétisés rapidement. L'incertitude était limitée, même si la faisabilité a demandé le développement de nouvelles technologies. Avec un coût de 3 milliards de dollars, c'est clairement un des grands projets technico-scientifiques qui a été le plus rentable.

5.2.4. LE CERN (ACCÉLÉRATEUR LHC)

Il est utile de rajouter aux exemples un projet à vision purement scientifique comme l'accélérateur LHC, dont le coût s'établit autour de 8,9 milliards d'euros (Wikipédia). En effet, on peut faire le raisonnement qu'en l'absence

éventuelle de tout débouché pratique., la recherche sur le FTQC conduit à des avancées fondamentales, théoriques et expérimentales, sur la nature profonde de la physique quantique. Dans cette perspective, la question de la valeur relative de ces avancées, comparées par exemple à la mise en évidence du boson de Higgs, ne peut éviter d'être posée, même si elle est probablement indécidable.

5.2.5. COMPARAISON AU FTQC

L'impact économique possible identifiable aujourd'hui est très inférieur à la fusion et au génome. De ce point de vue, le FTQC est plus comparable à l'exemple donné pour la recherche spatiale. On peut identifier des domaines d'applications, mais l'investissement massif sur un sujet incertain semble disproportionné par rapport à l'impact possible. Cependant, on ne peut connaître les évolutions à long terme, dans un monde où des machines quantiques existeraient. Les acteurs, états ou mégaentreprises, cherchent à rester en avance sur leurs concurrents par un raisonnement géostratégique dépassant le raisonnement économique court-termiste.

Le niveau d'incertitude est élevé et les filières possibles sont plus nombreuses que dans les exemples précédents, conduisant à une dispersion des moyens, qui devra cesser à l'étape de développement. Le niveau de dépense du capital-risque est de l'ordre de 1,2 milliard dans le monde en 2023, avec une baisse par rapport aux records de 2,35 milliards en 2021 et 2022 (il semblerait qu'une partie des investisseurs se reportent sur l'IA générative). Les états ont déjà dépensé plus d'une vingtaine de milliards. Sur un scénario optimiste d'une quinzaine d'années avant la première réalisation ayant une performance compétitive, un coût total mondial d'une cinquantaine de milliards semble une évaluation minimale.

Le programme spatial a été financé par les états. Le FTQC est partiellement financé par l'apport privé, d'une part des capitaux-risqueurs investissant dans les startups, d'autre part des groupes industriels disposant de liquidités massives. On peut certainement craindre que la première source ne s'épuise devant la distance de l'échéance. Pour la seconde, il faut supposer que ces supergroupes industriels ont des objectifs stratégiques sur des dizaines d'années. À la motivation stratégique, s'ajoute également la volonté de

recrutement de scientifiques brillants (voir ci-dessous). Si l'ampleur et l'incertitude de la tâche conduisaient à la remise en cause de l'objectif stratégique, le recrutement des cerveaux aura de toute manière renforcé ces groupes dont la compétitivité dépend de leur capital humain.

5.2.6. LE PROBLÈME DU *BRAIN DRAIN*

Malgré toutes les incertitudes sur les débouchés possibles du FTQC, ce sujet est extraordinairement attractif pour les jeunes de talent. Une motivation socio-économique à poursuivre un investissement sur le sujet est la crainte de l'évaporation définitive de ces talents si le sujet régresse en France alors qu'ils constituent une richesse, quelle que soit leur activité future. Les projets de la Silicon Valley ont été continûment un pôle d'attractivité pour les meilleurs chercheurs et ingénieurs mondiaux bien avant que les TICs ou l'IA ne concrétisent leurs promesses.

5.3. QUELQUES QUESTIONS

5.3.1. FAUT-IL PASSER PAR LE DÉVELOPPEMENT POUR ÉTABLIR LA FAISABILITÉ ?

Ici encore, c'est le spatial qui est l'exemple le plus proche. Dans les autres cas, des démonstrations technologiques à l'échelon recherche démontrent la faisabilité, même si les incertitudes sur les coûts et temps de développement peuvent rester majeures. De manière intéressante, la filière logique à semiconducteur d'IBM dans les années 1970 a montré un gap entre la faisabilité d'un ordinateur compétitif et des démonstrations de laboratoire ayant de très bonnes performances.

Il semble que pour la plupart des filières de réalisation d'un FTQC, l'objectif de performance sera difficile à atteindre sans un contexte de fabrication standardisée hors laboratoire: la faisabilité passe sans doute par le développement industriel. Paradoxalement, l'approche par nanotubes de carbone, la moins avancée actuellement en termes de résultats, a l'ambition de réaliser des itérations rapides en laboratoire pour créer un système complet dont les éléments individuels seraient suffisamment testés pour aboutir à la faisabilité. La conséquence de cette nécessité du développement

et passage à l'industriel est qu'il faudrait passer par un investissement massif, sans garantie de faisabilité.

5.3.2. EST-CE QU'UNE PREMIÈRE GÉNÉRATION À LA LIMITE DE L'AVANTAGE QUANTIQUE SERA UTILE ?

On peut en douter. L'apport risque d'être principalement scientifique. Ici encore, l'analogie avec le spatial s'impose : Spoutnik ne servait à rien. C'était la première marche vers des développements militaires et civils significatifs bien plus tard. Rappelons que dans l'ex-URSS, les lanceurs du programme spatial étaient un sous-produit du système de défense stratégique, bien plus grand.

5.3.3. VERTICALITÉ OU FILIÈRE ?

La réalisation d'un FTQC demandera non seulement une technologie de base capable de la performance, mais également des évolutions majeures dans les évolutions périphériques (communications, entrées/sorties, cryogénie...). Cela pose la question de la verticalité. En effet, si l'on peut envisager que l'industriel leader disposant de capacités financières importantes prenne des risques financiers, cela peut difficilement être le cas pour les industriels fournissant ces périphériques éminemment spécifiques.

Par exemple, les recherches d'IBM sont initialement faites en utilisant les réfrigérateurs à dilution de la Compagnie finlandaise Bluefors. Il apparaît que l'augmentation du nombre de qubits va conduire à des conceptions nouvelles de systèmes de cryogénie à haute puissance et haut rendement.

Bluefors peut-il effectuer ces recherches sur ses fonds propres ? IBM va-t-elle développer des réfrigérateurs en interne ? IBM va-t-elle acquérir Bluefors, privant le reste des acteurs de l'accès à ces technologies ?

L'exemple du spatial pointe vers la constitution d'une filière. La nécessité de multiples industriels périphériques rend difficile cette constitution à l'échelon national, le niveau européen étant le plus adéquat. La décision politique sera

d'autant plus difficile en raison de la grande variété des options techniques possibles, qui le resteront longtemps, et des incertitudes associées.

Comment cadrer l'investissement de R&D en termes de budget ? En l'absence de justification économique au départ, comment considère-t-on l'apport scientifique de la réalisation d'un FTQC par rapport, par exemple, au projet international du LHC du CERN ? Quel facteur multiplicatif rajouter pour l'espoir de retombées économiques ? La part R&D des développements spatiaux se compte en milliards, dont la plus grande part n'est pas autofinancée.

Si les startups innovatrices jouent aujourd'hui un grand rôle, est-ce qu'elles ont la capacité à s'intégrer dans le processus de développement, que ce soit en verticalité ou en filière ? On peut espérer qu'elles trouveront à valoriser le très grand capital intellectuel réuni dans des activités ayant un potentiel économique à plus court terme, avant que les investisseurs ne se découragent.

5.3.3.1. ÉVALUATION

Les activités actuelles visant à créer des *benchmarks* (voir §5.5.) sur l'avancement des FTQC auront l'avantage de contrer les fréquentes annonces de percées, qui masquent le fait que l'objectif est encore lointain et incertain. Même si ces *benchmarks* concernent des problèmes qui ont peu de chance d'être les débouchés finaux des FTQC, ils contribuent à maintenir une vision politique réaliste du domaine.

5.3.3.2. QUESTIONS GÉNÉRALES

D'un point de vue général, le FTQC à l'horizon de la vingtaine d'années est un projet dont les débouchés seront principalement scientifiques. Une première question est : est-ce que ces débouchés justifient l'investissement, avec pour référence les installations de physique des hautes énergies et la recherche spatiale ?

À l'échelon de quelques années, il est vraisemblable que la recherche sera principalement financée par les états, même si les groupes mécènes se maintiennent dans le sujet, plus longtemps que les capitaux-risqueurs. Pour un pays comme la France, il est douteux d'y voir l'avenir de la réindustrialisation. Cependant, le très bon niveau de la recherche française dans ce domaine,

à la fois dans les laboratoires industriels et les startups, pousse à poser la question suivante :

- Faut-il financer cette recherche pour contrer le *brain-drain* ?

Si on a réussi à contrer le *brain-drain* et si un débouché économique réel est découvert :

- Est-ce que ceux qui auront réalisé le développement auront un avantage décisif comme cela a été le cas pour la microélectronique silicium et internet et la suite, mais pas pour la microélectronique III-V ?

5.4. DÉVELOPPEMENT DES TECHNOLOGIES CONCURRENTES À L'HORIZON DES PREMIERS FTQC ?

La concurrence des ordinateurs quantiques viendra principalement des ordinateurs classiques qui vont progresser, comme par le passé, suivant trois axes, les technologies matérielles des circuits intégrés, leurs architectures et les logiciels, ces trois composantes ayant progressé en parallèle depuis l'origine³³⁵. Une nouvelle donne est apparue récemment avec les progrès fulgurants, quoique de nature différente, de l'intelligence artificielle.

Les circuits intégrés continuent à progresser, mais plus lentement que suivant la loi de Moore initiale, un doublement tous les deux ans environ du nombre de transistors des *central processing units* (CPU), unités de calculs universels. Cette croissance ne se fera pas comme au début grâce à une lithographie planaire de plus en plus fine. On est passé de largeurs de traits lithographiques de quelques microns à aujourd'hui des générations

335 John L. Hennessy and David A. Patterson, A New Golden Age for Computer Architecture, *Communications of the ACM* 62, 48 (2019)

lithographiques de l'ordre de 3 ou 2 nm³³⁶. Le gain initial en performance de calcul croissait comme le cube du facteur de diminution de taille, d'après les lois d'échelle de Dennard. La limite physique imposée par la tension minimale de commande du transistor à effet de champ a mené à un très net ralentissement de la diminution de la tension d'alimentation prévue, passant de 5V jusqu'à 1985 à 0,6V aujourd'hui, alors que les lois d'échelle auraient mené à une diminution de 60 fois, suivant l'évolution de la largeur de trait lithographique et les lois d'échelle. Autre conséquence: on atteint une limite pour la puissance électrique consommée, à 20 W ou 300 W pour les microprocesseurs d'ordinateurs portables ou fixes respectivement. Cette limitation de puissance joue un rôle dimensionnant dans les choix de composants (équilibre entre quantités de circuits logiques et mémoires sur un circuit) et les architectures. Malgré ces limitations apparues vers 2002, constituant la fin des lois de Dennard, ce qui a conduit à la stagnation de la vitesse d'horloge vers 3 GHz, il est prévu que le nombre de composants continue à augmenter grâce à des architectures 3D des composants, l'utilisation de nouveaux concepts de composants logiques et de mémoire, la multiplication de circuits spécialisés de grande efficacité pour une tâche précise sur une même puce, l'empilement de plaquettes de circuits permettant d'éviter la dissipation d'énergie nécessitée par les interconnexions à longue distance dans un plan. Le consensus des industriels, énoncé tous les deux ans dans les rapports de l'*International Roadmap on Devices and Systems* (IRDS)³³⁷, prévoit que l'augmentation des performances des puces continuera au même rythme pendant une douzaine d'années au moins, sans que cela signifie un arrêt au bout de cette période (c'est une constante de l'IRDS de ne pas prévoir les solutions au-delà d'une douzaine d'années), passant de plus de 100 milliards de transistors à plus de 1000 milliards.

336 En fait, la densité planaire des circuits n'augmente plus que très lentement: au lieu d'une diminution du trait lithographique d'un facteur 2 tous les quatre ans (multiplication par 4 de la densité, loi de Moore initiale), on n'a progressé que d'un facteur 3 en vingt ans (!), à cause des difficultés de fabrication. Il y a pourtant toujours plus d'intégration grâce à de nouvelles structures de transistors et architectures de circuits dans la dimension verticale, avec des dimensions qui ne sont plus liées à la lithographie. On a du coup introduit des générations « lithographiques » (7 nm, 5 nm, 3 nm, 2 nm, 1 nm) qui n'ont aucun lien avec la vraie largeur de trait (aujourd'hui de l'ordre de 12 nm), mais qui décrivent de nouvelles générations technologiques ayant des fonctionnalités équivalentes à celle de technologies planaires de 7 nm, 5 nm, 3 nm, 2 nm, 1 nm.

337 Disponible à <https://irds.ieee.org/editions>

L'arrivée récente de l'intelligence artificielle (IA) constitue une bien plus grande menace pour les applications du FTQC que les seuls progrès du hardware et des logiciels classiques: l'irruption de l'IA est due à la conjonction de deux composantes essentielles, le *big data* pour nourrir l'apprentissage des systèmes d'IA, et les réseaux de neurones profonds permettant d'améliorer grandement la précision des prédictions des premiers réseaux de neurones. Dans ce contexte, plutôt que résoudre exactement un problème à partir de la description d'un modèle, on construit, par entraînement à partir d'échantillons de données, un réseau de neurones qui constitue un modèle statistique du domaine dans lequel le problème est posé et approximativement résolu par inférence sur le réseau. L'usage de processeurs graphiques (GPU), munis d'opérations vectorielles ou matricielles, permet d'accélérer significativement l'entraînement et l'inférence des réseaux et le calcul optimisé des poids synaptiques. Cette tendance est renforcée par l'apparition de nouveaux processeurs spécialisés comme les NPU (*Neural Processing Unit*), d'Intel ou Apple par exemple, ou encore par l'émergence des processeurs neuromorphiques³³⁸ qui cherchent à imiter le cerveau humain. On obtient alors des outils extrêmement puissants pour aborder un très grand nombre de problèmes de manière statistique. Comme par ailleurs la puissance des processeurs spécialisés continue de progresser plus rapidement que celle des processeurs universels, les ordinateurs FTQC devront faire leur preuve dans un marché difficile pour eux. Par ailleurs, les méthodes d'apprentissage sont fondées sur l'utilisation de données archivées sur des mémoires de masse dotées par construction d'un accès lent. La quantité d'entrées/sorties sur ces mémoires ne prédisposent alors pas les processeurs quantiques à fournir une accélération significative.

Dès lors qu'on se contente de résultats statistiques et d'approximations et que l'on a pris les précautions nécessaires pour obtenir des résultats fiables, on obtient alors un outil extrêmement puissant pour aborder un très grand nombre de problèmes. Comme par ailleurs la puissance des GPU/NPU continue de progresser plus rapidement que celle des processeurs universels, les ordinateurs FTQC devront faire leurs preuves dans un marché

338 Cf. Rapport de l'Académie des technologies: *Les technologies matérielles supports du numérique futur – Trois questions 2022* (<https://www.academie-technologies.fr/publications/les-technologies-materielles-supports-du-numerique-futur-trois-questions/>)

difficile pour eux. Par ailleurs les méthodes d'apprentissage sont fondées sur l'utilisation de données archivées sur des mémoires de masse dotées par construction d'un accès lent. La quantité d'entrées/sorties sur ces mémoires ne prédisposent alors pas les processeurs quantiques à fournir une accélération significative.

Pour déterminer les applications futures où l'on considère que les ordinateurs quantiques seront incontournables, il est donc essentiel de prendre en compte les évolutions probables des technologies de processeur classique, de processeur spécialisé ainsi que les méthodologies d'apprentissage et d'en suivre en continu les progrès, car il va s'agir de pourchasser des cibles mouvantes. C'est essentiel pour ne pas disperser les efforts lorsqu'il s'agira de mettre en œuvre les premiers FTQC dans des applications pertinentes, dans dix à quinze ans.

5.5. BENCHMARKS ORIENTÉS APPLICATIONS

Avec le soutien du programme national de mesures, étalons et évaluation des technologies quantiques MetriQs-France du LNE, qui s'inscrit dans le cadre de la stratégie quantique nationale française, le projet BACQ est dédié aux *benchmarks* orientés applications pour l'informatique quantique. Le consortium réunissant Thales, Eviden, le CEA, le CNRS, Teratec et le LNE visent à établir des critères de référence en matière d'évaluation des performances, significatifs pour les utilisateurs industriels. Il s'agit pour le projet BACQ (*Benchmarks* applicatifs des calculateurs quantiques) de fournir une suite de *benchmarks* orientés applications pour une évaluation multicritère objective des performances de l'informatique quantique, clé des utilisations industrielles.

Mesurer les progrès vers l'avantage quantique et la réalisation de ses promesses, avec objectivité et fiabilité, présente un grand intérêt pour les utilisateurs finaux potentiels et est crucial pour le développement futur du domaine, désormais soumis à un battage médiatique et à une forte concurrence. Les défis, notamment pour réaliser 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 la potentielle évolution rapide des technologies.

Il existe un certain nombre d'initiatives pour comparer les performances des ordinateurs quantiques. Les exemples incluent 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 d'en dériver des indicateurs opérationnels de performance des différentes familles d'algorithmes exécutés sur les différents ordinateurs quantiques existants. Dédié à l'ensemble de la chaîne de valeur, depuis le développement du matériel quantique jusqu'aux cas d'utilisation industrielle, le projet BACQ est complémentaire des initiatives de *benchmarking* se concentrant uniquement sur des critères physiques de bas niveau du matériel. La suite de référence envisagée sera basée sur la résolution de plusieurs classes de problèmes couvrant des domaines d'application importants de l'informatique quantique qui sont significatifs pour les utilisateurs industriels: 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 types d'applications sont génériques et pourraient concerner 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 indépendants du matériel et d'autres dépendants du matériel (bas niveau): temps de calcul, latence, taille du problème, taux d'approximation, probabilité de résolution, précision, fidélité... Surtout, le projet prend également en compte les critères énergétiques pour l'évaluation des performances de consommation des machines.

La méthodologie proposée consiste en l'agrégation de métriques techniques de bas niveau et une analyse multicritère via l'outil MYRIAD-Q afin de fournir des indicateurs de performance opérationnelle des différentes solutions d'informatique quantique et de pointer les qualités de service intéressant 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 BACQ couvre également les machines basées sur des portes, en particulier le *Fault Tolerant Quantum Computing* (FTQC). L'approche pratique suivie

consiste à disposer d'une suite de *benchmarks*, adaptatifs dans une certaine mesure, adaptés aux capacités des machines disponibles et capables de démontrer leurs avantages respectifs, y compris, à plus long terme, une accélération exponentielle d'algorithmes spécifiques sur les machines FTQC.

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

Le partage de la suite de référence, aussi largement que possible, est un objectif important pour établir des méthodes de mesure de référence commune et garantir l'absence de biais avec l'inclusion de toutes les technologies. Les consultations des fournisseurs de technologies ainsi que des utilisateurs finaux sont essentielles pour développer un instrument qui répond aux besoins. Une fois spécifiée et développée, la suite de références sera disponible pour son utilisation par la communauté.

Pour parvenir à un outil universel, il faut établir une coopération avec des initiatives similaires dans le monde entier comme le font les séminaires TQCI (*Teratec Quantum Computing Initiative*) dédiés à l'« Aperçu des prochains *benchmarks* orientés applications pour l'informatique quantique en France et à l'étranger » qui sont organisés chaque année, par Teratec, Thales et le LNE. Un premier séminaire a été organisé en 2023 à Thales TRT à Palaiseau et un deuxième séminaire en 2024 à Reims.

La normalisation sera un autre moyen d'obtenir un consensus et une adoption à grande échelle, compte tenu des comités européens CEN-CENELEC JTC 22 WG3 sur l'informatique quantique et simulation, des comités internationaux ISO/IEC (JTC1 WG14 sur les technologies de l'information quantique et JTC-Q sur les technologies quantiques) et des groupes de travail IEEE (P7131 « QC Benchmarking », P3329 « Quantum Energy Initiative » et P3120 « Architectures for QC »).

En France, les normes sont prises en compte par AFNOR/CN QT sur les technologies quantiques.

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

L'évaluation des performances pratiques de l'informatique quantique sera envisagée à travers des *benchmarks* proches d'applications réelles, significatifs pour les utilisateurs finaux industriels (ainsi qu'académiques). L'objectif principal est de mesurer les progrès vers un avantage quantique pratique. À cet égard, il faut prévoir d'effectuer des comparaisons entre les différentes solutions informatiques quantiques ainsi que de les comparer avec les ordinateurs classiques actuels. Cette initiative d'analyse comparative permettra à terme de mettre en évidence les atouts de chaque solution d'informatique quantique selon des applications spécifiques.

La suite de *benchmarks* sera maintenue par le LNE, tiers indépendant et de confiance. Grâce à l'interaction avec la communauté des utilisateurs finaux, cet outil sera exploité afin d'analyser les résultats obtenus à partir des machines testées avec les différents *benchmarks* à l'aide de l'outil d'agrégation explicable. Le LNE établira un catalogue de performances, le maintiendra dans le temps et actualisera la définition des essais. Par ailleurs, l'appropriation de cette initiative par les partenaires français, européens et éventuellement internationaux sera favorisée grâce au développement d'outils de communication sur la démarche adoptée et de représentations visuelles de l'agrégation des résultats obtenus par les machines à partir des différents *benchmarks*. Les dialogues et collaborations internationales sur le sujet du *benchmarking* des ordinateurs quantiques seront favorisés afin que la démarche, portée par MetriQs-France, soit et reste une référence internationale. Le *benchmark* favorise le développement d'une normalisation internationale concernant les méthodes utilisées pour évaluer les spécifications des machines quantiques.

À travers le projet BACQ, des collaborations ont été initiées ainsi qu'un dialogue avec d'autres initiatives internationales d'analyse comparative: Fraunhofer IKS & FOKUS (Projet BenchQC) en Allemagne, TNO & TU Delft (Projet QPack) aux Pays-Bas, Qilimanjaro (Projet CUCO) en Espagne, QuIC (Use cases WG) en Europe, Projet HamLib (Intel, LBNL *et al.*) aux États-Unis, Fonds unitaire (projet Metriq) aux États-Unis et QED-C (QC Benchmarking WG) aux États-Unis.

Les résultats de *benchmarks* alimentent également les réflexions des initiatives de normalisation: Comité national AFNOR sur QT en France, CEN-CENELEC (JTC22 QT/WG3 Quantum Computing & Simulation) en Europe, ISO & IEC (JTC1/WG14, JTC3) au niveau international et IEEE (P7131 « QC Benchmarking », P3329 « Quantum Energy Initiative » et P3120 « Architectures for QC ») aux États-Unis.

La Commission européenne a mis en place l'EQCBC (*European Quantum Computing Benchmark Coordination Committee*) qui travaille sur un « *white paper* » qui sera prochainement publié sur le thème « *Systematic benchmarking of quantum computers: status and recommendations* ». Thales, le LNE et Alice&Bob sont co-auteurs pour la France de cette publication. L'EQCBC a pour objectif de coordonner les actions nationales de l'Union européenne, en particulier de la France, de l'Allemagne et des Pays-Bas pour favoriser l'émergence d'un *benchmark* européen des calculateurs quantiques.

5.5.1. RECOMMANDATIONS RELATIVES AU BENCHMARKING

- Utiliser le projet national BACQ (*Benchmarks* applicatifs des calculateurs quantiques) du programme MetriQs du LNE pour suivre l'évolution des performances des calculateurs quantiques FTQC.
- Coordonner les actions de *Benchmarks* pour les calculateurs FTQC au niveau européen, en favorisant les collaborations de la France avec l'Allemagne (Fraunhofer IKS) et les Pays-Bas (TNO).

5.5.2. RÉFÉRENCES BIBLIOGRAPHIQUES

Pour approfondir, on pourra consulter les références qui suivent :

BACQ: Application-oriented Benchmarks for Quantum Computing, *arXiv*: 2403.12205v1 [quant-ph]; <https://doi.org/10.48550/arXiv.2403.12205>

Bench-QC: *Application-driven benchmarking of quantum computers*, Fraunhofer Institute IKS, Germany; <https://www.iks.fraunhofer.de/en/projects/bench-qc-application-driven-benchmarking-of-quantum-computers.html>

QPack: *Benchmark for quantum computing*. Delft University of Technology, Delft, The Netherlands; <https://github.com/koenmesman/QPack?tab=readme-ov-file>

CUCO project '*Computacion Cuantica En Industrias Estrategicas*', Spain; <https://www.cuco.tech/en/project/>

Metriq "*Community-driven quantum benchmarks*", Unitary Fund; <https://metriq.info/>

QED-C benchmark; <https://github.com/SRI-International/QC-App-Oriented-Benchmarks>

DARPA QBI (*Quantum Benchmarking Initiative*); <https://www.darpa.mil/news-events/2024-07-16>; <https://www.darpa.mil/news-events/2024-08-15>

HamLib: A library of Hamiltonians for benchmarking quantum algorithms and hardware, in 2023 IEEE International Conference on Quantum Computing and Engineering (QCE), 2023. *arXiv*: 2306.13126v3 [quant-ph]; <https://doi.org/10.48550/arXiv.2306.13126>

E. Vergnaud, F. Schopfer, F. Barbaresco, first TQCI Seminar "Overview of upcoming application-oriented benchmarks for quantum computing in France and abroad", Thales Research & Technology, Palaiseau, France, 11 May 2023; https://teratec.eu/Seminaires/TQCI/2023/Seminaire_TQCI-230511.html

E. Vergnaud, F. Schopfer, F. Barbaresco, 2nd TQCI Seminar "Overview of upcoming application-oriented benchmarks for quantum computing in France and abroad", 4th & 5 June 2024, Reims, France; https://teratec.eu/activites_quantiques/TQCI_240604_programme.html

Jeanette Mirian Lorenz, Thomas Monz, Jens Eisert, Daniel Reitzner, Félicien Schopfer, Frédéric Barbaresco, Krzysztof Kurowski, Ward Van Der Schoot, Thomas Strohm, Cécile M. Perrault, Martin Knufinke, Systematic benchmarking of quantum computers : status and recommendations, EQCBC (European Quantum Computing Benchmark Coordination Committee) preprint, to be published

Anastasiia Butko, Katherine Klymko, Daan Camps, Nicolas Sawaya Authors Info & Claims, HamPerf: A Hamiltonian-Oriented Approach to Quantum Benchmarking, CF '24 Companion: Proceedings of the 21st ACM International Conference on Computing Frontiers: Workshops and Special Sessions, Pages 133-138; <https://doi.org/10.1145/3637543.3653431>

5.6. LIENS AVEC LE CALCUL HAUTE PERFORMANCE

On emploiera le terme de HPC (*High Performance Computing*, calcul haute performance) pour « calcul classique », avec le sens général de « moyen de calcul allant au-delà des équipements standard tels que des stations de bureau ou ordinateurs portables », jusqu'à des échelles extrêmes en centres de calcul spécialisés (à l'heure actuelle, « exascale » pour les plus grands systèmes)³³⁹.

Un système de calcul quantique a besoin d'une informatique de contrôle classique, en quelque sorte bas niveau, proche de l'électronique de contrôle des composants du système. Nous l'excluons du champ du HPC.

Le HPC peut intervenir à trois niveaux, en rapport avec le calcul quantique :

1. En tant que ressource et méthode de simulation/émulation de systèmes quantiques, dont des circuits quantiques;

339 Top 500 : <https://top500.org/>

2. En tant que moyen d'effectuer des traitements auxiliaires du calcul quantique, typiquement en lien avec la correction d'erreur ou la compilation ;
3. En tant que co-traitement de certains problèmes pouvant combiner une partie d'algorithme classique et une partie quantique (calcul « hybride »).

En général on pense, en parlant combinaison FTQC/HPC, au troisième niveau, mais il nous semble utile de brièvement commenter les autres situations, tant les destins du calcul classique et quantique semblent durablement liés.

5.6.1. ÉMULATION/SIMULATION

De manière générale les systèmes physiques modélisés de manière quantique peuvent bénéficier de simulation HPC, en particulier les qubits constitutifs de circuits et portes quantiques. À l'heure actuelle les simulations les plus abouties traitent de l'ordre de 55 qubits de manière exacte (en mode « vecteur d'état », et de l'ordre de quelques centaines avec des approximations (à base de réseaux de tenseurs) - les calculs les plus grands réalisés sont de classe quasiment exascale. On peut ainsi atteindre certaines connaissances du fonctionnement espéré de calculateurs ou algorithmes quantiques.

Des approches par matériel et logiciel spécialisés permettent de rendre ce type de démarche plus abordable, et d'émuler des calculateurs quantiques jusqu'à quelques dizaines de qubits sans mobiliser les plus grands calculateurs HPC. La mémoire d'un cluster de calcul dédié à une telle approche est le premier facteur dimensionnant (*a priori* chaque qubit supplémentaire demande de doubler la mémoire). De tels clusters bénéficient des méthodes HPC pour les approches SMP (clusters de calcul à large mémoire partagée) et peuvent aussi comporter des GPU pour accélérer les traitements. C'est le cas par exemple des systèmes Qaptiva d'EVIDEN, « appliances HPC » pouvant de plus émuler des bruits et erreurs, dans des formats physiques très compacts de l'ordre d'une armoire de calcul. (Qaptiva émule jusqu'à 41 qubits en mode vecteur d'état et au-delà de 75 qubits en mode bruité)³⁴⁰.

340 Qaptiva™ - Atos (<https://atos.net/en/solutions/high-performance-computing-hpc/quantum-computing-qaptiva>)

On peut aussi citer l'émulateur Hyperion de Qubit Pharmaceutical, qui s'appuie sur des serveurs Nvidia DGX et supporte jusqu'à 40 qubits en mode vecteur d'état³⁴¹. Ce type de démarche permet d'exécuter virtuellement des programmes quantiques complets, FTQC idéaux, voire bruités, et de les préparer et mettre au point en l'absence ou en avance de la disponibilité de calculateur quantique FTQC. Un environnement convenablement constitué permet de basculer du mode émulation en mode réel à partir des mêmes codes quantiques source et intermédiaire.

Par définition, ces approches de calcul seront dépassées par l'obtention d'un réel avantage quantique, non simulables/émulables classiquement en pratique. Mais elles conserveront toujours un intérêt, pour étudier et mettre au point des séquences et algorithmes quantiques, notamment pour observer l'évolution des données internes au calcul pendant celui-ci, ce qui n'est pas possible sur un ordinateur quantique.

5.6.2. TRAITEMENTS AUXILIAIRES

Comme signalé dans le § 3.2.3, le traitement des données pour correction des erreurs (détection des syndromes d'erreur) peut être très intense et requerra des optimisations matérielles classiques, comme l'adjonction de GPU, FPGA voire ASIC dédiés au plus près des traitements quantiques. La société Riverlane est un exemple d'acteur focalisé sur cet aspect³⁴².

L'organisation des séquences de calculs quantiques réalistes peut aussi nécessiter de décomposer et compiler/transpiler des circuits ou portions de circuits à la volée, pour des approches itératives par nature ou parce qu'un circuit complexe ne tient pas en une seule passe d'exécution (limites physiques des largeur et profondeur de circuits réalisables). Ceci peut aussi nécessiter de dédier des moyens classiques de calcul. Ce d'autant plus que

341 Qubit Pharmaceuticals and Sorbonne University achieve a major scientific breakthrough by simulating quantum calculations at more than 40 qubits on conventional computers | Sorbonne Université | Sorbonne université (sorbonne-universite.fr) — <https://www.sorbonne-universite.fr/en/presse/qubit-pharmaceuticals-and-sorbonne-university-achieve-major-scientific-breakthrough>

342 <https://www.riverlane.com/quantum-error-correction-stack>

la compilation, qui intègre la transpilation et l'optimisation, représente un coût variable d'exploitation, contrairement au calcul classique où c'est en général un coût fixe. Le calcul quantique étant l'équivalent du «*in-memory processing*» avec un chargement des données réalisé avec des portes quantiques directement intégrées dans le corps de l'algorithme (*ansatz* d'un algorithme variationnel, hamiltonien utilisé dans l'exponentiation d'une estimation de phase), le code est quasiment systématiquement spécifique au jeu de données utilisé, à l'exception des algorithmes à base d'oracles faisant appel à un accès mémoire qRAM accédant à des données classiques.

Ces moyens et approches s'apparentent au HPC, mais dans une variante «*embarquée*», où le HPC est subordonné au système quantique, pour en assurer une précision suffisante. Au-delà des servitudes de contrôle de bas niveau, et avant de parler de calcul réellement hybride, le calcul quantique a besoin d'une telle logique classique intégrée au plus près.

Cela explique par exemple les partenariats entre Nvidia, Quantum Machines et Alice&Bob. Sur des ordinateurs FTQC de grande taille, il n'est pas exclu qu'il faille leur adjoindre des clusters avec un grand nombre de ces serveurs DGX ou équivalents.

5.6.3. CALCUL HYBRIDE HPC/FTQC

On parle ici d'hybridation au niveau des traitements algorithmiques, en quelque sorte à parité entre calcul classique et quantique, chacun invoqué là où il est le plus adapté pour concourir à l'exécution d'une tâche: deux modèles de calcul radicalement différents cohabitent. La raison en est pragmatique, on cherche à utiliser à l'optimum les ressources: problèmes «*durs*» abordés par le quantique, servitudes et parties plus conventionnelles traitées classiquement, car le quantique y serait inefficace ou «*gaspillé*». Elle est aussi liée à la nature même de certains algorithmes quantiques, comme l'estimation de phase qui nécessite une préparation classique assez coûteuse à effectuer (à base, par exemple, de méthode DFT).

Les granularités et couplages en espace et en temps des découpages et répartitions de rôles sont variables, à ce jour pressentis dans de nombreux cas, mais en pratique encore peu ou pas expérimentés.

Les formes les plus simples sont, par exemple, le cas des algorithmes de Shor ou Simon, avec des pré- et post-traitements classiques des données, avec un noyau quantique « simple » de traitement. Ceci n'est pas une hybridation très imbriquée, mais illustre encore le caractère indissociable en pratique HPC/FTQC.

L'hybridation est plus marquée dans le cas des algorithmes quantiques variationnels (VQE, QAOA, QML). La vision est ici celle d'un processeur (ou cluster) classique qui appelle un (co-)processeur quantique pour résoudre un sous-problème et optimiser une fonction de coût de manière itérative, la logique générale, mais aussi des traitements significatifs de la résolution, étant prise en compte classiquement.

En fait l'algorithme de Shor est très hybride, il comporte beaucoup d'arithmétique classique au sens d'une boucle globale de recherche de facteurs et utilise le quantique dans chaque boucle uniquement pour une estimation de période de fonction (à base d'exponentiation modulaire et d'une QFT inverse, le coût en calcul quantique étant concentré dans l'exponentiation modulaire).

L'approche VQE peut servir en chimie quantique, simulation quantique et optimisation. Il s'agit d'un algorithme qui alterne classique et quantique pour trouver l'état (en général fondamental) d'un système physique donné. À partir d'une supposition, le processeur quantique calcule la valeur d'espérance du système par rapport à une observable, souvent l'hamiltonien, et un optimiseur classique est utilisé pour améliorer l'estimation en modifiant les paramètres du circuit quantique (dit « *ansatz* »).

L'approche similaire QAOA exprime des problèmes d'optimisation en termes de recherche de la configuration d'énergie la plus élevée d'un hamiltonien de spin, et alterne également optimisation classique de paramètres avec estimation quantique de fonction de coût.

Dès lors que ce type d'approche est visée, on retrouve une bonne partie des éléments du HPC :

- gestion des ressources de calcul en environnement de partage de ces ressources (allocation des CPU/GPU [*PU] et QPU, leur disponibilité, l'ordonnancement des tâches;
- communication entre *PU - CPU, GPU... - classiques et QPU;
- modes d'expression des alternances classique/quantique - la logique générale utilise un langage de programmation classique, qui peut être augmenté quantiquement par des directives [pragma] ou faire des appels à des bibliothèques spécialisées;
- support d'exécution [*runtime*] sous-jacent.

Dans le cadre du FTQC, les simulations chimiques à base de l'algorithme d'estimation de phase [QPE] nécessitent un précalcul classique significatif. En effet, il faut alimenter l'algorithme quantique avec une estimation calculée classiquement qui soit aussi proche que possible du résultat recherché. Plus ce calcul est précis, plus il coûte cher classiquement. Et moins ce calcul est précis, plus le calcul quantique va diverger de manière probabiliste du résultat recherché.

À ce jour de nombreux travaux et expériences sont développés, mais il n'y a pas encore de solutions et approches standardisées claires qui se dégagent.

Notons également qu'à ce stade de développement précoce, les processeurs classiques et quantiques sont empaquetés et configurés dans des systèmes distincts [baies, châssis...]. Des applications hybrides peuvent certainement s'accommoder de connexions « distantes » avec des *workflows* s'exécutant pour partie sur des sites différents, dès lors que les échanges de données sont limités et sans criticité de délai. Mais la localisation des *PU et QPU sur un même site HPC présente des avantages indéniables :

- passage à l'échelle des communications facilitées si nécessaire par réseau local;
- maintenance conjointe facilitée des systèmes;
- sécurité informatique commune dans la bulle HPC du centre de calcul.

En conclusion rapide de cette section, la cohabitation traitement classique/ traitement quantique est là pour longtemps. Dans sa forme d'hybridation HPC/FTQC à un niveau algorithmique et applicatif, beaucoup de développements et d'expérimentations sont encore à venir :

- développement de *middleware* [intergiciel] et adaptation des piles logicielles HPC+QC.
- expérimentations et retours d'expérience sur les différentes implémentations de qubits, au fur et à mesure de leur maturation et disponibilité, en environnement HPC « de production ». En effet l'adéquation possiblement variable des technologies de qubits aux applications visées doit être mieux comprise, ainsi que le détail des comportements en particulier temporels des qubits et circuits, avec impact sur la manière de coupler au calcul classique, suivant les durées et latences de préparation et d'exécution de circuits, comparativement aux durées des boucles et tâches de calcul HPC.

5.7. CAPITAL HUMAIN

Pour accompagner et accélérer le développement du FTQC en France, le capital humain est un axe essentiel. Il faut adapter et développer des formations afin d'être cohérent avec le besoin croissant de compétences en technologies quantiques, que ce soit en ingénieures et ingénieurs, chercheuses et chercheurs, enseignantes-chercheuses et enseignants-chercheurs, techniciennes et techniciens, manageuses et managers. Il s'agit de développer des formations initiales ou d'inclure de nouveaux modules dans les formations existantes, mais aussi de développer des formations continues, en partenariat avec la formation professionnelle et les acteurs industriels: les technologies quantiques créent en effet un besoin renouvelé de formation tout au long de la vie afin de se former ou reformer aux fondamentaux de la physique quantique ou aux évolutions constantes en technologies quantiques. Il faut créer, comme l'a déjà initié le projet QuantEdu France financé par France 2030, une forte dynamique de formation entre les acteurs de la formation, de la recherche et de l'industrie.

En outre, la main-d'œuvre qualifiée en informatique quantique, qu'il s'agisse d'ingénierie logicielle ou de recherche en physique, mathématiques,

informatique, est rare. Dans certains domaines, comme la correction d'erreurs, le besoin excède largement les ressources humaines disponibles. Cette tension encourage un phénomène de guerre des talents, qui a lieu aussi bien entre les différents acteurs d'une même région [entre le secteur académique et les entreprises, ou bien entre entreprises] qu'entre différentes régions du monde, au premier chef entre l'Europe et l'Amérique du Nord. Dans cet environnement très compétitif, un écosystème bien développé et dynamique de startups, de grands groupes industriels et d'universités est indispensable pour attirer et garder des personnes compétentes, et ce d'autant plus qu'il est difficile pour certains acteurs de proposer des salaires compétitifs avec d'autres régions du monde. À ce titre, les pôles régionaux qui fédèrent les acteurs présents sur un territoire, comme les maisons du quantique, peuvent constituer un atout. Une analyse plus détaillée sera réalisée en 2025 et développée dans la nouvelle version du rapport.

5.8. STRATÉGIES DE FINANCEMENT

Les investissements publics et privés dans l'informatique quantique en France sont relativement importants et répondent à des logiques variées. Il est crucial de bien les comprendre et de comparer la situation française au reste de l'Europe et à l'international pour évaluer la performance de l'action publique à cet égard. Remarquons toutefois que la France s'est dotée au printemps 2024 d'un programme de financement spécifique pour le FTQC, dénommé PROQCIMA.

PROQCIMA : un outil original de financement de l'innovation de rupture pour la France

Financé par le plan « France 2030 » du Secrétariat général pour l'investissement et placé sous le pilotage de l'Agence numérique de défense [AND] [rattaché à la Direction générale de l'armement, ministère de la Défense], PROQCIMA permettra de disposer, d'ici 2032, de deux prototypes d'ordinateur quantique tolérant aux fautes avec 128 qubits logiques. Doté de 500 M€, PROQCIMA met en place des accords-cadres, sur une durée longue [plus de huit ans], avec les cinq startups issues de la recherche française, développant chacune une technologie spécifique : Alice&Bob, C12, Pasqal, Quandela et Quobly. PROQCIMA prend la forme d'une compétition permettant de sélectionner les technologies les plus performantes en trois étapes :

- en 2028, seules les trois technologies les plus performantes continueront de bénéficier du financement de PROQCIMA pour développer les meilleurs qubits capables de passer à l'échelle;
- en 2032, seuls deux prototypes de calculateurs à 128 qubits logiques [tolérants aux fautes] seront retenus;
- en 2035, l'ambition est le passage à l'échelle industrielle avec 2048 qubits logiques.

Dans un contexte où il est impossible, dans l'état des connaissances, de sélectionner les technologies qui seront les plus performantes à terme, ce qui devrait nécessiter des programmes de recherche et de développements importants dans la durée, PROQCIMA permet de remettre les compétiteurs sur la même ligne de départ, de ne pas disperser les financements publics s'agissant du FTQC en France, d'assumer une gouvernance simplifiée via l'AND et de confirmer la nécessité de démontrer le passage à l'échelle industrielle, en acceptant le risque de l'échec.

Conclusion

Le groupe de travail, créé mi-2023, a initialisé une réflexion collective impliquant une grande partie de l'écosystème français autour de l'Académie des technologies. La masse d'informations et de données collectées a permis d'identifier des défis scientifiques et techniques essentiels, tels que, le passage à l'échelle avec la qualité et la quantité nécessaire des qubits physiques, la mise au point des codes correcteurs d'erreur et l'interconnexion de ces éléments.

Il reste notamment à analyser l'état d'avancement du développement d'algorithmes et d'applications, ainsi que des environnements de compilation. Il en est de même pour l'architecture technique des systèmes à construire. Les défis économiques, tels que les coûts et la création de valeur, les technologies habilitantes, les rôles respectifs des différents acteurs publics et privés, la comparaison avec les autres dynamiques européennes et internationales ainsi que les besoins en compétences restent à explorer plus en profondeur.

Pour faire en sorte que des ordinateurs quantiques tolérants aux fautes soient une réalité à terme, de nombreux progrès scientifiques et techniques sont encore nécessaires, notamment pour fonder des stratégies industrielles réalistes.

Il est donc essentiel de poursuivre la réflexion collective, de compléter et de mettre à jour régulièrement les informations collectées pour garantir une compréhension complète et actualisée des enjeux liés au calcul quantique tolérant aux fautes. Un deuxième rapport sera rédigé en 2026.

Annexes

A. Glossaire

Algorithme : méthode de résolution de problème qui est faite d'une suite finie d'opérations ou d'instructions. Le mot vient du nom du mathématicien perse du IX^e siècle, Al-Khwârizmî.

Algorithme quantique hybride : algorithme qui associe des traitements classiques dans des ordinateurs traditionnels et des traitements réalisés sur ordinateurs quantiques, là où ils sont nécessaires.

Algorithme variationnel : algorithme hybride quantique générique utilisant un optimiseur classique qui est utilisé pour entraîner un circuit quantique paramétré. Ses variantes sont VQE [*variational quantum eigensolver*] pour la simulation chimique, QML ou quantum machine learning et QAOA [*Quantum Approximate Optimization Algorithm quantum*] pour les optimisations.

AOD : *Acousto-optic deflector* déflecteur acousto-optique de lumière qui modifie l'orientation des faisceaux de lumière pour créer des pinces optiques servant à déplacer et piéger à volonté les atomes dans le vide, et en général dans des structures géométriques à deux dimensions.

ASIC : *Application-Specific Integrated Circuit*, circuit intégré spécifique à une application, un type de circuit électronique conçu et optimisé pour réaliser une tâche ou une application particulière. Il est spécialement fabriqué pour répondre aux besoins d'une seule application ou d'un ensemble d'applications spécifiques. Cela le rend extrêmement efficace en termes de vitesse, de consommation d'énergie et de coût par unité une fois produit en masse. Les ASIC pourraient remplacer les FPGA pour le contrôle électronique des qubits, notamment supraconducteurs.

Atomes de Rydberg : état excité d'un atome ayant un ou plusieurs électrons et dont le nombre quantique principal n (indice de la couche d'électrons dans

l'atome qui est un entier compris entre 1 et le nombre de couches d'électrons dans l'atome) est élevé, au-delà d'une dizaine. Les transitions entre niveaux sont dans le domaine hyperfréquence, et ils sont donc manipulés dans ce domaine de fréquences.

Atomes froids: atomes refroidis à très basse température, en général avec des techniques utilisant des lasers et l'effet Doppler. Ils sont utilisés dans certains types d'ordinateurs quantiques dits à atomes froids. Les atomes utilisés sont des atomes neutres (pas ionisés) et assez souvent, le rubidium, un métal alcalin.

Avantage quantique: intervient lorsqu'un ordinateur quantique exécute un traitement plus rapidement que son équivalent optimum adapté à un supercalculateur. Cet avantage peut être décliné sur un autre aspect que la durée du calcul. Ainsi, un avantage énergétique quantique porte sur la consommation d'énergie en lieu et place du temps de calcul.

BACQ: *Benchmarks* applicatifs des calculateurs quantiques.

Blueprint: feuille de route d'un fournisseur de technologie sur les années à venir.

Boson (simulation): résolution d'un problème de physique quantique avec du calcul quantique ou un simulateur quantique analogique.

BPP: *Bounded-error Probabilistic Polynomial*, classe de problèmes décisionnels résoluble par un algorithme probabiliste classique fonctionnant en temps polynomial avec un taux d'erreur borné.

BQP (classe de problème): classe de complexité des problèmes qui peuvent être traités par des algorithmes quantiques. Signifie « *bounded-error quantum polynomial time* ». C'est la classe des problèmes qui peuvent être résolus en temps polynomial par rapport à la taille du problème avec une probabilité d'obtenir une erreur ne dépassant pas le tiers des résultats. Cette classe est comprise entre la classe P (problèmes qui peuvent être résolus en temps polynomial sur machine classique) et NP (problèmes dont on peut vérifier une solution en temps polynomial sur une machine classique).

Break-even: seuil à partir duquel avec un code de correction d'erreur quantique donné, on obtient des qubits logiques ayant un taux d'erreur inférieur au taux d'erreur de ses qubits physiques.

Chiplet: circuit intégré spécialisé, généralement intégré à l'intérieur d'un même boîtier. Contrairement à une puce monolithique traditionnelle qui regroupe toutes les fonctions, un système à chiplet répartit les fonctions entre plusieurs modules semiconducteurs indépendants, chacun étant optimisé pour une tâche spécifique (calcul, mémoire, communication, etc.).

Circulateur: isolateur à trois entrées qui permet d'éviter que le signal amplifié par un TWPA après la lecture d'un qubit vienne perturber le qubit mesuré.

CLOPS: *Cycle Layer Operations Per Seconds*. Nombre de cycles de portes quantiques qu'un ordinateur quantique peut exécuter par secondes. Dans les ordinateurs quantiques d'IBM de 2024, il est de l'ordre de 4000 cycles par seconde.

Cluster state: base de départ d'un calcul MBQC (*Measurement Based Quantum Computing*) avec un ensemble de qubits intriqués sur lequel sont ensuite réalisées de mesures.

Cluster states: se dit d'états intriqués de n-qubits.

CMOS: technique de fabrication courante de semiconducteurs utilisée pour produire des processeurs et de la mémoire, et qui est réutilisée pour créer des qubits manipulant des spins d'électrons.

CNOT: porte à deux qubits qui inverse le signe du second qubit cible en fonction de celui du qubit de contrôle.

Code bosonique: système matériel qui met en œuvre une correction d'erreur intégrée grâce à l'usage de modes bosoniques, qui sont des oscillateurs harmoniques quantiques avec des niveaux continus d'énergie. Cela comprend les *cat-codes* et les qubits GKP.

Code de surface: type de code de correction d'erreurs quantique qui supporte des erreurs relativement élevées et est adapté aux structures de qubits en deux dimensions où les qubits sont reliés à leur plus proche voisin.

Codes de correction d'erreurs: décrit à la fois les méthodes logiques et architectures physiques permettant de contourner les erreurs générées par le bruit dans le calcul quantique universel et une variante de cryptographie post-quantique.

CPU: *Central Processing Unit*, Unité centrale de traitement des ordinateurs classiques

Crosstalk: décohérence qui relève de l'influence de qubits sur des qubits voisins ou distants, que ce soit par des signaux électroniques de pilotage ou des interactions physiques entre qubits.

Cryo-CMOS: circuit électronique CMOS en silicium conçu pour fonctionner à très basse température. Il sert généralement à assurer une partie du contrôle électronique de qubits qui sont situés sur une autre puce.

Cryogénie: technique de refroidissement. La cryogénie à très basse température est utilisée dans une bonne partie des ordinateurs quantiques, tous ceux qui sont à base d'électrons ou d'atomes froids. Les températures requises pour stabiliser des qubits et réduire leur taux d'erreur sont très proches du zéro absolu: entre 5 et 20 mK. Les systèmes les plus utilisés sont des réfrigérateurs à dilution qui exploitent de l'hélium 3 et de l'hélium 4. La cryogénie est aussi utilisée pour les systèmes de lecture à bas bruit et haut rendement de qubits à base de photons ainsi que pour la génération de photons.

Décohérence: marque la fin de la cohérence d'un objet quantique ou d'un qubit, c'est-à-dire de la mémoire de son état quantique initial. Elle est notamment provoquée par les interactions entre les qubits et leur environnement. On utilise souvent indifféremment l'expression temps de cohérence (temps pendant lequel les qubits sont en état de superposition et d'intrication avec d'autres qubits) ou de décohérence (temps au bout duquel cette superposition et l'intrication se terminent), ce qui revient au même.

Diaphonie : voir *crosstalk*.

Dilution : partie d'un cryostat qui permet de descendre à une température d'environ 15 mK utilisée pour refroidir les puces de qubits supraconducteurs.

Émulateur quantique : système logiciel et/ou matériel utilisant un ordinateur classique servant à exécuter un logiciel destiné à un ordinateur quantique. Cela permet de faire des tests de programmes quantiques sans disposer d'ordinateur quantique. La vitesse d'exécution est moins bonne que sur un calculateur quantique, surtout dès que l'on dépasse quelques dizaines de qubits. Et au-delà d'une cinquantaine de qubits, la capacité des machines classiques est insuffisante pour réaliser ce genre d'émulation. Il ne faut pas confondre l'émulation avec la simulation quantique. Cette dernière simule des phénomènes de physique quantique avec un ordinateur quantique analogique.

FBQC : *Fusion-Based Quantum Computation*, variante de méthode de calcul par la mesure utilisée en photonique et proposée par la société PsiQuantum. Il repose sur des états de clusters regroupant des photons intriqués sur lesquels le calcul a lieu par des mesures successives de photons et sur des fusions entre clusters qui consistent à faire des tests de Bell entre clusters, équivalents à des portes à deux qubits générant une intrication.

Fidélité : caractérise en pourcentage la probabilité d'obtenir un résultat correct sur une opération sur des qubits. Se dit d'une action telle que l'initialisation d'un qubit, une porte quantique à un ou deux qubits, et la mesure de l'état d'un qubit. On s'intéresse en général aux fidélités des portes à deux qubits qui sont les plus basses par rapport aux fidélités des portes à un qubit qui sont toujours meilleures. La fidélité de la lecture conditionne la qualité des résultats du calcul ainsi que l'efficacité de la correction d'erreurs qui repose aussi sur des mesures.

Figure de mérite : indicateur caractérisant un système. Une fidélité d'une porte à deux qubits caractérise une puce de qubits.

Fluxonium : type de qubit supraconducteur.

FPGA: *Field-Programmable Gate Array*, circuit intégré qui peut être configuré après sa fabrication, contrairement aux circuits ASIC (*Application-Specific Integrated Circuit*), qui sont conçus pour exécuter une tâche fixe. Un FPGA est constitué d'un réseau de blocs logiques programmables interconnectés, ce qui lui permet d'exécuter presque n'importe quel algorithme numérique en fonction de la configuration appliquée. Ces circuits sont cependant moins performants que les ASIC d'un point de vue de la vitesse de calcul et de l'efficacité énergétique.

FTQC: *Fault-Tolerant Quantum Computer*. Ordinateur quantique résistant aux fautes. *A priori*, avec un très grand nombre de qubits et des codes de correction d'erreurs.

GHZ: état superposé Greenberger-Horne-Zeilinger à trois qubits ou plus qui permet de démontrer l'inexistence de variables cachées dans l'intrication quantique d'au moins trois particules et avec un nombre fini de mesures. La notion date de 1989 et sa validation expérimentale de 1999.

GKP: type de qubit bosonique autocorrigé. Corrige en même temps l'erreur de flip et l'erreur de phase du qubit.

Grover (algorithme): algorithme quantique de recherche d'un élément dans un tableau non indexé.

Hadamard (porte): porte permettant de générer un état superposé entre 0 et 1 dans un qubit.

Heuristique: méthode utilisée pour résoudre des problèmes de manière pratique, rapide et approximative, lorsque des solutions exactes ou optimales sont difficiles ou impossibles à trouver dans un délai raisonnable.

Hilbert (espace): espace vectoriel réel ou complexe muni d'un produit scalaire euclidien ou hermitien, qui sert à mesurer des distances et des angles et de définir une orthogonalité. C'est une généralisation du concept d'espace euclidien à trois dimensions. En mécanique quantique, l'état d'un quantum est représenté par un vecteur dans un espace de Hilbert à autant de dimensions que le nombre d'états de base (ou observables) de ce quantum. Il s'agit d'espaces géométriques qui servent notamment à mesurer

des longueurs et des angles généralisés, de faire des projections sur des dimensions et de définir l'orthogonalité entre « vecteurs » abstraits.

HHL: *Harrow-Hassidim-Lloyd*, algorithme quantique de résolution d'équation linéaire.

HPC: *High-Performance Computing*.

Intrication: liaison entre deux objets quantiques qui sont reliés entre eux de telle sorte qu'une modification de l'un entraîne celle de l'autre. Ce processus est utilisé pour relier des qubits entre eux par des portes quantiques à deux ou trois qubits dans les ordinateurs quantiques. Il l'est également dans les systèmes de cryptographie et de télécommunications quantiques à base de photons intriqués, exploités dans les QKD. Leur mesure est corrélée, mais aléatoire. L'intrication ne permet pas de définir une information à un point A et de l'intriquer avec B. Par contre, on peut s'appuyer sur une intrication pour téléporter l'état d'un qubit d'un point A à un point B. Comme cela nécessite l'emploi de deux canaux d'informations bits classiques en plus du canal optique de l'intrication, l'information sur le qubit ne peut pas être transmise plus vite que la lumière.

Ion: atome non neutre, qui a une charge électrique positive ou négative. Elle est négative si son nombre d'électrons dépasse celui des protons (anions) et positive dans le cas contraire (cations).

Ion piégé: ce sont des ions utilisés dans certains types d'ordinateurs quantiques. Ils sont généralement piégés magnétiquement ou électriquement et on contrôle leur état avec des lasers.

Josephson (effet): effet supraconducteur utilisé dans les qubits d'ordinateurs quantiques dits à supraconducteurs comme ceux d'IBM et Google.

LDPC: *Low-Density Parity Check*, code de correction d'erreur classique utilisé pour transmettre des données de manière fiable sur des canaux de communication bruyants. Ces codes sont appelés « à faible densité de parité », car leur matrice de contrôle de parité possède un faible nombre d'éléments non nuls, ce qui les rend efficaces à traiter en termes de calcul. Leur équivalent quantique est le qLDPC.

MAXCUT: problème d'optimisation combinatoire consistant à diviser les sommets d'un graphe en deux sous-ensembles distincts de manière à maximiser le nombre (ou le poids) des arêtes reliant ces deux sous-ensembles.

MBQC ou **MQCM**: *Measurement Based Quantum Computing*, méthode de calcul quantique inventée en 2001 par Robert Raussendorf et Hans Briegel qui utilise un nombre élevé de qubits intriqués dans des grilles à deux dimensions et dans lesquelles des lectures d'état de qubits sont réalisées pour modifier la structure de la grille. Ces mesures servent aussi à guider l'algorithme.

MOT: piège magnéto-optique, qui sert à piéger des atomes froids dans une chambre à vide à l'aide de lasers.

NISQ: *Noisy Intermediate-Scale Quantum*, dénomination des calculateurs quantiques actuels et à venir dans un futur proche, qui sont de taille intermédiaire en nombre de qubits (quelques dizaines à centaines) et sujets à un bruit quantique qui en limite les capacités. Cette appellation a été créée par le chercheur américain John Preskill.

NP (classe de problème): classe de problèmes dont la solution est vérifiable dans un temps polynomial relativement à la taille du problème. Comprend notamment les problèmes dits exponentiels ou intraitables, dont le temps de la résolution est exponentiel par rapport à leur taille. Un ordinateur quantique permet de résoudre une partie des problèmes NP.

NP-complet (classe de problème): problème de décision dont il est possible de vérifier une solution en temps polynomial et pour qui tous les problèmes de la classe NP se ramènent à celui-ci via une réduction polynomiale. Cela signifie que le problème est au moins aussi difficile que tous les autres problèmes de la classe NP. Les problèmes du voyageur de commerce et du remplissage du sac à dos sont des problèmes NP-complet.

NP-difficile (classe de problème): problème vers lequel on peut ramener tout problème de la classe NP par une réduction polynomiale. S'il est également dans la classe NP, on dit que c'est un problème NP-complet. Si $P \neq NP$, alors, les problèmes NP-difficile ne peuvent pas être résolus en temps polynomial.

NPU : *Neural Processing Unit*, Unité de traitement neuronal.

Opération unitaire: opération sur un vecteur qui préserve sa longueur. Dans le cas des qubits dont le vecteur a toujours une longueur de 1, les portes quantiques unitaires appliquent dessus une transformation qui préserve cette longueur. Dans la représentation des qubits dans la sphère de Bloch, l'opération fait tourner le vecteur représentant l'état du qubit dans cette sphère.

P (classe de problème): problème qui peut être résolu en temps polynomial par rapport à sa taille, sur une machine de Turing déterministe.

Permanent: le permanent d'une matrice carrée est une opération qui associe un nombre à cette matrice en combinant ses éléments de manière très structurée. On considère tous les chemins possibles qui parcourent une fois chaque ligne et chaque colonne, et pour chacun de ces chemins, on multiplie les éléments correspondants de la matrice. Le permanent est ensuite obtenu en additionnant toutes ces multiplications. Cette opération est particulièrement importante en physique quantique, car elle permet de décrire certaines probabilités d'interférence entre particules identiques, comme les photons, dans des systèmes optiques. Son calcul est extrêmement difficile pour les grandes matrices.

Phaseurs: dispositifs optiques contrôlés électriquement qui modifient la phase d'un signal optique.

Portes quantiques universelles: se dit de jeux de portes quantiques à partir desquelles toutes les autres portes quantiques peuvent être reproduites.

Portes quantiques: opérations de manipulations de l'état de qubits qui agissent sur un ou plusieurs qubits. Les portes à plusieurs qubits (Toffoli, Friedkin...) qui exploitent le principe de l'intrication quantique. Les opérations de portes quantiques sont générées par des actions physiques sur les qubits qui dépendent de leur nature. Pour les qubits supraconducteurs, il s'agit d'envoi de micro-ondes entre 5 et 10 GHz via des conducteurs électriques. Pour les ions piégés, ce sont des opérations pilotées par des lasers. Pour des qubits CMOS, ce sont des tensions électriques. Pour les qubits reposant sur des particules à masse (électrons, ions, atomes froids), les portes quantiques

agissent sur les qubits, mais ceux-ci ne bougent pas. Pour des qubits à base de photons, ceux-ci circulent et traversent des portes quantiques qui modifient leur état (phase, fréquence, ou autre).

Porte-T: porte réalisant une transformation de phase de 45° qui présente l'intérêt de permettre la construction d'un jeu de portes universelles. Cette porte est corrigée avec un code de correction d'erreur particulier qui coûte très cher au regard des codes de correction d'erreur des portes de type X, Z et CNOT.

Porte Toffoli: porte à trois qubits qui permet de créer un jeu de portes quantiques universel.

Post-sélection: technique de sélection du résultat d'une opération consistant à éliminer les résultats considérés comme étant mauvais.

PQC: *Post Quantum Cryptography*, cryptographie résistante aux algorithmes conçus pour les ordinateurs quantiques. Elle repose sur l'usage de clés publiques qui ne sont pas décomposables avec des ordinateurs classiques ou des ordinateurs quantiques. C'est lié au fait qu'il s'agit d'un problème « NP-difficile ».

PSPACE: classe de complexité en informatique théorique qui regroupe les problèmes décisionnels pouvant être résolus en utilisant une quantité de mémoire (espace) polynomiale par rapport à la taille de l'entrée. Contrairement à d'autres classes comme P ou NP, la classe PSPACE se concentre sur la contrainte de mémoire utilisée, indépendamment du temps nécessaire pour effectuer les calculs.

QAOA: *Quantum Approximate Optimization Algorithm*, algorithme variationnel servant à résoudre des problèmes d'optimisation combinatoire.

QCCD: *Quantum Charge-Coupled Device*, architecture pour les ordinateurs quantiques à base d'ions piégés qui exploite la capacité de certains ions à interagir par couplage électrique pour effectuer des opérations quantiques tout en permettant une grande modularité et une évolutivité.

QFT: *Quantum Fourier Transform*. Variation quantique de la transformée de Fourier. La transformée de Fourier classique permet de décomposer un signal (comme en audio) en fréquences (ou spectre de fréquences). La QFT fait cela sur une suite de nombres entiers et détermine sa plus grande fréquence observable.

qLDPC: *quantum Low-Density Parity Codes*. Codes de correction d'erreur très en vogue qui nécessitent un faible nombre de qubits physiques par qubits logiques au prix d'une meilleure connectivité entre qubits distants.

QML: *Quantum Machine Learning*.

QPE: *Quantum Phase Estimate*. Algorithme FTQC qui sert à obtenir la phase d'un hamiltonien et indirectement de l'énergie de l'état au repos d'un système quantique à N-corps.

QPU: *Quantum Processing Unit*.

Qubit bosonique: Un qubit bosonique supraconducteur repose généralement sur un résonateur micro-ondes linéaire à faibles pertes servant de mémoire quantique bosonique. Les qubits de chat d'Alice&Bob sont un cas particulier de qubit bosonique.

Qubit logique: assemblage de qubits physiques mettant en œuvre un dispositif matériel ou logiciel de correction d'erreur. Vu du développeur de logiciel, il présente le comportement d'un qubit physique dont la fidélité serait meilleure que celle de ces derniers. La fidélité des qubits logiques dépend notamment du nombre de qubits physiques qu'ils contiennent, de la qualité des codes de correction d'erreur et de la stabilité de la fidélité avec l'augmentation du nombre de qubits.

Qubit ou qubit physique: unité d'information élémentaire de l'informatique quantique dans les ordinateurs quantiques. Elle stocke un état quantique associant deux états distincts d'une particule ou d'un système quantique à base de plusieurs particules (spin d'électron, état supraconducteur d'un groupe d'électron, niveau d'énergie d'un atome ou d'un ion piégé, polarisation ou autre propriété d'un photon). Sa représentation mathématique est un vecteur comprenant deux nombres complexes.

QUBO: *Quadratic Unconstrained Binary Optimization*. Technique de formulation de problème d'optimisation qui est ensuite exploitable par conversion automatique par des ordinateurs analogiques tels que les *quantum annealers* de D-Wave ou les ordinateurs analogiques quantiques de Pasqal.

Qudit: est une forme générique de qubit qui a n états quantiques possibles au lieu de deux. L'approche est rarement utilisée, en tout cas dans des ordinateurs quantiques hors des laboratoires de recherche.

Qutrit: c'est une forme de qubit qui au lieu d'avoir deux états quantiques possibles, en a trois. C'est un cas particulier des qudits.

Réfrigérateur à dilution: nom donné aux cryostats de la plupart des ordinateurs quantiques qui sont utilisés pour refroidir la puce de calcul quantique à moins de 20 mK. La dilution est liée au fait que ces systèmes utilisent un mix de deux isotopes de l'hélium: le 3 et le 4, qui sont dilués l'un dans l'autre dans la boucle de réfrigération, les deux isotopes ayant des propriétés légèrement différentes. Un cryostat à l'hélium 4 ne descend qu'à 4 K, un cryostat à l'hélium 3 descend à 300 mK tandis qu'un cryostat utilisant les deux génère une température qui descend jusqu'à 10 mK. À noter que la variante la plus courante est le réfrigérateur à dilution «à sec» par opposition à «humide». Cette version utilise une moins grande quantité d'hélium et laisse plus de place dans le «chandelier» pour y caser l'appareillage électronique et quantique.

Registre: ensemble de bits ou de qubits.

Rydberg (atomes): état excité d'un atome possédant un ou plusieurs électrons et dont le nombre quantique principal n (indice de la couche d'électrons dans l'atome qui est un entier compris entre 1 et le nombre de couches d'électrons dans l'atome) est très élevé. Ces atomes sont généralement de grande taille, proportionnelle à n^2 , et avec des interactions interatomiques très fortes. Ces interactions permettent l'intrication de sous-ensembles atomiques voire d'atomes uniques. Ces atomes ont été utilisés par l'équipe de Serge Haroche pour détecter de manière non destructive la présence d'un photon dans une cavité, et ainsi étudier la décohérence quantique. Mais l'hydrogène peut aussi

être un atome de Rydberg s'il est excité avec de hauts niveaux d'énergie, faisant passer son électron à une couche quantique de nombre élevé.

SAT : classe de problème de logique ou problème de satisfaisabilité booléenne, de logique d'ordre 0. C'est un problème de décision, qui, étant donné une formule de logique propositionnelle, détermine s'il existe une assignation des variables propositionnelles qui rend la formule vraie.

SFQ : *Single Flux Quantum*, technique de circuits électroniques fonctionnant à basse température et supraconducteurs. Envisagés pour le contrôle à basse température de qubits tels que les qubits supraconducteurs et silicium. Permet de réduire le câblage utilisé pour contrôler les qubits.

SGPI : Secrétariat général pour l'investissement

Shor (algorithme) : algorithme de factorisation quantique de nombres entiers inventé par Peter Shor en 1994. Il permettrait en théorie de casser des clés publiques RSA en les décomposant en nombres premiers.

Silicium 28 : isotope de silicium permettant de créer des *wafers* de silicium adaptés à la création de qubits en silicium. Le silicium 28 a un spin nul qui n'influe pas sur le spin des électrons piégés servant à gérer les qubits. Il est purifié en Russie et peut être ensuite déposé en couche mince en phase gazeuse sur du silicium classique.

SLM : modulateur spatial de lumière qui contrôle la phase de photons issus de lasers. Est utilisé pour le contrôle des atomes froids.

Spin : état d'une particule décrivant sa rotation sur elle-même ou un moment magnétique. S'applique aux électrons, aux neutrons et aux atomes. Le spin de particules composites est l'addition du spin de ses composantes. Un proton et un neutron ont un spin de $\frac{1}{2}$. Un électron a un spin de $+\frac{1}{2}$ ou $-\frac{1}{2}$.

Spin de noyau : spin du noyau d'un atome.

SMP : *Symmetric Multiprocessing*, ou multiprocesseur symétrique, architecture dans laquelle plusieurs processeurs partagent un espace

mémoire unique et accèdent à cette mémoire de manière symétrique, c'est-à-dire avec des droits d'accès égaux.

SQUID: *Superconducting Quantum Interference Device*, dispositif extrêmement sensible capable de détecter de très faibles champs magnétiques. Il repose sur les principes de la supraconductivité et de l'effet Josephson. Il est notamment utilisé pour la captation de précision du magnétisme dans les circuits de certains capteurs quantiques.

Superposition : principe fondamental de la mécanique quantique selon lequel un système quantique peut être préparé sous la forme d'une combinaison de plusieurs états de base, comme le spin haut ou bas d'un électron dans une direction donnée ou des niveaux d'excitation d'un atome. C'est notamment lié à la dualité onde particule et le fait que l'on peut combiner linéairement deux fonctions d'onde d'un objet quantique pour créer un nouvel état de cet objet.

Supraconductivité : capacité de la matière à permettre de conduire l'électricité sans résistance. Elle se manifeste généralement à basse température. Les qubits de certains types, notamment à base d'électrons, sont refroidis à très basse température pour permettre cet effet, soit au niveau des qubits pour les qubits supraconducteurs, soit pour les dispositifs et câbles de lecture de l'état des qubits. À noter le faux ami : en anglais, on ne dit pas *supra*, mais *superconductivity*.

Suprématie quantique: qualifie une situation où un ordinateur quantique peut réaliser un calcul qui est inaccessible aux meilleurs supercalculateurs du moment en un temps humainement raisonnable. Le différentiel de temps de calcul entre le calcul quantique et le calcul classique doit être de plusieurs ordres de grandeur ou dépasser la durée d'une vie humaine. La suprématie peut concerner un calcul utile ou pas. Ainsi, la suprématie quantique revendiquée par Google en octobre 2019 concerne-t-elle un algorithme de génération et de vérification de nombres aléatoires qui n'a pas d'intérêt pratique. Un autre débat porte sur le bien-fondé de cette appellation de *supremacy* qui écho au thème polémique de la « *white supremacy* ». L'expression a été créée par John Preskill en 2011.

SWAP: porte quantique qui intervertit l'état de deux qubits.

TDA: *Topological Data Analysis*, méthode de *clustering* automatique qui relève de l'apprentissage automatique.

Technologie habilitante: «technologie qui permet à une autre de fonctionner», technologie indispensable pour un ordinateur quantique (par exemple, la cryogénie, le câblage et l'électronique de contrôle).

TeraQops: *Tera Quantum Operation per second*.

Threshold: seuil à partir duquel avec un code de surface, le qubit logique aura une meilleure fidélité que les qubits physiques. En pratique, il faut que les qubits physiques aient un taux d'erreur dix fois plus faible pour que le nombre de qubits physiques par qubits logiques soit raisonnable, car au niveau du *threshold*, ce nombre est infini.

TLS: *Two-Level Systems* désigne un bain de systèmes parasites se couplant aux qubits supraconducteurs. Leur origine est méconnue et probablement multiple (fluctuateurs électriques piégés aux interfaces substrats/air, substrat/métal ou métal/air, fluctuateurs magnétiques basse fréquence...).

Toffoli (porte): aussi appelée CCNOT, est une porte quantique opérant sur trois qubits qui modifie la valeur du troisième qubit si celle des deux premiers est à 1.

Transduction: conversion d'un signal d'un type vers un signal d'un autre type. Par exemple pour passer du régime des micro-ondes (en GHz) au régime des photons optiques.

Transformation unitaire: opération mathématique réversible transformant l'état quantique d'un système quantique.

Transmon: type de qubit supraconducteur utilisé notamment par IBM, Google et IQM.

TSV: *Through Silicon Vias*, connectique verticale des circuits intégrés qui permet de relier des éléments des circuits intégrés entre leur couche supérieure et leur couche inférieure. La technique peut servir à étendre cette connectivité à des puces constituées de plusieurs circuits intégrés

superposés. Elle est critique pour la mise au point de puces de qubits supraconducteurs.

TWPA: *Travelling-Wave Parametric Amplifier*. Amplificateur fonctionnant à la limite quantique et à environ 15 mK qui amplifie la pulsation micro-ondes réfléchiée par un qubit supraconducteur lors de sa lecture.

VQE: *Variational Quantum Eigensolver*: algorithme quantique hybride utilisé dans la simulation chimique créé en 2013. Son principal contributeur est Alan Aspuru-Guzik, un chercheur qui faisait partie de la startup Zapata Computing.

Wafers: galettes de semiconducteur (silicium ou autre) sur lesquelles sont gravées des puces électroniques.

X: porte quantique à un qubit qui inverse son amplitude, passe de $|0\rangle$ à $|1\rangle$ ou de $|1\rangle$ à $|0\rangle$ pour ce qui est des états de base.

Y: porte quantique à un qubit qui réalise une rotation de 180° autour de l'axe Y dans la sphère de Bloch.

Z: porte quantique à un qubit qui applique un changement de signe sur la composante β du vecteur du qubit, soit une inversion de phase et une rotation de 180° par rapport à l'axe Z.

B. Membres du groupe de travail

- Frédéric BARBARESCO (Thales)
- Thierry BONHOMME (Académie des technologies, [co-président](#))
- Boris BOURDONCLE (Quandela, [secrétaire général](#))
- Philippe DULUC (Eviden)
- Marko ERMAN (Thales et Académie des technologies)
- Olivier EZRATTY (Epita et Quantum Energy Initiative)
- Philippe GRANGIER (CNRS Laboratoire Charles Fabry)
- Daniel KAPLAN (Académie des technologies)
- Catherine LAMBERT (Cerfacs, [présidente](#))
- Jean-Claude LEHMANN (Académie des technologies)
- Anthony LEVERRIER (Inria Paris)
- Frédéric MAGNIEZ (CNRS - IRIF)
- Mazyar MIRRAHIMI (Inria Paris)
- Jean-Philippe NOMINÉ (CEA DAM)
- Sophie PROUST (Inria, Agence de programme numérique et Académie des technologies)
- Gérard ROUCAIROL (Académie des technologies, [co-président](#))
- Claude WEISBUCH (CNRS, École polytechnique et Université de Californie à Santa Barbara (USA), Académie des technologies)
- Lydia YAHIA CHERIF (Académie des technologies, [référente](#))

N.B.: La déontologie académique exige que tout contributeur à la l'élaboration d'un rapport n'apporte au collectif que sa seule expertise, en se gardant de promouvoir tout intérêt personnel ou corporatif. En vue d'une parfaite transparence, précisons ici que certains membres du groupe, en raison de leur position professionnelle, se sont tout particulièrement pliés à cette discipline, notamment Boris BOURDONCLE, Frédéric BARBARESCO, Philippe DULUC et Marko ERMAN

Contributions additionnelles au rapport de : Philippe CAMPAGNE-IBARCQ (Inria), Tom DARRAS (Weling), Eleni DIAMANTI (CNRS), Julien LAURAT (Sorbonne Université), Jean LAUTIER-GAUD (Weling).

C. Personnes auditionnées

- Cyril ALLOUCHE (Eviden)
- Frédéric BARBARESCO (Thales)
- Antoine BROWAEYS (Pasqal)
- Henri CALANDRA (TotalEnergies)
- Alain CHAMPENOIS (Quobly)
- Tom DARRAS (Welinq)
- Étienne DECOSSIN (EDF)
- Pierre DESJARDINS (C12)
- Matthieu DESJARDINS (C12 Quantum Electronics)
- Daniel ESTÈVE (CEA)
- Jérémie GUILLAUD (Alice&Bob)
- Félix GIVOIS (Genci)
- Anne-Lise GUILMIN (Eviden)
- Loïc HENRIET (Pasqal)
- Olivier HESS (Eviden)
- Iordanis KERENIDIS (CNRS)
- Anthony LEVERRIER (Inria)
- Christophe LABREUCHE (Thales)
- Stéphane LOUISE (CEA)
- Shane MANSFIELD (Quandela)

- Sabine MEHR (Genci)
- Tristan MEUNIER (CNRS)
- Grégoire MISGUICH (CEA)
- Damien NICOLAZIC (Eviden)
- Cécile PERRAULT (Alice&Bob)
- Jean-Philip PIQUEMAL (Sorbonne Université)
- Pierre ROUCHON (Université PSL)
- Félicien SCHOPFER (CNRS)
- Pascale SENELLART (Quandela)
- Emmanuelle VERGNAUD (Teratec)
- Daniel VERWAERDE (Teratec)
- Maud VINET (Quobly)
- Xavier WAIN TAL (CEA)

Ce rapport a été soumis pour commentaires aux personnes suivantes : Antoine BROWAEYS, Pierre DESJARDINS, Matthieu DESJARDINS, Jérémie GUILLAUD, Loïc HENRIET, Shane MANSFIELD, Tristan MEUNIER, Pascale SENELLART, Maud VINET.

Ce rapport fait le point sur la construction et l'utilisation potentielle d'ordinateurs dits FTQC (*Fault Tolerant Quantum Computing*) pour effectuer de manière fiable des calculs complexes en surmontant les problèmes posés par les erreurs et le bruit inhérents aux systèmes quantiques.

Après avoir rappelé la réalité de l'avantage quantique et ses besoins, le rapport décrit l'utilisation des codes correcteurs d'erreurs dans la conception des ordinateurs FTQC. Il est fait état ensuite de l'avancement des cinq technologies physiques les plus avancées dans le monde pour construire de tels ordinateurs et les obstacles auxquels elles auront à faire face pour réaliser le passage à l'échelle nécessaire à l'exécution d'applications utiles. Enfin sont évoqués, l'environnement technico-économique des ordinateurs quantiques, la manière de comparer et évaluer leurs performances ainsi que leur coexistence future avec d'autres technologies de calcul (silicium 3D, IA) ou avec des supercalculateurs.

Académie des technologies
Le Ponant – Bâtiment A
19, rue Leblanc
75015 PARIS
+33(0)1 53 85 44 44
secretariat@academie-technologies.fr
www.academie-technologies.fr

ISBN : 979-10-97579-63-0



9 791097 579630

Couverture : EnigmaEasel - Adobe stock