Ambassade de France à Washington
Mission pour la Science et la Technologie
4101 Reservoir Road, NW, Washington DC 20007
Tél. : +1 202 944 6249
Fax : +1 202 944 6219
Mail : publications.mst@ambafrance-us.org
URL : http://www.ambafrance-us.org

Domaine	**Informatique, mécanique quantique**
Document	**Dossier Sciences Physiques Etats-Unis**
Titre	**L'ordinateur quantique**
Auteur(s)	**Daniel Ochoa** (attaché scientifique à San Francisco)
Date	**30 avril 2008**
Contact MST	**Daniel Ochoa ; attache-stic.mst@consulfrance-sanfrancisco.org**
Numéro	**SMM08_**

Mots-clefs	Mécanique quantique, informatique, ions piégés, supraconducteurs, optique quantique, RMN, atomes froids
Résumé	Énoncés il y a plus de quatre-vingts ans, les principes de la Mécanique Quantique continuent à fasciner le grand public, tant ils semblent contraires à l'intuition du monde physique que développe chacun d'entre nous. Pourtant, si on les envisage du point de vue de l'information traitable par une machine miniaturisée à l'extrême, où chaque bit d'information doit être exprimé avec la plus petite énergie possible, ces principes quantiques apparaissent, de façon surprenante, bien plus naturels et rationnels que ceux de la mécanique classique. Le nouvel éclairage qu'apporte à la physique quantique la science de l'information va en fait beaucoup plus loin qu'un commentaire esthétique. Petit à petit, au cours des quinze dernières années, les physiciens, en association avec les informaticiens et les mathématiciens, ont compris que les "bits quantiques" sont en réalité plus puissants collectivement que les traditionnels "bits classiques" sur lesquels sont basés les ordinateurs actuels. Ils permettent par exemple une accélération exponentielle de certains calculs, comme la factorisation des nombres, nécessaire au décryptage des informations confidentielles échangées sur le réseau Internet. En même temps, les bits quantiques permettent de coder l'information de manière à ce qu'aucune copie ne soit possible. L'ordinateur quantique est la machine – encore hypothétique – qui traiterait ces bits quantiques. Elle n'existe à ce jour qu'en pièces détachées, que de nombreux laboratoires cherchent à améliorer et à combiner, et laisse le champ ouvert à de nombreuses questions. Est-il possible de faire fonctionner un ordinateur quantique? Nous n'avons pour l'instant qu'une preuve de principe qu'une telle machine puisse être un jour construite, et sa réalisation effective demeure un défi pour la science et la technologie. Mais à supposer qu'elle soit un jour construite, quelle gamme de problèmes résoudrait-elle? Le rapport qui suit fait le point sur ces questions.

NB : Toutes nos publications sont disponibles auprès de l'Agence pour la Diffusion de l'Information Technologique (ADIT), 2, rue Brûlée, 67000 Strasbourg (http://www.adit.fr).

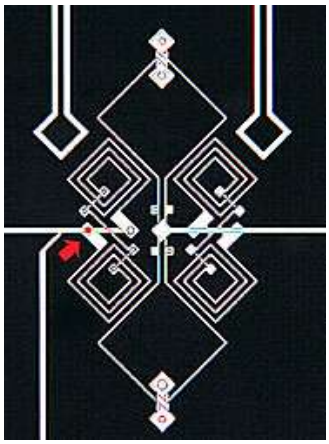
Sciences Physiques Etats-Unis
Nanosciences, Microélectronique, Matériaux

Mission pour la Science et la Technologie

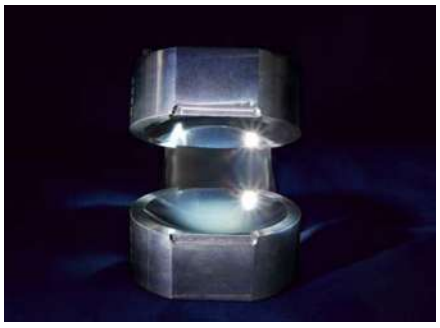
L'ORDINATEUR QUANTIQUE

Un état de l'art des recherches aux Etats-Unis et ailleurs

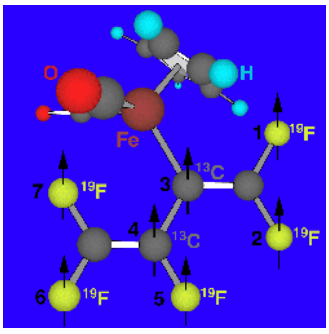
Avril 2008



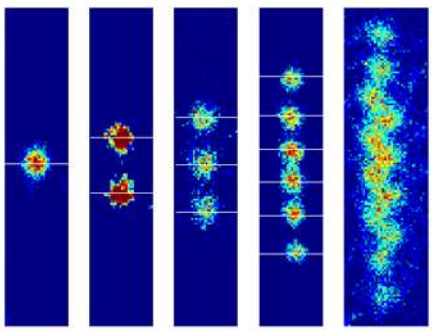
Circuit supraconducteur
formant un qubit de phase.
Crédits : R.Simmonds, NIST



Cavité supraconductrice
pour l'optique quantique.
Crédits : S. Haroche, LKB, ENS



Molécule de fluorine utilisée en
RMN pour factoriser le nombre 15.
Crédits : IBM Almaden



Ions magnésium piégés sur circuit,
formant des qubits intriqués.
Crédits : D. Wineland, NIST

Préface

Énoncés il y a plus de quatre-vingts ans, les principes de la Mécanique Quantique continuent à fasciner le grand public, tant ils semblent contraires à l'intuition du monde physique que développe chacun d'entre nous. Pourtant, si on les envisage du point de vue de l'information traitable par une machine miniaturisée à l'extrême, où chaque bit d'information doit être exprimé avec la plus petite énergie possible, ces principes quantiques apparaissent, de façon surprenante, bien plus naturels et rationnels que ceux de la mécanique classique. Le nouvel éclairage qu'apporte à la physique quantique la science de l'information va en fait beaucoup plus loin qu'un commentaire esthétique. Petit à petit, au cours des quinze dernières années, les physiciens, en association avec les informaticiens et les mathématiciens, ont compris que les "bits quantiques" sont en réalité plus puissants collectivement que les traditionnels "bits classiques" sur lesquels sont basés les ordinateurs actuels. Ils permettent par exemple une accélération exponentielle de certains calculs, comme la factorisation des nombres, nécessaire au décryptage des informations confidentielles échangées sur le réseau Internet. En même temps, les bits quantiques permettent de coder l'information de manière à ce qu'aucune copie ne soit possible. L'ordinateur quantique est la machine – encore hypothétique – qui traiterait ces bits quantiques. Elle n'existe à ce jour qu'en pièces détachées, que de nombreux laboratoires cherchent à améliorer et à combiner, et laisse le champ ouvert à de nombreuses questions. Est-il possible de faire fonctionner un ordinateur quantique? Nous n'avons pour l'instant qu'une preuve de principe qu'une telle machine puisse être un jour construite, et sa réalisation effective demeure un défi pour la science et la technologie. Mais à supposer qu'elle soit un jour construite, quelle gamme de problèmes résoudrait-elle? Le rapport qui suit fait le point sur ces questions. Et aussi incertaines que soient actuellement les réponses, je suis persuadé que les recherches effectuées dans cette nouvelle quête du Graal amèneront de grands progrès à la fois dans les sciences et dans les technologies de l'information.

Michel Devoret
Professeur au Collège de France
F.W. Beinecke Professor of Applied Physics, Yale University

I. INTRODUCTION

Les ordinateurs actuels, basés sur la microélectronique Silicium, approchent de limites fondamentales dictées par les lois de la mécanique quantique. Le problème principal est que toute leur architecture est fondée sur des lois physiques appartenant à la mécanique classique, qui considèrent comme nuisibles la plupart des phénomènes quantiques. Pour accélérer ces ordinateurs classiques, et leur donner la puissance de calcul que l'on connaît, l'industrie de la microélectronique s'évertue depuis 40 ans à réduire les dimensions des transistors qui les composent. Cependant, lorsque ces dimensions atteindront une dizaine de nanomètres, ce qui devrait arriver dans une dizaine d'années, les phénomènes quantiques commenceront à être prédominants. Les électrons jusque là bien ordonnés révèleront leur nature quantique, qui est, entre autres, probabiliste. Les transistors pourraient ainsi, ne plus être de manière déterministe dans l'état ON ou OFF, mais se retrouver dans une superposition des deux, avec une certaine probabilité d'être dans l'état ON ou dans l'état OFF. Un tel comportement n'appelle aucune alternative : il faudra soit adapter l'architecture des ordinateurs pour minimiser les nuisances occasionnées par les effets quantiques, ou alors changer radicalement d'architecture en ouvrant les bras à ces effets quantiques. L'ordinateur quantique suit cette deuxième approche.

L'ordinateur quantique est un concept récent. Dans les années 80, Richard Feynman envisageait pour la première fois un 'simulateur universel'. Il remarquait que certains phénomènes quantiques, qui ne pouvaient pas être simulés efficacement sur un calculateur classique, pouvaient l'être bien plus efficacement en utilisant les effets quantiques. Cette idée fut reprise peu de temps après par Deutsch qui dégagea les grandes lignes de ce qui allait devenir l'ordinateur quantique, en introduisant les concepts fondateurs de 'qubits' et 'portes quantiques'. Dans un système quantique, l'espace de calcul augmente exponentiellement avec la taille du système, ce qui permet un parallélisme de calcul exponentiel. Un tel parallélisme profite à l'algorithme de Shor pour factoriser un nombre entier en un temps de calcul seulement polynomial, et non

pas exponentiel comme c'est le cas avec les tous les algorithmes classiques connus. Une telle accélération pourrait rendre caduques les techniques de cryptage actuelles, qui reposent essentiellement sur la difficulté de factoriser un grand nombre. La découverte de l'algorithme de Shor en 1994 a fait surgir un certain engouement pour le calcul quantique, qui a été renforcé peu de temps après avec la découverte de l'algorithme de Grover en 1997. Cet algorithme permet une accélération importante, et que l'on croyait impossible, du processus de recherche d'un élément dans une liste non-structurée. La découverte, coup sur coup de ces deux algorithmes a donné presque instantanément une crédibilité pratique au concept d'ordinateur quantique. Elle a même pu faire croire un temps, que l'ordinateur quantique était si puissant qu'il allait bientôt remplacer l'ordinateur classique, et bouleverser notre société.

Cependant, depuis maintenant une dizaine d'année, aucun autre algorithme révolutionnaire n'a été mis à jour, et divers problèmes ont surgi. L'intrication, sur laquelle repose le parallélisme du calcul quantique, s'est avérée être extrêmement fragile, et sujette à de grâves phénomènes de décohérence. Des techniques efficaces de correction d'erreur ont été mises à jour, mais imposent de lourdes contraintes sur l'architecture des systèmes. Toujours est il que, sur le plan théorique, les travaux récents ont mis en avant certaines limitations de l'ordinateur quantique, et que la révolution tant attendue se fait encore attendre.

Expérimentalement, il a longtemps été difficile de disposer de systèmes suffisamment robustes pour lutter contre la décohérence, et réaliser ne serait-ce qu'un qubit relevait de l'exploit. Toutefois, la persistance des chercheurs a payé, avec une foison de résultats remarquables durant ces cinq dernières années. Les approches sont très diverses, présentant des avantages et des inconvénients distincts. Les principales d'entre elles sont passées en revue dans ce dossier : circuits supraconducteurs, spins électroniques dans des boîtes quantiques semiconductrices, ions piégés, atomes froids en réseaux, optique quantique, résonance magnétique nucléaire en solution. Dans beaucoup de ces disciplines, les équipes de recherche américaines sont parmi les plus actives, et sont à l'origine de résultats remarquables. Ce dossier se concentre sur ces résultats, sans négliger toutefois ceux des équipes des autres pays (dont évidemment la France), lorsqu'ils présentent un intérêt particulier.

Toutes ces approches restent pour l'instant en concurrence, et leur diversité laisse espérer que l'une d'elle parviendra un jour à résoudre simultanément les problèmes de décohérence et d'adressabilité de ces systèmes quantiques. La route qui mène à l'ordinateur quantique est malheureusement encore bien longue, les chercheurs mettront certainement une bonne vingtaine d'année au moins à la parcourir. En revanche, il est tout à fait possible que des systèmes quantiques primitifs voient le jour dans quelques années, permettant d'explorer la richesse du monde de l'informatique quantique.

II. THEORIE ELEMENTAIRE DE L'INFORMATIQUE QUANTIQUE

L'ordinateur quantique, qu'on notera parfois QC pour 'Quantum Computer', n'est à l'heure actuelle, rien de plus qu'un beau concept théorique : celui d'une machine utilisant la mécanique quantique pour résoudre des problèmes beaucoup plus vite qu'un ordinateur classique ne pourra jamais le faire. Comme on le verra dans les chapitres suivants, des ébauches de dispositifs expérimentaux existent, mais ne permettent pour l'instant que des manipulations élémentaires, comme la factorisation du chiffre 15 (le record actuel). L'ordinateur quantique promet évidemment beaucoup plus que cela, du moins sur le papier. Son concept théorique se trouve à l'intersection de plusieurs disciplines, comme la physique quantique, l'informatique, et la théorie de l'information. Pour bien comprendre ce qu'il représente, comment il fonctionne, ce qu'il permet de faire et ne pas faire, et quelles sont ses limites, il faut revenir sur quelques notions fondamentales appartenant à ces différentes disciplines. C'est l'objet de ce chapitre. Un traitement plus détaillé de ces notions peut être trouvé dans d'excellents articles de revue[1,2].

Nous commençons par donner une définition de l'ordinateur quantique, et pour cela introduisons les briques qui le composent : les qubits et les portes quantiques. Nous verrons comment les qubits se comportent vis-à-vis de la combinatoire du calcul quantique, et ce qui les rend si différents des bits classiques : pourquoi leur composition aboutit à un espace d'états exponentiellement grand, donnant tout sa puissance de parallélisme à l'ordinateur quantique. Nous verrons enfin ce qui rend les mesures probabilistes des qubits si délicates à effectuer.

Ce dossier traite en priorité de l'ordinateur quantique, qui est un concept très récent datant d'une vingtaine d'années. Il s'inscrit dans la lignée des recherches plus vastes portant sur l'information quantique, et qui elles, ont débuté bien avant. On peut remonter jusqu'à 1935, date à laquelle Einstein, Podolsky et Rosen proposèrent le paradoxe EPR qui porte leur nom. Ce paradoxe a été formalisé dans les années 60 par Bell avec ses fameuses inégalités, puis résolu dans les années 80, théoriquement par Feynman et expérimentalement par Aspect. D'autres recherches ont suivi, et la théorie de l'information quantique a fait surgir un grand nombre de résultats très importants, et fascinants intellectuellement, comme le

théorème du non-clonage, la téléportation quantique, le codage super-dense, et la cryptographie quantique. Afin de ne pas surcharger ce chapitre, et de ne pas dévier du QC qui est l'objet principal du dossier, les explications concernant ces concepts sont relégués en Annexe. Nous les évoquons ici, car ils sont au cœur de la théorie de l'information quantique, dont est issu le QC, et dont ils constituent en quelque sorte la 'préhistoire'. Certains de leurs résultats font, en effet, appel à des notions élémentaires de porte et de calcul quantique, et tous ces concepts manipulent allègrement les qubits. Le théorème du non-clonage dit qu'il est impossible de cloner un état quantique inconnu, c'est-à-dire de copier un qubit inconnu. Le codage super-dense évoque la possibilité de transmettre à distance l'information contenue dans deux bits classiques, à l'aide de l'envoi d'un seul qubit. Les qubits étant bien plus difficiles à manipuler que les bits classiques, ce concept présente peu d'intérêt en pratique. Il est néanmoins important dans le cadre de ce dossier, car il constitue un des premiers concepts manipulant des qubits à l'aide de portes quantiques. Dans la même lignée de concepts, la téléportation quantique est plus intéressante en pratique, et a donné lieu à des expériences remarquables. Elle ne permet pas le transport de matière, comme on le voit souvent dans les romans à succès et œuvres cinématographiques, mais uniquement celui d'information quantique : deux bits classiques suffisent à transmettre l'information quantique d'un qubit. Pour finir, même si elle s'éloigne un peu plus du QC, la cryptographie quantique est également évoquée en Annexe, car elle est d'une importance notable pour les applications pratiques, surtout dans le domaine de la sécurité. Elle a également joué un rôle moteur dans les recherches en théorie de l'information.

Après l'exposé des briques de base, ce chapitre procède en donnant la définition d'un QC, au sens le plus moderne. On verra qu'il s'agit d'une machine de Turing universelle qui, de la même manière qu'un ordinateur classique, a besoin pour fonctionner d'être alimentée par des algorithmes. Ces algorithmes sont beaucoup plus difficiles à concevoir dans le monde quantique que dans le monde classique, et seule une poignée a pu être mise à jour par des recherches, pourtant très actives. Dans cette poignée, on trouve cependant quelques pépites comme les algorithmes de Shor et de Grover. L'algorithme de Shor résout le problème de factorisation des nombres entiers en temps polynomial, alors qu'un algorithme classique requiert un temps exponentiel. L'algorithme de Grover permet de chercher un élément dans une liste non structurée. Il ne change pas la classe de complexité du problème, qui reste solvable en temps exponentiel, mais apporte une accélération importante (et maximale) du calcul. Le paragraphe II.3 n'entre pas en détail dans le fonctionnement des deux algorithmes, mais en donne les grandes lignes et surtout leur intérêt pratique et leurs limites. Il donne également un aperçu d'une classe de problèmes qu'un QC permettra de résoudre bien plus efficacement qu'un ordinateur classique : la simulation de phénomènes physiques à l'échelle atomique. Bien que moins médiatique que les problèmes évoqués précédemment avec les algorithmes de Shor et Grover, cette classe de problèmes est peut être celle qu'un QC saura résoudre le plus efficacement.

Ce chapitre consacré à l'informatique quantique serait incomplet s'il n'évoquait pas les codes correcteurs d'erreur. Sans eux, les phénomènes de bruit, à travers la décohérence quantique, seraient beaucoup trop importants pour que le QC puisse un jour exister. Le paragraphe II.4 donne un aperçu des phénomènes fondamentaux limitant le temps de cohérence des qubits dans un QC, et des stratagèmes mathématiques qui sont mis en œuvre pour s'en affranchir.

Enfin, le paragraphe II.5 termine le chapitre en donnant quelques éléments théoriques généraux permettant de mieux comprendre comment se situe un QC en relation avec les différentes classes de complexité. On apporte une réponse à la question fondamentale : un QC permet-il de résoudre en temps polynomial un problème *NP-complet* ? Si c'est le cas, il permettrait de résoudre en temps polynomial tous les problèmes *NP*, une perspectives fascinante, mais malheureusement peu probable. Ce paragraphe évoque également l'ordinateur quantique adiabatique, dont le concept et les réalisations font actuellement l'objet de controverses.

II.1. Les briques de base d'un ordinateur quantique

II.1.1. Le Qubit

Comme tout système quantique, un QC évolue dans un espace de fonctions d'ondes, modélisé mathématiquement par un espace de Hilbert. Les fonctions d'ondes peuvent être des positions, moments, polarisations, spins etc… En pratique, il suffira de considérer des espaces de dimensions finies, dont les états seront représentés par la notation habituelle des bra <x| et ket |x> inventée par Dirac. Plus précisément, en ce qui concerne l'ordinateur quantique, parmi la multitude de représentations possibles que nous offrent les espaces de Hilbert, l'unité élémentaire habituelle est le qubit, c'est-à-dire un système à deux niveaux, tel qu'un spin ou un atome à deux niveaux. Il a été démontré mathématiquement[3] qu'un ensemble de qubits suffisait à décrire, en terme d'informations, toute la complexité d'un système quantique.

Un qubit est un vecteur unitaire évoluant dans un espace vectoriel complexe de dimension deux, pour lequel une certaine base orthonormée $\{|0\rangle,|1\rangle\}$ a été choisie. Cette base peut correspondre aux polarisations $|\uparrow\rangle$ et $|\rightarrow\rangle$, ou bien $|\nearrow\rangle$ et $|\nwarrow\rangle$ d'un photon. Elle peut également correspondre aux états {spin haut, spin bas}

d'un électron, ainsi qu'aux états {fondamental, excité} d'un niveau à deux états.

Un qubit s'écrira ainsi $|\Psi\rangle = a|0\rangle + b|1\rangle$ où $a^2 + b^2 = 1$, qu'on écrira sans perte de généralité: $|\Psi\rangle = \cos\theta|0\rangle + e^{i\phi}\sin\theta|1\rangle$, avec $0 \le \theta < \frac{\pi}{2}$ et $0 \le \phi < 2\pi$, à un facteur de phase près. Les coordonnées sphériques θ et ϕ définissent un point unique sur la sphère unité, que l'on appelle en l'occurrence 'sphère de Bloch'. Intuitivement, un qubit peut se représenter ainsi simplement par un point sur cette sphère unité.

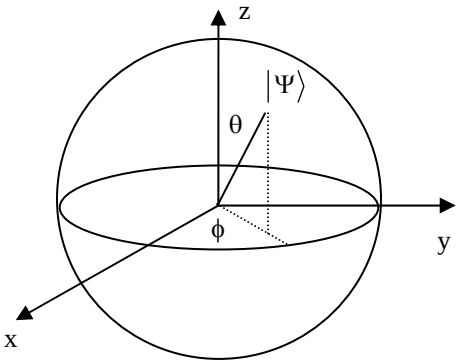


Figure 1 Représentation d'un qubit comme un vecteur unitaire sur la sphère de Bloch

II.1.2. La composition des qubits

Un ordinateur classique travaille avec des bits, qui prennent uniquement les valeurs 0 ou 1. Le QC, lui, travaille avec des qubits, dont la propriété fondamentale est qu'ils peuvent être composés, ce qui les distingue des bits classiques. Par exemple, dans la base $\{|0\rangle, |1\rangle\}$, un qubit peut être dans la superposition $a|0\rangle + b|1\rangle$, où a et b sont des nombres complexes normalisés ($|a|^2 + |b|^2 = 1$). Dans ce cas, la probabilité de mesurer le qubit dans l'état $|0\rangle$ sera $|a|^2$, celle de le mesurer dans l'état $|1\rangle$ sera $|b|^2$.

C'est là une des propriétés (mais aussi limitations) fondamentales du calcul quantique : même dans une superposition d'un très grand nombre d'états, la mesure réduit la fonction d'onde à un seul état. Dans le cas présent, la mesure de l'état $a|0\rangle + b|1\rangle$ réduira la fonction d'onde aléatoirement dans l'état $|0\rangle$ ou $|1\rangle$, avec les probabilités $|a|^2$ et $|b|^2$ associées à ces deux états. La mesure d'un qubit ne permet au final de lire qu'un seul bit classique, et encore pas forcément celui qui est désiré. Cette mesure étant un procédé classique, il n'est pas possible d'extraire d'un qubit plus d'information que d'un bit classique. Comme le résultat d'un calcul quel qu'il soit devra finir par être mesuré pour être exploitable, la force du QC ne réside donc pas dans la simple propriété de superposition des qubit, mais plutôt dans la taille de l'espace des états qu'elle autorise.

II.1.3. Un espace d'états exponentiellement grand

Nous entrons ici au cœur de ce qui fait la différence entre un ordinateur classique et un ordinateur quantique. Cette différence tient essentiellement au phénomène d'intrication et à la croissance exponentielle de l'espace des états qui s'ensuit.

En physique classique, les états possibles d'un système de *n* bits (plus généralement de particules dont les états individuels peuvent être représentés par un vecteur dans un espace à deux dimensions), forment un espace vectoriel de dimensions 2*n*. En comparaison, un système quantique de *n* qubits dispose d'un espace d'états de dimension 2^n. Une base de trois qubits sera ainsi donnée par :

$\{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}$,

où les kets sont des représentations simplifiées pour les produits tensoriels : $|0\rangle \otimes |0\rangle \otimes |0\rangle$, $|0\rangle \otimes |0\rangle \otimes |1\rangle$ etc…

La différence essentielle avec les systèmes classiques tient au fait que certains états quantiques, par exemple $|00\rangle + |11\rangle$, sont intriqués. De tels états intriqués ne peuvent pas être décrits en terme d'états de chacun des qubits qui les composent. En d'autres termes, il est impossible de trouver a_1, a_2, b_1, b_2 tels que $(a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle) = |00\rangle + |11\rangle$. Ces états intriqués correspondent à quelque chose qui n'a pas d'équivalent en physique classique. Ils sont à l'origine de la dimension exponentielle (en 2^n) du nombre d'états d'un système de *n* qubits.

II.1.4. Intrication et mesure

L'intrication des états quantiques peut être comprise de façon plus intuitive en considérant le phénomène qui a lieu lorsqu'on les mesure. De manière générale, des particules sont intriquées si la mesure de l'une d'elles n'a aucune influence sur les autres. Prenons l'exemple de l'état : $1/\sqrt{2}(|00\rangle + |11\rangle)$. Il est intriqué car la probabilité que la mesure du premier qubit donne $|0\rangle$ est 1/2 si le deuxième qubit n'a pas été mesuré. En revanche, si le deuxième qubit a été mesuré, cette probabilité devient 1 ou 0 selon que la mesure du deuxième qubit a donné $|0\rangle$ ou $|1\rangle$. En comparaison, l'état $1/\sqrt{2}(|00\rangle + |01\rangle)$ n'est pas intriqué, car il peut s'écrire sous la forme du produit tensoriel $|0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, et la mesure du premier

qubit donnera $|0\rangle$ quelque soit le résultat de la mesure du deuxième qubit. De même le deuxième qubit a 50% de chance d'être mesuré dans l'état $|0\rangle$ ou $|1\rangle$, que le premier qubit ait été mesuré ou non.

II.1.5. Les portes à la base du calcul quantique

Pour progresser dans l'idée de calcul quantique, il nous faut introduire les concepts de portes quantiques. Qui dit calcul quantique, dit évolution et transformation d'un système quantique dont la dynamique est gouvernée par les équations de Schrödinger. Afin de préserver l'orthogonalité, les transformations légitimes doivent être unitaires, et donc réversibles. On peut se les représenter comme des rotations d'espaces vectoriels complexes.

Les transformations les plus simples sont appelées 'portes quantiques'. Il y en a une infinité (chaque rotation sur la sphère de Bloch en est une), contrairement à la théorie classique de l'information pour laquelle il n'existe que deux portes (l'identité et l'inversion *NOT*).

Les portes quantiques fondamentales les plus utilisées sont expliquées en Annexe XI.6. Les portes {*I, X, Y, Z*} sont les plus élémentaires, *I* étant l'identité, *X* l'inversion appelée *NOT*, et *Z* un changement de signe. La transformation de Walsh-Hadamart permet de paralléliser facilement les algorithmes quantiques. Les portes de Toffoli et de Freddkin, sont dites 'complètes', car elles sont capables d'engendrer toutes les portes logiques de la combinatoire des circuits.

La porte C_{not} (Controled-NOT), joue également un rôle fondamental et on la retrouvera souvent par la suite. Cette porte opère sur deux qubits en inversant le second si le premier est $|1\rangle$ et en le laissant inchangé dans le cas contraire, ce qui se résume par les opérations :
$C_{not} : |00\rangle \to |00\rangle, |01\rangle \to |01\rangle, |10\rangle \to |11\rangle, |11\rangle \to |10\rangle$.
C_{not} est parfois appelée XOR et notée $\oplus$, son effet sur l'état $|a\rangle|b\rangle$ étant donné par $a \to a, b \to a \oplus b$.

II.2. Qu'est ce qu'un ordinateur quantique ?

II.2.1. Definition

Nous disposons dorénavant de suffisamment de matériel pour nous pencher sur le cœur du sujet de ce chapitre, à savoir l'ordinateur quantique, sa définition et son universalité.

Un ordinateur quantique[4,5,6] est un concept théorique dont l'objectif est de permettre de manipuler et analyser l'information quantique. Plusieurs théoriciens en ont donné une définition assez précise[7]. Nous retenons ici celle de David DiVincenzo des laboratoires IBM[8], qui est utilisée aujourd'hui par la majorité des équipes de recherche. Un ordinateur quantique (QC pour 'Quantum Computer') est un système de qubits qui doit présenter les caractéristiques suivantes :

1. Pouvoir initialiser tous les qubits dans un état bien défini (|0000…>) au début du calcul.
2. Etre capable de mesurer les qubits à la fin du calcul.
3. Les qubits doivent avoir un temps de décohérence suffisamment long : beaucoup plus long que la durée d'opération d'une porte quantique (au moins 10,000 fois plus long pour que les QEC soient efficaces, voir paragraphe II.4).
4. Disposer de suffisamment de portes quantiques pour pouvoir effectuer toutes les opérations quantiques.
5. L'architecture du système doit être en mesure d'accommoder un grand nombre de qubits.

Comme on le verra dans les prochains chapitres, certains des dispositifs expérimentaux les plus récents permettent de satisfaire les quatre premiers points. Pour le moment, le dernier point reste le plus difficile à satisfaire.

Cette description en 5 points ne dit rien sur l'architecture que pourra posséder un tel ordinateur quantique. Expérimentalement, on verra que les approches sont très variées, et que souvent les architectures sont surprenantes, et ne correspondent en rien à l'image 'classique' que l'on se fait d'un ordinateur. En effet, les microprocesseurs auxquels nous sommes habitués sont composés de portes logiques fixes, gravées dans le silicium, et de bits 'mobiles', se présentant comme des impulsions électriques qui se propagent dans le circuit à travers les différentes portes. Dans la plupart des ébauches d'ordinateurs quantiques que l'on rencontre, c'est l'inverse qui se produit, à savoir que les qubits sont fixes et matériels, alors que les portes quantiques sont des interactions électromagnétiques que l'on allume ou éteint à volonté.

II.2.2. Machine de Turing universelle

La définition en 5 points de DiVincenzo appelle la question suivante : un tel ordinateur quantique est il universel au sens de Turing, c'est-à-dire est il capable de simuler l'action de n'importe quel autre (voir Annexe XI.7) ? La réponse est positive : un QC est une machine de Turing universelle, satisfaisant même au principe plus général de Turing-Church.

En effet, tout système quantique est donné par un vecteur dans l'espace de Hilbert, qui peut être représenté par un nombre fini de qubits. Toute évolution du système quantique est alors une transformation unitaire d'états des qubits. Or, comme l'a montré D. Deutsch[9], il est possible d'engendrer toutes les opérations quantiques, c'est-à-dire toute les transformations unitaires de l'espace de Hilbert, avec seulement deux portes quantiques : la porte à deux qubits C_{not} et la porte de rotation quantique à un qubit. Cette dernière est définie de manière générale par une simple matrice rotation V(θ,ϕ) faisant tourner le qubit des angles (θ,ϕ) sur la sphère de Bloch. Parmi l'infinité de

portes V(θ,ϕ) une seule (θ et ϕ irrationnels) permet théoriquement d'engendrer toutes les autres par applications répétées. En pratique on n'a pas besoin de recourir à un tel stratagème car on contrôle généralement les angles θ et ϕ à volonté.

Le fait que seulement deux portes soient suffisantes pour fabriquer un QC est la raison principale pour laquelle le concept de porte quantique est si puissant[10,11,12]. Au final, l'évolution de tout système quantique peut ainsi être simulé sur un QC, ce dernier est bien une machine de Turing universelle.

II.3. Les algorithmes quantiques

Nous savons que les ordinateurs classiques sont capables de simuler des comportements quantiques. Comme toutes nos théories de physique s'écrivent en termes d'équations que l'on sait écrire et manipuler sur un ordinateur, il semble hautement improbable que les futures théories de physique fassent naître des problèmes que l'on ne puisse pas simuler sur une machine de Turing classique suffisamment puissante. Comme l'ordinateur classique, le QC est une machine de Turing universelle, capable de simuler à la fois des comportements classiques et quantiques. Mais alors, existent-t-il des calculs qu'un QC puisse faire, et qui restent hors de portée de tous les ordinateurs classiques, les plus puissants soient-ils ?

Cette question est liée à celle de complexité, que l'on aborde en Annexe XI.8. En théorie, un QC n'étend pas, à proprement parler, la classe de problèmes qu'un ordinateur classique sait résoudre. Il permet à certains d'entre eux, d'être résolus plus rapidement. En pratique, un problème 'difficile' peut s'avérer impossible à résoudre, tant sa résolution est longue. C'est pour ce genre de problèmes que le QC apporte une réponse.

II.3.1. Simuler la Nature

La première application d'un QC est celle de simuler des systèmes quantiques. Afin de simuler un vecteur d'état dans un espace de Hilbert à 2^n dimensions, un ordinateur classique a besoin de manipuler des vecteurs contenant 2^n nombres complexes, alors qu'un QC n'a besoin que de n qubits. Simuler l'évolution du système demandera, du côté de l'ordinateur classique, de manipuler des matrices contenant 2^{2n} éléments, alors qu'un QC utilisera des opérations unitaires dans un espace de Hilbert de dimension 2^n. Dans les deux cas, la simulation sera inefficace, et demandera un nombre exponentiel d'opérations ou de portes logiques. Le QC sera ainsi beaucoup plus efficace que l'ordinateur classique en terme de mémoire à stocker, et marginalement plus efficace sur le calcul lui-même. Il n'est donc pas garanti qu'un QC puisse simuler efficacement tous les systèmes quantiques. On a pu montrer cependant, que le QC est plus efficace pour une large classe de systèmes quantiques, incluant plusieurs systèmes pour lesquels il n'y a pas d'algorithme classique efficace, comme les systèmes à plusieurs corps avec interactions locales[13].

II.3.2. L'algorithme de Deutsch-Josza

Dans les années 80, David Deutsch de l'université d'Oxford, fut le premier à imaginer un algorithme quantique mettant vraiment à profit l'intrication[14]. La complexité du problème qu'il permettait de résoudre paraît aujourd'hui assez limitée, mais c'est avant tout la méthode qui a retenu l'attention, et évidemment la primauté de la découverte.

Très schématiquement, l'algorithme de Deutsch permet de détecter en une mesure si une 'pièce de monnaie' quantique est pipée ou non. Une telle pièce est normale si elle comporte un côté pile et un côté face, elle est pipée si les deux faces sont identiques. En physique classique, il faut regarder les deux faces pour savoir avec certitude si une pièce de monnaie est pipée ou non. En physique quantique, grâce à l'intrication et à l'algorithme de Deutsch, une seule mesure est nécessaire. L'algorithme, assez simple, repose pour l'essentiel sur le parallélisme du calcul quantique grâce à la transformation de Hadamart (voir Annexe XI.6).

En 1992, ce problème fut généralisé par Deutsch et Josza, à une fonction à n qubits[15]. Sa résolution fut améliorée en 1998 par Cleve, aboutissant à la forme actuelle de l'algorithme qui porte le nom de Deutsch-Josza[16]. Cet algorithme permet, en une seule mesure, de déterminer si une fonction $f:\{0,1\}^n \to \{0,1\}$ est constante (elle ne donne que des 0 ou que des 1) ou 'balancée' (elle donne la moitié du temps 0 et l'autre moitié 1).

II.3.3. Factoriser en nombres premiers, l'algorithme de Shor

Il existe finalement peu de problèmes pour lesquels il a été démontré que le QC calculerait plus efficacement qu'un ordinateur classique. Cela ne prouve pas qu'il n'en existe pas beaucoup d'autres, mais il reste à les trouver (en soi, ceci constitue un bon stimulant pour poursuivre les recherches théoriques sur l'information quantique). Le principal de ces problèmes est celui de la factorisation d'un nombre en facteurs premiers. Ce problème est d'autant plus difficile que les facteurs premiers en question sont grands, ce qui en fait un élément central des algorithmes de cryptographie actuels, dont le principal est le RSA (Rivest, Shamir, Adleman)[17] expliqué en Annexe XI.9.

La méthode classique la plus efficace pour factoriser un nombre entier N est la méthode GNFS (General Number Field Sieve)[18] qui demande un nombre d'étapes de calcul de l'ordre de $s=\exp(2L^{1/3}(\log L)^{2/3})$, où $L=\ln N$. Le record de factorisation utilisant cette méthode revient à une équipe allemande de la BSI (Bureau fédéral pour la sécurité de l'information), qui en mai 2005 a annoncé

avoir factorisé le RSA 200, c'est-à-dire un nombre entier de 200 digits décimaux, soit 653 bits, en deux nombres premiers de 100 digits. Cette factorisation s'inscrivait dans le cadre du concours 'RSA Factoring Challenge' des laboratoires RSA, qui s'est terminé en 2007. En évaluant la formule ci-dessus, avec $N \sim 2.10^{200}$ soit $L=460$, on trouve $s=7.10^{12}$. Ces quelques 7000 milliards d'étapes de calcul ont été effectuées sur un réseau d'ordinateurs travaillant en parallèle. En ne disposant que d'un seul ordinateur moderne cadencé à 2.2GHz, ce calcul aurait pris environ 75 ans.

Maintenant supposons qu'avec la même technologie, on décide de résoudre le RSA 400, soit un entier à 400 digits au lieu de 200. L se trouve alors doublé et s devient de l'ordre de 2.10^{17}. Le temps de calcul est alors multiplié par un facteur 100,000, ce qui donne environ 7 millions d'années avec les technologies actuelles, rendant ainsi le problème insoluble. La leçon est importante dans le cadre qui nous intéresse : un problème *difficile* théoriquement peut se révéler *impossible* à résoudre en pratique. C'est sur ce point que le QC peut apporter une solution.

S'inspirant du travail préliminaire de Daniel Simon chez Microsoft[19], Peter Shor, à l'époque aux Bell Labs, et maintenant au MIT, dévoila en 1994 et à la surprise générale, un algorithme[20,21,22] permettant à un QC de factoriser un nombre entier avec un temps de calcul polynomial. Cet algorithme repose principalement sur une méthode quantique originale pour trouver la périodicité d'une fonction. Sans entrer dans les détails, relativement complexes et disponibles dans plusieurs articles de revue[1,2], l'algorithme procède en utilisant d'abord l'intrication quantique, qui permet de calculer la fonction sur tous les états possibles. Il mesure ensuite une certaine partie de l'état intriqué obtenu, réduisant ainsi la fonction d'onde sur des états qui correspondent aux valeurs de la fonction. Il applique ensuite à cet état réduit une version quantique de la transformation de Fourier. Enfin, en mesurant les qubits restants de l'état obtenu, il en extrait la période. En disposant d'un tel algorithme, la factorisation est alors relativement aisée. Grâce à l'algorithme d'Euler[23], elle revient à trouver la période d'une fonction particulière ($f(x) = a^x \bmod N$, N étant l'entier à factoriser, et $a<N$ étant choisi aléatoirement).

Plusieurs implémentations de l'algorithme de Shor sur un QC ont été décrites[24,25,26]. Elles requièrent pour l'espace de stockage, environ $4logN$ qubits (soit $\sim 1.7L$) plus $O(logN)$ d'espace supplémentaire, et pour le temps de calcul, environ $300((logN)^3)$ soit $(\sim 25L^3)$ portes quantiques. Ainsi, pour factoriser le RSA 200, un QC disposant d'un tel algorithme aurait besoin d'environ 1200 qubits et 2 milliards de portes quantiques[27]. En considérant un temps d'opération moyen de 1µs par porte quantique, soit un QC cadencé à une fréquence de 1MHz, et sachant que l'algorithme doit être répété plusieurs fois (environ 60) pour aboutir à un résultat fiable, le calcul de factorisation prendrait ainsi environ 33h. Si on compare cette durée aux 75h du record RSA200, tenant compte de la difficulté qu'il y a à réaliser un QC (c'est un euphémisme), ce dernier n'offre clairement pas un avantage décisif par rapport à la technologie classique. En revanche, si on double le nombre de digits en passant au RSA400, on a vu que le problème était impossible à résoudre avec les technologies classiques. Avec un QC, le nombre de qubits est simplement doublé (2400), le nombre de portes quantiques passe à 19 milliards, le temps de calcul est multiplié par 10 environ, soit 330h, ou 14 jours, ce qui reste parfaitement concevable.

L'algorithme de Shor est actuellement le seul exemple d'accélération exponentielle du temps de calcul, ou, formulé différemment, de passage d'une croissance exponentielle à une croissance polynomiale du temps de calcul. Un QC équipé d'un tel algorithme serait alors particulièrement attractif, il permettrait de résoudre efficacement certains problèmes, qui s'avèrent insolubles avec un ordinateur classique. Pour l'instant, cette faculté ne s'applique malheureusement qu'au problème de factorisation.

II.3.4. Chercher dans une base de données : l'algorithme de Grover

Malgré des efforts considérables de la communauté des chercheurs, le nombre d'algorithmes quantiques utiles découverts jusqu'à présent reste relativement limité. Pour la plupart, il s'agit de variantes de l'algorithme de Shor permettant de trouver la période d'une fonction, et de l'algorithme de Grover, permettant de chercher dans une base de donnée non structurée.

Le problème est le suivant : étant donné une liste non structurée $\{x_i\}$, trouver l'élément qui satisfasse $x_i=t$. La liste est dite non-structurée, car on ne fait aucune hypothèse sur l'ordre dans lequel les éléments y sont rangés : connaître x_i ne dit absolument rien sur x_j avec $j>i$. Il pourrait s'agir par exemple de chercher un numéro de téléphone particulier dans le bottin, pour une personne dont on ne connaît pas le nom. Par opposition, une liste structurée suppose que l'on dispose d'un certain type d'information concernant l'espace de recherche. Il s'agirait dans ce cas de chercher directement le nom d'une personne dans le bottin. La recherche serait bien entendu beaucoup plus rapide, car on disposerait alors du classement alphabétique des noms. Un autre exemple est donné par le problème de colorabilité d'une carte avec seulement 3 couleurs. La liste serait ici l'ensemble des affectations de couleurs pour les différents pays, et le problème serait de chercher dans cette liste, les combinaisons qui satisfassent la condition que tous les pays adjacents aient des couleurs différentes. La liste en question est structurée car elle comporte une structure interne qui peut être exploitée par les algorithmes pour rendre la recherche plus efficace.

Concernant la recherche dans une liste non-structurée, on montre facilement qu'avec un ordinateur classique, il est impossible de faire mieux qu'en cherchant tous les éléments de la liste les uns après les autres. Ceci requiert en moyenne *N/2* étapes pour une liste de *N* éléments, ces nombres pouvant facilement augmenter de façon exponentielle avec la taille du problème, ce qui aboutit à une impasse calculatoire pour de grands *N*.

En 1997, L. Grover des Bell Labs présentait un algorithme quantique[28] qui permet de résoudre ce problème en seulement $\approx\sqrt{N}$ étapes. Cet algorithme est présenté brièvement en Annexe XI.10. Il procède schématiquement selon les étapes suivantes. Tout d'abord intervient une parallélisation du calcul, grâce à la transformation de Walsh-Hadamart qui crée une superposition de tous les états de la liste à rechercher. La fonction test est appliquée à cette superposition, et toute l'idée est de faire émerger l'élément recherché de la superposition résultante, en augmentant son amplitude, et donc la probabilité de le mesurer. Pour cela, l'algorithme procède en une succession d'étapes de transformations unitaires correspondant à des inversions par rapport successivement à zéro et à la moyenne. Si la liste ne comprend qu'un seul élément x_0 à rechercher, et si n est le plus petit entier tel que $N \le 2^n$, au bout de $\frac{\pi}{4}\sqrt{2^n}$ étapes, l'algorithme permet de mesurer l'élément x_0 avec un taux d'échec de seulement $2^{-n}=1/N$. Naturellement, en mesurant directement la superposition initiale, le taux d'échec serait de $1-2^{-n}$. Charles Bennet a démontré en 1997 que l'algorithme de Grover était optimal pour la recherche dans une liste non structurée : aucun algorithme quantique ne peut faire mieux[29].

Par rapport aux algorithmes classiques, en faisant passer la recherche de *N/2* à $\sqrt{N}$ étapes, l'algorithme de Grover ne fait pas passer le problème dans une autre classe de complexité. Un problème classé *difficile*, dont le nombre d'étapes augmente exponentiellement avec la taille du problème, demeure *difficile*. En revanche, l'accélération du calcul qui est offerte, d'un facteur $\sqrt{N}/2$ devient très importante lorsque *N* est grand, ce qui est potentiellement intéressant pour le cassage de code cryptés[30]. Pour finir sur un exemple, chercher un numéro de téléphone dans un bottin comportant un million de noms, demanderait un demi million d'étapes sur un ordinateur classique, et seulement 1000 étapes avec un QC disposant de l'algorithme de Grover.

II.4. Les codes correcteurs d'erreurs

Comme on l'a vu dans la section précédente, implémenter un algorithme quantique efficace pour résoudre un problème intéressant, par exemple factoriser un nombre entier comportant plus d'une centaine de digits (chiffres), demanderait de pouvoir disposer de milliers de qubits et de milliards de portes quantiques. On verra dans le chapitre suivant que les meilleurs dispositifs expérimentaux ne permettent pour l'instant que de traiter une petite dizaine de qubits, et tout au plus quelques milliers de portes quantiques. La comparaison met à jour un gouffre béant entre rêve est réalité. A quoi tient une telle différence ?

Le problème principal auquel sont confrontés les dispositifs expérimentaux est celui de la décohérence. L'interaction des qubits avec l'environnement perturbe leur état quantique, et les fait évoluer d'une façon non-unitaire et non-intentionnelle. Il existe bien quelques démonstrateurs de laboratoire exhibant des temps de décohérence record, mais ces temps ne concernent que quelques qubits (1 ou 2). Or, pour réaliser un ordinateur quantique, plusieurs milliers de qubits sont nécessaires, et c'est là tout le problème. Il est en fait irréaliste pour l'instant, de concilier les critères 3 et 5 de la définition de DiVincenzo : un système comportant un grand nombre de qubits aura forcément des temps de décohérence beaucoup trop longs. Steane a même estimé en 1998, que la décohérence d'un système quantique conçu pour factoriser un nombre entier à 130 digits serait 10^7 fois trop élevée[1]. Il serait aujourd'hui plus facile d'imaginer accélérer la puissance de calcul des ordinateurs classiques d'un facteur 10^6 que d'atteindre des temps de décohérence aussi faibles[31].

En réalité, si les ordinateurs classiques fonctionnent aussi bien, c'est qu'ils sont relativement insensibles au bruit, et utilisent sans se priver la dissipation et donc la décohérence. Un interrupteur, par exemple, a besoin pour fonctionner d'amplifier le signal de passage on-off grâce à un ressort, et de dissiper l'énergie accumulée par le mouvement sous forme de chaleur. Sans cette dissipation, il oscillerait continûment entre les deux états on et off, sans jamais s'arrêter. Dans un circuit électronique, la dissipation est assurée par des résistances, mais le principe est le même. Bien évidemment, tout ceci ne s'applique pas pour un QC, la décohérence étant à limiter au maximum et la dissipation étant incompatible avec une évolution unitaire. En outre, le principe de non-clonage (voir Annexe XI.2) nous dit qu'il est impossible d'amplifier un état quantique inconnu. Les principes fondamentaux, à la base de la robustesse des ordinateurs classique, ne s'appliquent donc pas pour un QC.

La situation pourrait donc sembler désespérée, les fondements même de la mécanique quantique laissant à penser qu'il sera à jamais impossible de stabiliser un QC contre les méfaits du bruit. Pourtant, en jouant très subtilement sur les concepts de théorie de l'information, il a été possible de sortir de l'impasse. Les concepts qui ont été découverts portent le nom de correction quantique d'erreur (QEC pour Quantum Error Correction). Leurs principes de base ont été établis en 1996 par Steane[32], Calderbank et Shor[33], sur la base des notions de

'purification de l'intrication' introduites par Bennett[34] et Deutsch[35].

La QEC est basée sur un réseau de portes quantiques et de mesures, et les chercheurs se sont posés la question du degré de perfection que devait posséder un tel réseau pour fonctionner. En d'autres termes, le réseau n'introduit-il pas plus de bruit qu'il n'en supprime ? Shor a montré qu'il était possible de rendre de tels réseaux tolérants vis-à-vis des erreurs au sein même du réseau[36]. La QEC permet donc bien de supprimer plus d'erreurs qu'elle n'en introduit.

Nous n'entrerons pas ici dans le détail de la QEC, qu'on pourra trouver dans plusieurs articles de revue[1,2]. Dans les grandes lignes, le principe est similaire à celui des codes de correction d'erreur classiques : des qubits redondants sont ajoutés pour détecter et corriger les erreurs. La reconstruction est simplement un peu plus complexe à cause du caractère quantique, et de l'impossibilité de copier et cloner les états (théorème du non-clonage). Pour un jeux d'erreurs E_i, la QEC consiste en un code C qui encode un état à n qubits $|\psi\rangle$ en un état à n+k qubits $|\phi\rangle = C|\psi\rangle$, et un 'syndrome d'extraction' S_C qui a pour effet de lever une partie de l'intrication qui affecte l'état d'erreur $\sum_i e_i E_i |\phi\rangle$. La QEC procède tout d'abord en ajoutant un certain nombre de qubits $|0\rangle$ (appelé 'ancilla') à cet état d'erreur, et à lui appliquer le syndrome d'extraction. La mesure des derniers qubits du résultat donne un indice i_0 et un état projeté $E_{i_0}|\phi, i_0\rangle$. On peut alors retrouver l'état original $|\phi\rangle$ en appliquant à cet état projeté la transformation d'erreur inverse $E_{i_0}^{-1}$, correspondant à l'indice i_0.

En théorie, la QEC est efficace et permet de réduire significativement les contraintes de décohérence associées aux qubits. Le problème est que, pour fonctionner sur un QC, elle imposerait des contraintes énormes à ce dernier[37]. Par exemple, supposons qu'un QC 'intéressant' (voir ci-dessus), comporte mille qubits et 10 milliards de portes quantiques. Sans QEC, le taux de bruit par qubit et par porte devrait être inférieur à 10^{-13}, ce qui est totalement irréaliste. Avec la QEC, le taux de bruit tolérable passerait à 10^{-5}, ce qui difficile à réaliser, mais possible. En revanche, le QC devrait alors comporter entre 10 et 100 fois plus de qubits, et introduire pour la correction, un millier de portes supplémentaires pour chaque étape du calcul.

II.5. Forces et faiblesses d'un ordinateur quantique

Après avoir passé en revue les principaux algorithmes quantiques, et les codes quantiques d'erreurs, nous prenons ici un peu de recul et, avec les apports récents des mathématiques sur le sujet, essayons d'évaluer les forces et les limitations d'un QC.

II.5.1. Un ordinateur quantique peut il résoudre P≠NP ?

Comme on l'a vu, l'algorithme de Shor permet une accélération exponentielle du temps de calcul requis pour factoriser un entier en nombres premiers. Ce problème de factorisation est de classe *NP*, c'est-à-dire vérifiable en temps polynomial avec un ordinateur classique (voir Annexe XI.8). En outre, comme il n'a pas été possible jusqu'à présent de le résoudre en temps polynomial avec un algorithme classique, on suppose qu'il n'appartient pas à la classe *P*. Or, l'algorithme de Shor permet à un QC de résoudre ce problème en temps polynomial. Il appartient donc à une nouvelle classe, dite *BQP* (Bounded-error Quantum Polynomial time) [38], de problèmes *NP* qu'un QC permet de résoudre en temps polynomial. Comme le montre la figure suivante, *BQP* inclut *P*, et pour l'instant on pense que $BQP \neq P$ car la factorisation n'est toujours pas résoluble en temps polynomial par un algorithme classique. En réalité, on ne sait pas très bien où se situe la frontière de *BQP*. En dehors du problème de factorisation, et d'un autre problème, dit du logarithme discret, il existe peu d'autres problèmes dans cette catégorie, à l'interface entre *BQP* et *P*.

Le succès de l'algorithme de Shor constitue une performance mathématique indéniable qui a fait couler beaucoup d'encre, mais qui demeure très isolée pour l'instant. Si le problème de factorisation pouvait être *NP-complet*, la situation serait bien différente : sa résolution par un QC en temps polynomial signifierait que tous les problèmes *NP* pourraient être résolus en temps polynomial par ce même QC. Malheureusement, il apparaît presque certain que le problème de factorisation n'est pas *NP-complet*. L'algorithme de Shor exploite en effet des propriétés mathématiques très particulières du problème, qui font que les interférences quantiques sont particulièrement efficaces. Or les problèmes *NP-complets* ne possèdent pas de telles propriétés. Pour être *NP-complets*, leurs propriétés ont plutôt tendance à être très générales, s'appliquant à tous les problèmes. C'est le cas, par exemple, du problème de recherche dans une liste non-structurée. Comme on l'a vu, ce problème peut être résolu par un QC grâce à l'algorithme de Grover, mais pas en temps polynomial. Ce problème *NP-complet* est un problème *difficile* à résoudre, que ce soit avec un ordinateur classique ou avec un QC.

La question principale que l'on se pose est la suivante : existe-t-il un algorithme quantique capable de résoudre efficacement (en temps polynomial) un problème *NP-complet* ? Pour l'instant, personne n'a été capable d'en mettre à jour, mais personne n'a été capable non plus de démontrer qu'un tel algorithme n'existe pas. Après tout,

personne n'a pu prouver qu'il n'existe pas non plus d'algorithme classique capable d'un tel exploit. Ce que l'on peut dire, c'est qu'un tel algorithme quantique devrait, comme celui de Shor, exploiter la structure du problème d'une manière spéciale, que l'on ne sait pas concevoir aujourd'hui. Le problème est qu'une telle exploitation 'magique' du problème pourrait, de la même manière, être mise à profit par un ordinateur classique. Le QC n'apporterait pas alors un avantage décisif par rapport à son homologue classique. Avec une telle perspective, beaucoup de chercheurs pensent aujourd'hui que, non seulement *P≠NP*, mais qu'en plus un QC ne sera jamais capable de résoudre un problème *NP-complet* en temps polynomial[39].

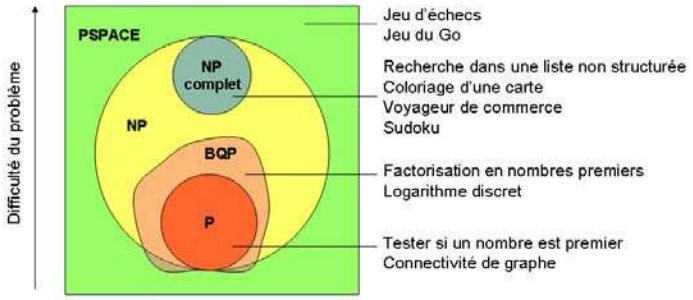


Figure 2 Classes de complexité, et la situation de quelques exemples de problèmes. La classe BQP est celle des problèmes qu'un QC peut résoudre en temps polynomial. Il est possible que BQP déborde de NP, c'est-à-dire qu'il existe des problèmes qu'un QC résolve plus vite que le temps pris par un ordinateur classique pour en vérifier la solution. Image reproduite d'après : S. Aaronson, Scientific American, 63-69, March 2008

II.5.2. L'ordinateur quantique adiabatique

L'ordinateur quantique adiabatique est un concept intéressant, reposant sur des principes physiques différents de ceux du QC traditionnel tel qu'on l'a exposé jusqu'ici. Ce concept a suscité beaucoup d'espoirs et de polémiques, car certains chercheurs ont affirmé qu'il était capable de résoudre des problèmes NP-complets[40,41].

Le principe de fonctionnement d'un ordinateur quantique adiabatique repose sur une évolution lente et contrôlée du Hamiltonien d'un système[42]. Schématiquement, le problème que l'on désire résoudre est tout d'abord traduit sous la forme d'un système physique tel, que la solution du problème soit donnée par son état fondamental. Cet état étant inconnu, l'idée du calcul adiabatique est de modifier le système en question, en un autre système dont on connaît l'état fondamental. Exprimé différemment, cela revient à changer le Hamiltonien du système que l'on ne sait pas résoudre, pour un Hamiltonien qui soit solvable. Une fois ce nouvel Hamiltonien résolu, et l'état fondamental du système connu, le système est très progressivement ramené vers le système initial. Si la modification du Hamiltonien est suffisamment lente, on montre que le système reste dans l'état fondamental, qui représente alors la solution du problème de départ. La mesure de cet état donne la solution correcte de manière probabiliste, mais avec un taux de succès d'environ 90%.

Une des difficultés principales de ce concept réside dans la lenteur du procédé, qui nuit à la vitesse d'opération de l'ordinateur. En effet, si les changements du Hamiltonien sont trop rapides, le système sortira de l'état fondamental par sauts, pour aller explorer des états excités. Des travaux théoriques ont montré que ces sauts ont une chance très importante d'avoir lieu en des points bien spécifiques lors de la transformation du Hamiltonien. En ces points, les niveaux excités sont proches du niveau fondamental, favorisant ainsi l'excitation incontrôlée. La transformation du Hamiltonien doit alors se faire très lentement au passage de ces points. Elle peut toutefois être bien plus rapide le reste du temps, ce qui est préconisé pour éviter de ralentir dramatiquement l'ordinateur.

Expérimentalement, il a été suggéré qu'une architecture d'ordinateur quantique adiabatique pouvait être réalisée à l'aide de circuits supraconducteurs, et de courants permanents circulant à travers des jonctions Josephson. L'entreprise canadienne D-Wave prétend avoir fait la démonstration d'un circuit à 28 qubits utilisant ce principe. Cette affirmation laisse toutefois sceptique la communauté scientifique[43].

Ses partisans attribuent au concept d'ordinateur quantique adiabatique des propriétés remarquables. Il serait très robuste à la décohérence, et permettrait de résoudre tous les problèmes en temps polynomial. Il est apparu cependant que beaucoup de ces affirmations n'ont pas survécu au processus de 'peer review' des principaux journaux scientifiques. Il se pourrait, entre autres, que les simulations mises en avant pour étayer la théorie sous-estiment l'influence des niveaux excités, en ne prenant en compte que les 100 premiers[44]. Outre ces problèmes théoriques, qui font encore débat dans la communauté scientifique, les difficultés expérimentales pour réaliser un premier prototype sont certainement bien plus grandes que ce que prétend l'entreprise D-Wave.

II.6. Vers les premières réalisations expérimentales

La plupart des portes quantiques élémentaires ont déjà été réalisées expérimentalement à l'aide de dispositifs quantiques simples : par exemple, les portes NOT et XOR peuvent être modélisées respectivement par l'émission stimulée entre deux niveaux d'énergie et par une transition dans un système à 4 niveaux. Tout l'enjeu consiste à passer de ces dispositifs de base à un véritable ordinateur quantique, comportant plusieurs qubits en communication, que l'on peut commander et mettre en mémoire à souhait. Durant les dix dernières années, la communauté scientifique mondiale a été très dynamique sur ce sujet, les

Etats-Unis faisant office de chef de file. Un grand nombre de pistes très prometteuses ont été suivies:

- les qubits supraconducteurs
- les qubits semiconducteurs à boites quantiques
- les ions piégés
- la résonance magnétique nucléaire en solution
- les réseaux d'atomes froids
- l'optique quantique

Dans les chapitres suivants, nous décrirons ces différentes approches expérimentales, leurs principes et les avancées majeures les plus récentes.

L'approche la plus naturelle est de considérer le QC comme une prolongation de l'ordinateur classique, utilisant comme substrat des matériaux solides comme les semiconducteurs, ou les supraconducteurs. Cette approche est séduisante, car elle autorise l'utilisation des procédés de fabrication éprouvés de la microélectronique, permettant la miniaturisation et l'augmentation exponentielle de puissance des circuits classiques que l'on connaît. Cependant, elle se heurte aussi à des problèmes de bruit, liés à la nature macroscopique des substrats, et à leur couplage inévitable avec les qubits. En effet, le calcul quantique est basé sur des phénomènes d'interférences quantiques extrêmement subtils et fragiles, sensibles à la décohérence, c'est à dire détruits à la moindre interaction avec l'environnement. Dans le cas des substrats de type semiconducteur (a fortiori supraconducteurs), il faudra donc refroidir à de très basses températures, de l'ordre du Kelvin.

En comparaison, l'approche utilisant des ions piégés repose sur des principes totalement différents, et semble à priori plus complexe et éloignée de l'ordinateur quantique tel qu'on pourrait l'imaginer. Pourtant, les progrès récents, lui ont donné une véritable impulsion, et permettent d'en espérer beaucoup.

Actuellement, ces deux approches sont considérées comme les plus prometteuses par la communauté scientifique[160].

III. LES CIRCUITS SUPRACONDUCTEURS

Une des approches les plus séduisantes pour aborder l'ordinateur quantique consiste à utiliser des circuits électroniques utilisant des substrats solides, autorisant l'usage des techniques de lithographie de la microélectronique, et permettant de concevoir des circuits complexes avec un contrôle spatial précis des qubits et une précision nanométrique. La principale difficulté liée à cette approche est la décohérence quantique engendrée par le couplage du qubit à son environnement. En effet, contrairement aux dipôles électriques d'atomes ou d'ions isolés, les variables d'état d'un circuit électronique (courant, tension) subissent une décohérence quantique rapide due à un fort couplage avec un environnement comportant un grand nombre de degrés de liberté. Les supraconducteurs procurent de nombreux avantages par rapport aux semiconducteurs. Non seulement ils permettent d'annuler toutes les dissipations électroniques, mais ils permettent également de disposer d'un état quantique macroscopique appelé condensat supraconducteur.

III.1. Principes de base[45]

En dessous d'une certaine température critique, les électrons d'un supraconducteur s'associent en paires appelées paires de Cooper. L'état fondamental du supraconducteur peut être ainsi vu comme un condensat de Bose-Einstein de ces paires de Cooper dans un état quantique macroscopique. Cet état est caractérisé en tout point par un paramètre d'ordre Δ donné par : $\Delta = |\Delta| e^{i\varphi}$ où $|\Delta|$ est le « gap » en énergie du supraconducteur et φ est la phase supraconductrice. Lorsque l'énergie thermique est suffisamment petite $k_B T \ll |\Delta|$, toutes les excitations microscopiques étant gelées, cette phase constitue un degré de liberté macroscopique très robuste du système. L'état électronique fondamental du système est un unique état bien séparé énergétiquement des états excités à quasi-particules.

La jonction Josephson est une brique de base pour construire un qubit supraconducteur. Elle est formée de deux électrodes supraconductrices couplées faiblement par effet tunnel à travers une fine couche isolante. La jonction est alors caractérisée par deux énergies : l'énergie Josephson E_J qui caractérise la « force » du couplage tunnel, et l'énergie de charge d'une paire de Cooper sur la capacitance de la jonction, $E_C = (2e)^2 / 2C$. Ces deux énergies sont associées dans le « Hamiltonien » de la jonction : $H = E_C \hat{n}^2 - E_J \cos\hat{\delta}^2$ où δ est la différence des phases φ des électrodes de part et d'autre de la jonction, et où n est le nombre de paires de Cooper ayant traversé la jonction[i].

Lorsque $E_C \gg E_J$, c'est-à-dire pour les petites jonctions (surface inférieure à $0.1\mu m^2$ pour des jonctions en aluminium), les états propres du système (constitué de la jonction seule) sont proches d'états dits de charge, dans la limite opposée $E_C \ll E_J$ on est proche d'états dits de phase.

[i] *Ces deux variables sont conjuguées quantiquement : $\left[\hat{n}, \hat{\delta}\right] = i$, donnant en particulier la relation d'incertitude $\Delta n \Delta\delta \geq 1$, phase et nombre de paires de Cooper ne pouvant pas être déterminées simultanément avec précision arbitraire.*

Il y a principalement deux manières de construire un qubit supraconducteur, qui diffèrent par la façon de coder l'information quantique. La première approche consiste à se placer dans la limite $E_C \gg E_J$ en utilisant de petites jonctions Josephson (surface inférieure à $0.1\mu m^2$ pour des jonctions en aluminium), délimitant un îlot supraconducteur dont la charge électrique est bien définie. Les états de base de tels 'qubits de charge' appelés également boîtes à électrons, sont les états de charge de l'îlot,.

La deuxième approche se place dans la limite opposée $E_C \ll E_J$ utilise des jonctions Josephson plus grandes, et se base sur la cohérence quantique macroscopique entre des états de flux magnétique. Elle donne des qubits appelés 'qubits de phase'. Il s'agit de réalisations particulières du fameux SQUID.

Entre ces deux cas limites, on trouve plusieurs cas intermédiaires, donnant les 'qubits de flux' et les 'qubits de charge-flux'. En résumé, les différentes catégories de qubits supraconducteurs que nous analysons par la suite, sont les suivantes :

- Qubits de charge ($E_J / E_C \ll 1$) - Chalmers (Suède), NEC (Japon)
- Qubits de charge-flux ($E_J / E_C \approx 1$) - CEA, Yale
- Qubits de flux ($E_J / E_C \approx 10$) - Delft
- Qubits de phase ($E_J / E_C \gg 1$) - UCSB, NIST

III.2. Les qubits de charge

Un qubit de charge est réalisé à l'aide d'un petit îlot supraconducteur, dont les dimensions n'excèdent pas quelques centaines de nanomètres, et qui est relié à une électrode supraconductrice à l'aide d'une jonction Josephson de faible capacitance[46]. Un tel dispositif utilise l'effet tunnel cohérent des paires de Cooper, qui est, dans une certaine mesure, similaire à l'effet tunnel des électrons passant entre de très petits îlots conducteurs que l'on trouve dans les dispositifs de transistors à électrons uniques utilisant les phénomènes de blocage de Coulomb. Ces îlots doivent être suffisamment petits pour que les énergies de charge des électrons ou dans notre cas, des paires de Cooper, dominent toutes les autres énergies du système, notamment l'énergie de couplage de la jonction Josephson : $E_C \gg E_J$. La charge de l'îlot constitue alors le degré de liberté principal du qubit de charge, les états de base $|0\rangle$ et $|1\rangle$ différant par le nombre de paires de Cooper présentes sur l'îlot.

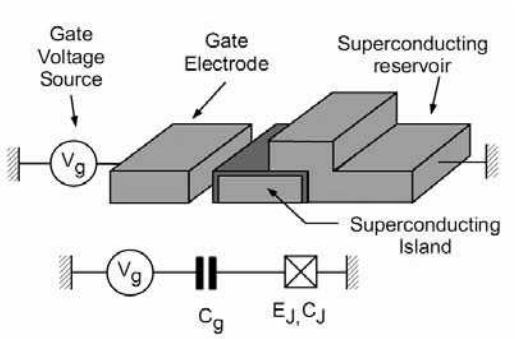


Figure 3 Schéma de principe d'un qubit de charge, dans sa version la plus simple. L'îlot supraconducteur est relié au réservoir supraconducteur par une jonction Josephson, et une tension de contrôle est appliquée via une grille. Les états de base $|0\rangle$ et $|1\rangle$ diffèrent par le nombre de paires de Cooper présentes sur l'îlot. Tiré de la thèse de Audrey Cottet, groupe quantronique (CEA)[47].

Le qubit de charge le plus simple est illustré sur la figure ci-dessus. Il consiste en un petit îlot supraconducteur comportant un nombre excédentaire *n* de paires de Cooper, relié à un réservoir supraconducteur par une jonction Josephson de capacitance C_J et d'énergie E_J. Une grille de contrôle de capacitance C_G applique à l'îlot une tension V_G.

A basse température (de l'ordre du mK), les seules charges qui traversent la jonction par effet tunnel sont les paires de Cooper. De manière plus précise, le Hamiltonien du système peut s'écrire : $H = 4E_C\left(\hat{n} - n_G\right)^2 + E_J \cos\hat{\delta}$, où $E_C = e^2/\left(2\left(C_J + C_G\right)\right)$ est l'énergie de charge de l'îlot, $n_G = C_G V_G / 2e$ est la charge induite sur la grille et δ est la différence de phase supraconductrice entre l'îlot et le réservoir. Lorsque $n_G = 1/2$, les énergies de charge associées aux états *n*=0 et *n*=1 sont égales, ce qui rend ces états dégénérés, et les mélangent via l'énergie de couplage de la jonction Josephson. Seuls alors les états *n*=0 et *n*=1 jouent un rôle, les autres ayant des énergies bien supérieures, et le qubit de charge se comporte comme un système quantique élémentaire à deux niveaux $|0\rangle$ et $|1\rangle$.

La manipulation du qubit se fait principalement en modifiant la tension de grille. Afin de pouvoir atteindre tous les points sur la sphère de Bloch, le dispositif élémentaire exposé ci-dessus est remplacé par un dispositif un peu plus évolué faisant intervenir deux jonctions Josephson formant une boucle supraconductrice, c'est-à-dire un SQUID[48] (voir annexe ainsi que la figure suivante). Dans cette version, un courant appliqué à une ligne de contrôle extérieure, couplée inductivement avec le SQUID, induit un flux magnétique Φ dans le SQUID modifiant la phase δ aux bornes des deux jonctions en série, et rendant l'énergie Josephson réglable.

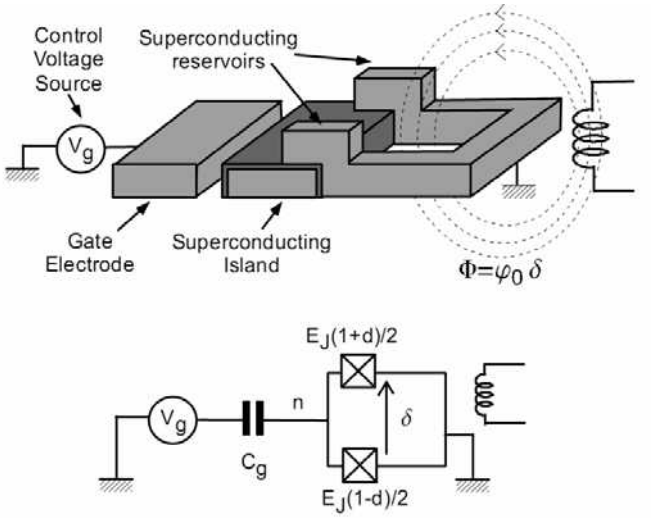


Figure 4 Un qubit de charge comportant deux jonctions Josephson au lieu d'une, et une structure en boucle formant un SQUID. Le dispositif comporte deux paramètres de contrôle : la tension de grille V_G ainsi que le flux Φ dans la boucle, qui permet de modifier le déphasage δ entre les deux jonctions, et donc l'énergie Josephson effective du qubit. Tiré de la thèse de Audrey Cottet, groupe quantronique (CEA).

III.3. Le Quantronium

En 1998, le groupe Quantronique du CEA à Saclay, autours de Michel Devoret et Daniel Estève, a été le premier a concevoir, réaliser et faire fonctionner des boîtes à paires de Cooper. Dans l'expérience de Vincent Bouchiat, le nombre moyen de paires de Cooper dans l'îlots était mesuré à l'aide d'un transistor à électron unique[49,50].

Un an plus tard, le groupe de Nakamura des laboratoires NEC au Japon reprenait le concept, en le complétant d'un dispositif de mesure comprenant une jonction additionnelle fortement polarisée en tension, et d'un dispositif de pilotage des qubits par impulsions de grille ultra-rapides[51]. Le qubit de charge étant préparé dans la superposition des états propres n=0 et n=1 décrite plus haut, les auteurs ont pu en mesurer les oscillations quantiques cohérentes. Cette expérience historique marque l'avènement des qubits dans des circuits électroniques. La mesure était effectuée en détectant un courant tunnel traversant une sonde additionnelle. Bien que cette expérience était la première à mesurer une superposition cohérente des états $|0\rangle$ et $|1\rangle$, le temps de cohérence du système n'excédait pas quelques ns, à cause de la décoherence due au dispositif de mesure lui-même, et du bruit de charge crée par les charges présentes à proximité de l'îlot.

Afin de résoudre ces problèmes, le groupe Quantronique du CEA, reprenait le concept de sa boîte à paires de Cooper, et développait en 2002 un nouveau circuit appelé 'Quantronium'[52]. Ce circuit comportait un dispositif de mesure utilisable sur commande, et préservant beaucoup mieux la cohérence du qubit . A cette époque, les premières expériences sur les qubits de flux donnaient des temps de cohérence très faibles, qui pouvaient être attribués à des fluctuations dans les paramètres de contrôle donnant des variations dans les fréquences de transition des qubits et des déphasages. Le quantronium a été développé dans un souci de minimiser ces fluctuations, avec une architecture le protégeant de ces déphasages.

Le quantronium est composé d'un îlot couplé à un réservoir en boucle (SQUID) par deux petites jonctions Josephson. Le dispositif de mesure fait intervenir une plus grosse jonction Josephson insérée dans la boucle du réservoir, aux bornes de laquelle vient se greffer un circuit parallèle de mesure comportant une source de courant et un lecteur de tension. L'état du qubit est préparé à l'aide de la tension de grille U et du flux magnétique Φ traversant le SQUID, qui est crée à l'aide d'une bobine d'induction extérieure. Cet état est ensuite manipulé en appliquant des impulsions microondes u(t) à la grille de commande. Il est finalement mesuré en appliquant une impulsion de courant I_b(t) à la grosse jonction Josephson, et en lisant la tension à ses bornes, qui dépend de l'état du qubit $|0\rangle$ ou $|1\rangle$.

Le quantronium fonctionne dans le régime $E_J / E_C \approx 1$, où énergie Josephson et énergie de charge sont de même ordre de grandeur. Pour cette raison, il est qualifié de qubit de charge-flux. On verra dans la partie suivante, consacrée aux qubits de flux, que ces derniers ont des états propres dégénérés correspondants à des courants permanents circulant dans la boucle du SQUID en sens inverse. Opéré à n_G=1/2, le quantronium se place également dans une superposition de ces états propres à courants inversés, ce qui permet de les discriminer à la mesure. Dans la littérature, on trouve également le qualificatif de qubit de charge-phase, car le quantronium est piloté en charge et lu en phase.

Grâce au quantronium, l'équipe du CEA a pu mesurer les oscillations de Rabi du qubit, prouvant qu'il s'agit bien d'un contrôle quantiquement cohérent d'un système à deux niveaux. Par ailleurs, la mesure du temps de relaxation du système a donné T_1=1.8µs. Les oscillations de Rabi ne sont toutefois pas suffisantes pour mesurer le temps de cohérence du système en évolution libre T_2. Pour ce faire, une mesure des franges de Ramsey a donné $T_2 = 0.5\mu s$, ce qui permet d'envisager une moyenne de 8000 précessions libres avant décohérence. Le facteur de qualité de cohérence quantique vaut alors 25000, ce qui est suffisant pour envisager des calculs quantiques simples, à condition que ce temps de cohérence soit conservé dans des échantillons à plusieurs qubits réalisant des fonctions logiques.

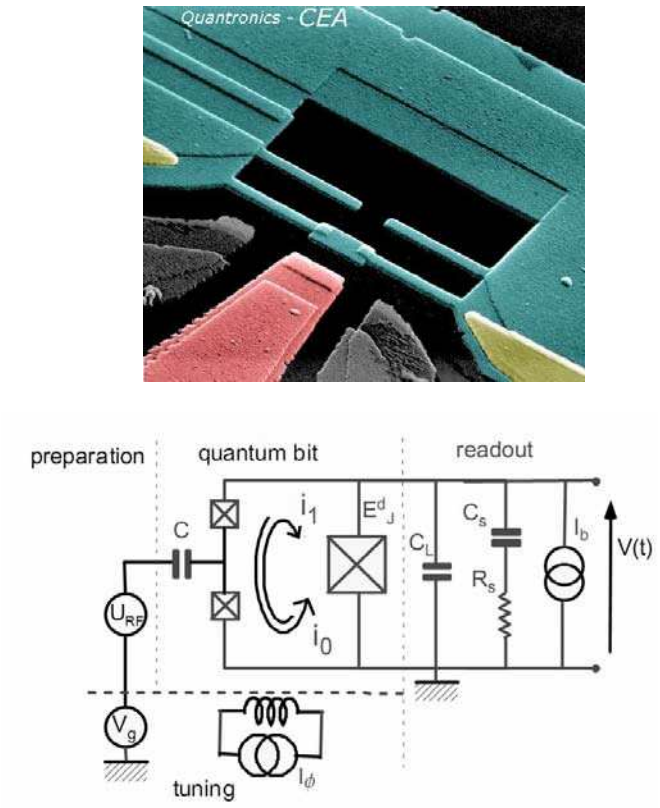


Figure 5 Haut: micrographie électronique du circuit Quantronium réalisé par l'équipe du CEA en 2002. La boucle principale avec ses trois jonctions Josephson est en bleu, la grille de commande en rouge, et les électrodes jaunes sont des pièges à quasi-particules. Bas : schéma simplifié du circuit. Crédits : D. Vion, CEA Saclay

Avec une valeur proche de la microseconde, le Quantronium a été pendant longtemps le qubit présentant le temps de cohérence le plus long[ii]. Son succès, en tant que qubit de charge-flux, a semble-t-il quelque peu éclipsé les recherches portant sur les qubits de charge purs, au détriment des qubits de flux ou de phase, qui bénéficient d'une plus grande facilité de fabrication, et d'une sensibilité moindre aux défauts de réalisation, ce qui leur confère une plus grande robustesse.

Pourtant, les qubits de charge ont bénéficié quelques de propositions théoriques[53] intéressantes, et de réalisations expérimentales remarquables. Notamment, une équipe japonaise, autours des professeurs Tsai et Nakamura, a utilisé des qubits de charge avec grand succès, en montrant d'abord le couplage cohérent entre deux qubits[54], puis en réalisant une porte quantique C_{not} à l'aide de deux qubits[55].

III.4. Les qubits de flux

Contrairement aux qubits de charge, dont l'état dépend de la présence ou non d'une paire de Cooper sur un îlot de dimensions nanométriques, les qubits de flux s'intéressent à des courants macroscopiques qui mettent en jeux des milliards d'électrons se déplaçant de façon cohérente, et autorisant ainsi des interférences quantiques à l'échelle macroscopique.

De manière générale, un qubit de flux est un SQUID RF à une jonction dont la dynamique est contrôlée par la différence de phase de part et d'autre de la jonction (plutôt que par la charge dans le cas du qubit de charge). En reprenant les résultats de l'annexe consacrée au SQUID, on voit qu'en fixant le flux magnétique extérieur à $\Phi_{ext} = \Phi_0 / 2$, le système est dégénéré est peut être réduit à un système à deux états, constituant alors les états de base $|0\rangle$ et $|1\rangle$ du qubit. La variable de commande est alors le champ magnétique extérieur, qui permet de procéder à toutes les opérations élémentaires sur le qubit.

Les qubits de flux sont fabriqués de telle manière à ce que l'énergie de la jonction Josephson soit supérieure à celle de l'énergie de charge, d'un facteur 10 environ : $E_J \approx 10 E_C$. Les jonctions Josephson sont plus grosses que celles des qubits de charge, et donc plus faciles à fabriquer et à tester individuellement. En revanche, les qubits de flux à trois ou quatre jonctions (voir ci-dessous) sont difficiles à fabriquer car il faut contrôler avec une très grande précision les tailles relatives des jonctions. Les qubits de flux semblent plus robustes que les qubits de charge car ils sont complètement insensibles aux mouvements des charges autours des jonctions.

Une des équipes les plus en pointe dans l'exploration des propriétés des qubits de flux est celle du Professeur Mooij à l'université de technologie de Delft, aux Pays Bas. En 1999, dans le journal Science[56], elle proposait un concept de qubit en flux à trois jonctions Josephson, qui allait par la suite être repris dans la plupart des travaux du groupe. Il s'agit d'un SQUID comportant 3 petites jonctions Josephson d'énergies E_J, E_J, et 0.75 E_J, qui comporte deux états stables de flux $|0\rangle$ et $|1\rangle$ correspondant à 0 et 1 quantum de flux dans la boucle, et aux deux sens de circulation d'un même courant permanent (voir figure ci-dessous). Le qubit est commandé par application d'un flux magnétique extérieur dans la boucle.

[ii] *Aujourdhui les temps de cohérence atteignent 2 voire 4 µs dans certains transmons de Yale et certains qubits en flux de NEC*

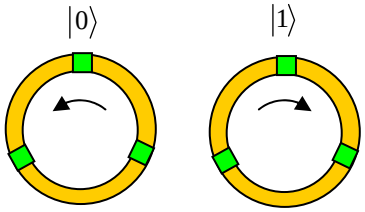


Figure 6 Les états de base $|0\rangle$ et $|1\rangle$ d'un qubit de flux tel que proposé en 1999 par le groupe de J. E. Mooij à l'université de Delft.

En 2000, presque simultanément avec un groupe de l'université Stony Brooks à New York[57], le groupe de Mooij observait expérimentalement la superposition cohérente des deux états à courants permanents, à l'aide de leur qubit de flux à 3 jonctions[58]. Les deux groupes utilisaient des techniques de spectrométrie permettant de mesurer la séparation des niveaux d'énergie, plus précisément l'anti-croisement des niveaux, dû au couplage tunnel entre les deux états macroscopiques. Il restait encore à démontrer la cohérence quantique macroscopique (MQC) dans le domaine temporel. Ceci fut fait en 2003, toujours par le groupe de Mooij[59], en utilisant un qubit de flux à trois jonctions attaché à un SQUID comportant deux plus grosses jonctions Josephson (voir figure ci-dessous). Les mesures d'oscillations de Rabi et Ramsey donnaient respectivement un temps de relaxation des états de 900ns et un temps de déphasage de 20ns. Actuellement, le même qubit en flux opéré au bon point de travail donne des temps de cohérence dépassant la microseconde.

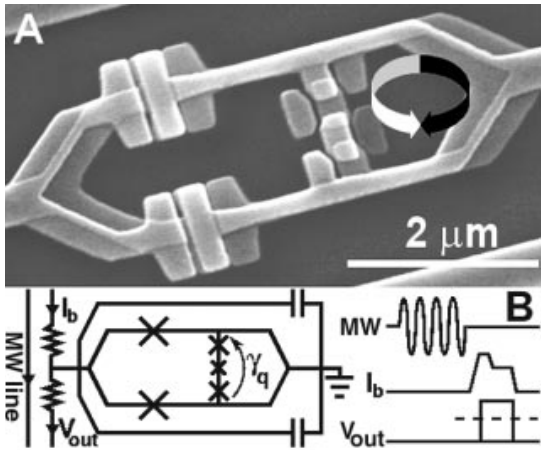


Figure 7 Image par microscope électronique (haut) et circuit schématique du qubit de flux à trois jonctions Josephson utilisé par le groupe de Mooij (Université de Delft) en 2003 pour démontrer la cohérence quantique macroscopique dans le domaine temporel. Les deux états en superposition sont des courants permanents circulant en sens inverse, comme représenté en haut par les deux flèches blanche et noire. Le reste du circuit sert à la lecture des états et à la commande par injection de flux magnétique (MW line). Crédits : J. E. Mooij, dans I. Chiorescu et al Science 299, 1869 (2003)

Poussé par un tel succès, le groupe de Delft a poursuivi ses travaux très activement, toujours en utilisant son qubit à flux à 3 jonctions. En 2005, il a fait état du couplage de deux qubits mesurés spectralement[60], et en juin 2007 il publiait la démonstration éclatante de la réalisation d'une porte C_{not} à l'aide de deux qubits[61], mais nous n'entrerons pas ici plus dans les détails.

Pour en revenir aux recherches américaines, le groupe de John Clarke à l'université UC Berkeley publiait en 2006 un article faisant état du couplage cohérent et réglable entre deux qubits de flux[62]. Les deux qubits étaient couplés par leur inductance mutuelle et par un SQUID qui en même temps lisait leur état de flux magnétique (voir figure), comme pour le dispositif utilisé par le groupe de Delft en 2005. Dans les expériences des deux groupes, la mise en évidence du couplage se faisait spectralement par une mesure de la séparation (splitting) des niveaux d'énergie des deux qubits au voisinage de leur point de croisement.

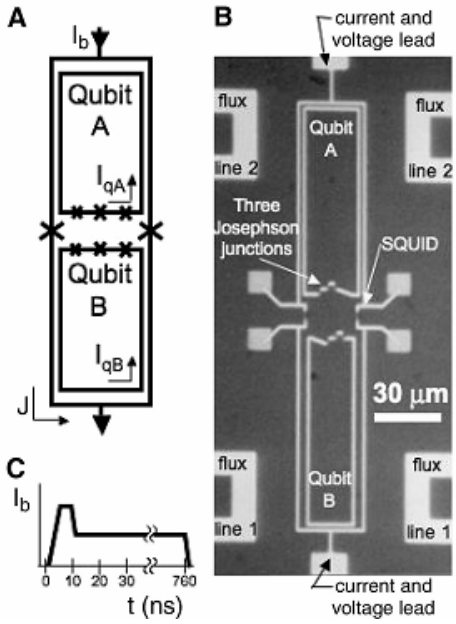


Figure 8 Expérience de couplage réglable entre deux qubits de flux, présentée par le groupe de John Clarke de l'université de Berkeley. Les deux qubits A et B sont entourés par un SQUID extérieur qui mesure leur états de flux et contrôle leur couplage inductif. Crédits : John Clarke, UC Berkeley, dans T. Hime, et al. dans Science 314, 1427 (2006)

III.5. Les qubits de phase

A l'époque où l'équipe du CEA dévoilait son Quantronium et ses temps de cohérence record, la communauté scientifique prenait conscience des problèmes de décohérence auxquels étaient confrontés la plupart des autres qubits : les qubits de charge étaient particulièrement sensibles au bruit de charges et les qubits de flux au bruit de flux magnétique. C'est dans ce

contexte que John Martinis, à l'époque au NIST à Boulder dans le Colorado, a développé les qubits de phase[63].

Un qubit de phase fonctionne dans la limite $E_J / E_C \gg 1$ où l'énergie Josephson est nettement plus grande que l'énergie de charge. Cette limite est atteinte pour des circuits comportant de très larges jonctions Josephson, typiquement 10µm, pour lesquelles l'énergie de charge est très faible, assurant ainsi une immunité au bruit de charge. Le qubit reste sensible au bruit de flux, mais dans des proportions théoriquement raisonnables, et il possède d'autres avantages intéressants. Le premier est qu'il ne fonctionne pas avec des paramètres réglés sur un point d'opération optimal, ce qui facilite grandement le couplage de plusieurs qubits. Un deuxième avantage est qu'il dispose d'une méthode de mesure originale, en 'single-shot', c'est-à-dire où chaque mesure donne directement la valeur du qubit, 0 ou 1, sans devoir recourir à des mesures supplémentaires.

Un qubit de phase consiste en une large jonction Josephson, formant une capacité et une inductance parallèles (voir schéma de la figure suivante). La dynamique du système est contrôlée par la variable δ, la différence de phase de part et d'autre de la jonction. Lorsque la jonction est placée dans un SQUID RF (voir l'annexe sur les SQUIDs) et qu'elle est parcourue par un courant proche du courant critique, l'énergie du système U forme un double puits de potentiel asymétrique en fonction de δ. Les deux états de plus basse énergie du puits le moins profond (à gauche sur la figure) correspondent aux états quantiques $|0\rangle$ et $|1\rangle$ séparés par une énergie E_{01}. Des impulsions microondes rapides à la fréquence $\nu_{01} = E_{01} / h$ permettent de préparer une superposition quelconque de ces deux états. Une fois que la préparation est complète, une impulsion rapide de flux modifie l'asymétrie entre les deux puits de potentiels, en diminuant la barrière entre eux. Si le qubit est dans l'état $|1\rangle$ la particule (fictive) de phase peut passer par effet tunnel dans le puits adjacent plus profond, ce qui cause un changement soudain de δ, et induit un flux magnétique dans la boucle. En revanche, si le qubit est dans l'état $|0\rangle$, il ne se passe rien. La différence entre les deux états $|0\rangle$ et $|1\rangle$ peut ainsi être détectée avec un SQUID couplé inductivement avec le qubit.

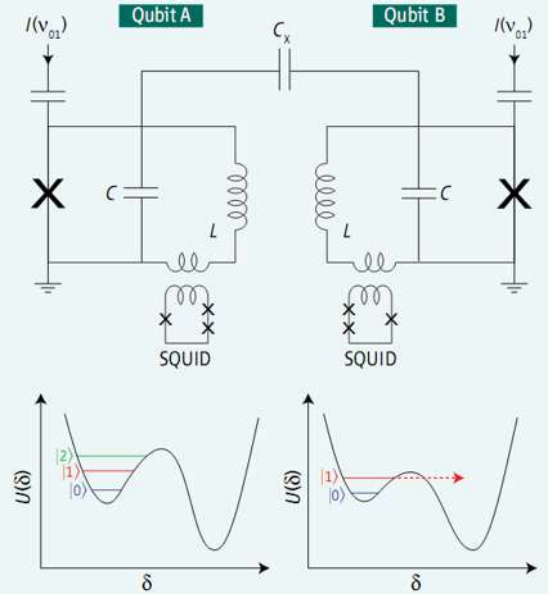


Figure 9 Haut: Schéma électrique de deux qubits de phase couplés par une capacitance et commandés par une source de courant micro-ondes. Bas : Energie potentielle d'un qubit de phase en fonction de la différence de phase δ. A gauche, les états $|0\rangle$ et $|1\rangle$ sont confinés dans le puits de potentiel. A droite, une impulsion de flux abaisse la barrière et le système quitte l'état $|1\rangle$ en traversant la barrière. C'est le principe de mesure 'single-shot' du qubit de phase. Crédits : Irfan Siddiqi et John Clarke, UC Berkeley, dans Science 313 1400 (2006)

En 2005, l'équipe de John Martinis, alors à UCSB, parvenait à coupler deux qubits de phase et d'en observer les corrélations cohérentes[64]. Le circuit utilisé pour cette expérience est montré dans l'image du haut de la figure précédente[65]. En 2006, la même équipe introduisait une architecture améliorée du qubit de phase[66], séparant explicitement la capacitance parallèle de la jonction Josephson, et aboutissant à des mesures de temps de relaxation et de temps de cohérence de T_1=110ns et T_2=90ns. Ces valeurs sont certes inférieures à celles des qubits en charge et en flux, mais l'architecture particulière de ce qubit de phase permettait d'obtenir une fidélité de mesure remarquable de 90%, et ainsi d'envisager des mesures d'intrication par tomographie d'état, comme on le décrit dans le paragraphe suivant.

III.6. Bus quantique et stockage d'état

Après le départ de John Martinis, l'activité du NIST à Boulder sur les qubits de phase s'est poursuivie autours de Raymond Simmonds. Récemment, son groupe à démontré le couplage de deux qubits de phase à l'aide d'une cavité micro-ondes, et le transfert cohérent d'états entre les deux qubits[67]. L'expérience présente des similitudes avec celle du groupe de Yale utilisant des transmons (voir le paragraphe consacré aux transmons). Le montage utilisé est illustré sur la figure suivante. Les deux qubits sont

couplés par une cavité demi-onde de 7mm (les qubits en bouts de cavité sont donc situés aux ventres du champ électromagnétique).

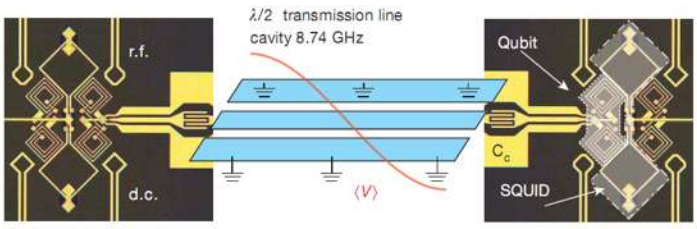


Figure 10 Illustration du couplage de deux qubits de phase par une cavité micro-ondes. Ce montage à permis à l'équipe de Ray Simmonds au NIST à Boulder, de démontrer le transfert cohérent et la mise en mémoire d'états quantiques. Crédit : R. Simmonds, NIST dans M. Sillanpää et al. Nature, **449**, 438 (2007)

L'état des qubits est préparé et modifié à l'aide d'impulsions rapides de flux apportées par des bobines RF (en haut sur la micrographie de l'image précédente). L'énergie des qubits est modifiée à l'aide d'impulsions de flux apportées par des bobines DC (en bas sur la micrographie). Le couplage entre les qubits et la cavité s'effectue en modifiant leur désaccord de fréquence, de manière à ce que les qubits soient résonants ou non avec la cavité. Le transfert d'état entre le qubit A (à gauche) et le qubit B (à droite) s'effectue de la manière suivante : Utilisant les bobines DC, les deux qubits sont d'abord mis hors résonance avec la cavité. Une impulsion de flux RF prépare alors le qubit A dans une superposition d'états $|0\rangle$ et $|1\rangle$. Le qubit A est ensuite mis en résonance avec la cavité pendant un temps t_A suffisant pour qu'il s'intrique avec cette dernière. L'état du système devient une superposition d'états du qubit et d'états de photons ($|0\rangle$ ou $|1\rangle$ photon) de la cavité. Le couplage entre le qubit A et la cavité est alors coupé, puis le système évolue librement pendant un certain temps t_S qui correspond au temps de mise en mémoire de l'état quantique. Ensuite l'opération s'effectue à l'envers avec le qubit B : la cavité est mise en résonance avec ce dernier pendant un temps t_B puis l'état des deux qubits est mesuré. Les probabilités P_A et P_B que les qubits A et B soient dans l'état $|1\rangle$ sont montrées sur la figure suivante, en fonction des temps t_A et t_B. Comme on peut le constater, ces probabilités correspondent bien aux valeurs théoriques.

Le dispositif expérimental permet bien de transférer des états quantiques du qubit A au qubit B, et même de stocker l'état dans la cavité micro-ondes. Il s'agit, avec l'expérience de Yale décrite précédemment, d'une des premières réalisations du 'bus quantique' tant espéré. Toutefois, la fidélité du bus ne pourra être totalement quantifiée que lorsque l'on sera capable d'opérer sur les qubits une mesure d'état par tomographie quantique, comme on l'explique dans le paragraphe suivant.

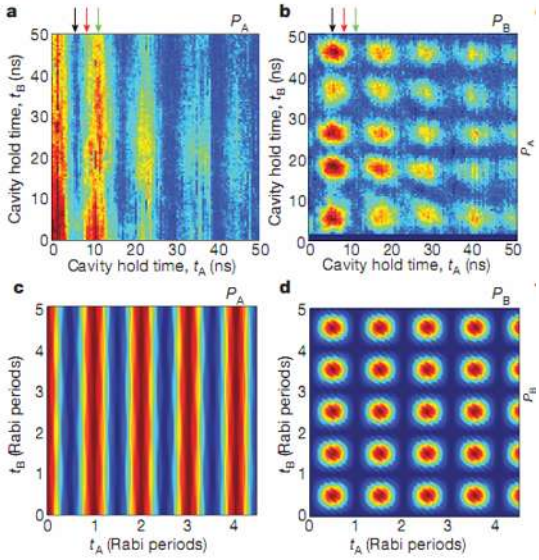


Figure 11 Mesures et simulation de la probabilité de population des qubits A et B en fonction des temps d'interaction avec la cavité t_A et t_B, dans l'expérience de couplage quantique de l'équipe de R. Simmonds au NIST. Crédit : R. Simmonds, NIST dans M. Sillanpää et al. Nature, **449**, 438 (2007)

III.7. Mesure de l'intrication de deux qubits par tomographie

La fidélité de mesure exceptionnelle du qubit de phase a permis à l'équipe de John Martinis de publier en 2006 un article dans le journal *Science*, faisant état d'une mesure d'intrication entre deux qubits à l'aide d'une procédure de tomographie d'état[68].

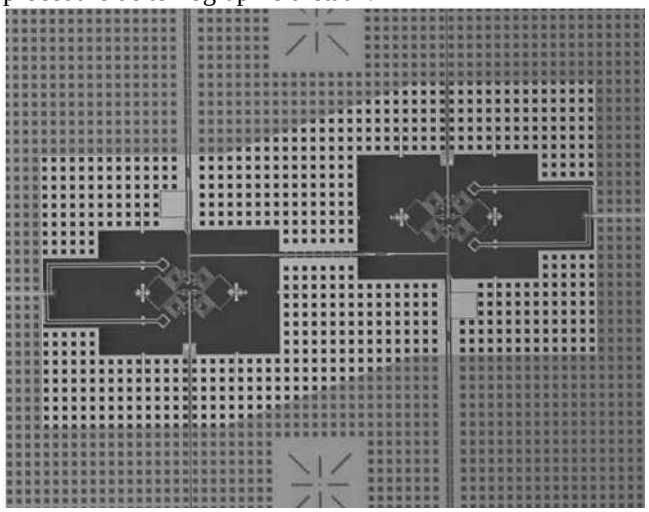


Figure 12 Micrographie électronique du circuit à deux qubits de phase couplés, utilisé par l'équipe de John Martinis à UCSB pour ses mesures d'intrication par tomographie. Crédits : John Martinis dans un supplément à l'article : Matthias Steffen, J. M. Martinis et al., Science, 313, 1423 (2006)

Le circuit utilisé pour cette expérience est similaire à celui de l'expérience de 2005 montré sur la figure précédente. Une micrographie électronique en est montrée sur la figure précédente.

Tout d'abord, lorsque les qubits sont dans l'état $|0\rangle$ et $|1\rangle$, et à la même fréquence de résonance, ils interagissent et l'ensemble oscille entre les états couplés $|01\rangle$ et $i|10\rangle$. Après avoir laissé le système évoluer librement pendant un temps t_{free} variable, les états des deux qubits sont mesurés simultanément, ce qui donne les probabilités d'occupation P_{00}, P_{01}, P_{10}, et P_{11}, qui sont représentées sur la figure suivante en fonction de t_{free} et pour trois états de départ différents : sur le schéma (B) l'état de départ est $|01\rangle$ et l'ensemble oscille entre $|01\rangle$ et $i|10\rangle$. Sur le schéma (C), l'état de départ est $\left(|01\rangle-|10\rangle\right)/\sqrt{2}$ qui est un état propre du Hamiltonien du système (état de Bell) et qui n'évolue pas dans le temps. En (D) l'état de départ est $\left(|01\rangle+i|10\rangle\right)/\sqrt{2}$ qui, lui, n'est pas état propre du Hamiltonien, et comme pour $|01\rangle$, oscille en fonction de t_{free}.

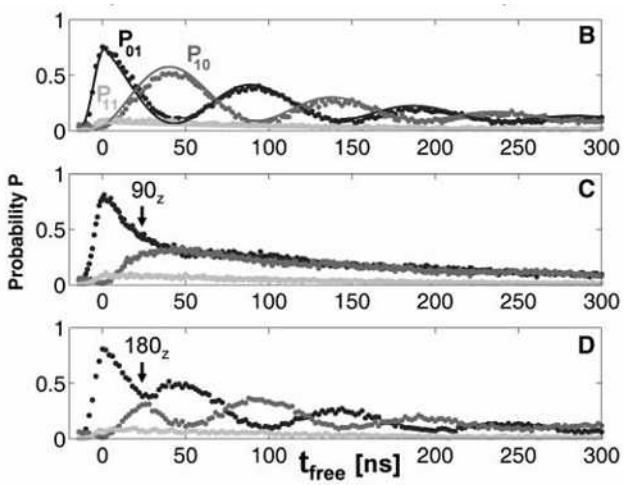


Figure 13 Probabilités d'occupation des états $|01\rangle$, $|10\rangle$ et $|11\rangle$ en fonction du temps d'évolution libre du système préparé initialement dans l'état $|01\rangle$ (figure B), $\left(|01\rangle-|10\rangle\right)/\sqrt{2}$ (figure C) et $\left(|01\rangle+i|10\rangle\right)/\sqrt{2}$ (figure D). Crédits : John Martinis dans Matthias Steffen, J. M. Martinis et al., Science, 313, 1423 (2006)

Cette mesure des probabilités d'occupation des deux qubits en fonction du temps d'évolution démontre clairement l'intrication des deux qubits. Pourtant, l'article va encore plus loin dans la vérification expérimentale, en introduisant une mesure de tomographie. Cette technique, introduite originellement en 1852 dans le contexte de l'optique linéaire[69], consiste dans le cas de deux qubits couplés[70], à mesurer différentes combinaisons linéaires des probabilités d'occupation P_{01}, P_{10}, et P_{11} (au total 27 nombres) afin de reconstruire la matrice densité de l'état du système. Cette matrice, dont la définition générale pour un état pur $|\psi\rangle$ est $\rho=|\psi\rangle\langle\psi|$, donne une description fidèle est complète de l'état quantique. En particulier, dans le cas qui nous intéresse de deux qubits couplés, ses termes diagonaux traduisent l'intrication des qubits.

Dans l'expérience du groupe de John Martinis, la porte quantique $=\sqrt{iSWAP}$ transforme l'état $|10\rangle$ en l'état $|\psi\rangle=\left(|01\rangle-i|10\rangle\right)/\sqrt{2}$, qui est ensuite mesuré par tomographie. Cette porte quantique est importante en logique quantique, car elle est universelle (à condition de lui adjoindre les portes à un qubit[71], voir aussi le passage sur la porte de Fredkin dans l'Annexe XI.6). La matrice densité théorique de l'état à mesurer est :

$$\rho=\begin{pmatrix}0&0&0&0\\0&1/2&-i/2&0\\0&i/2&1/2&0\\0&0&0&0\end{pmatrix}$$

et sa mesure par tomographie est montrée sur la figure ci-dessous.

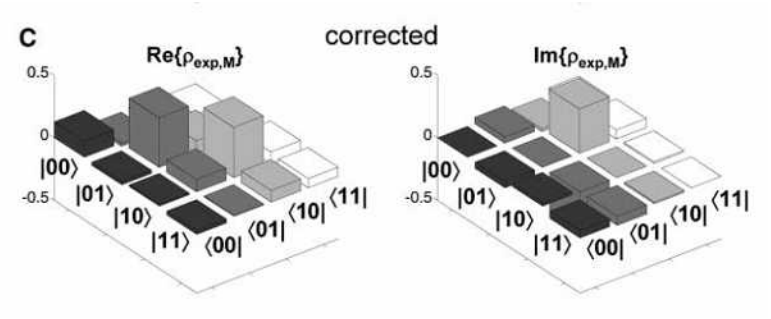


Figure 14 Mesure par tomographie de l'état $|\psi\rangle=\left(|01\rangle-i|10\rangle\right)/\sqrt{2}$. Les parties réelles et imaginaires de la matrice densité sont représentées à gauche et à droite. Crédits : John Martinis dans Matthias Steffen, J. M. Martinis et al., Science, 313, 1423 (2006)

On constate visuellement la fidélité de la mesure, reproduisant qualitativement les coefficients de la matrice densité, notamment les coefficients diagonaux traduisant l'intrication. Une évaluation quantitative donne une fidélité de 87%.

Cette expérience est la première démontrant de façon aussi précise l'intrication de deux qubits quantiques supraconducteurs. Elle constitue ainsi un modèle que beaucoup d'autres équipes essaient de reproduire.

III.8. Le Transmon

L'équipe du professeur Schoelkopf à l'université Yale a introduit très récemment un nouveau concept de qubit très prometteur, appelé transmon[72]. Un transmon est un

qubit de charge d'un point de vue du pilotage et de la lecture, mais pratiquement un qubit de phase de par $E_J / E_C \approx 100$. Les chercheurs ont montré que lorsque ce ratio augmente, la dispersion des charges décroit exponentiellement, ce qui fait que le transmon est beaucoup moins sensible au bruit de charge que le qubit de charge.

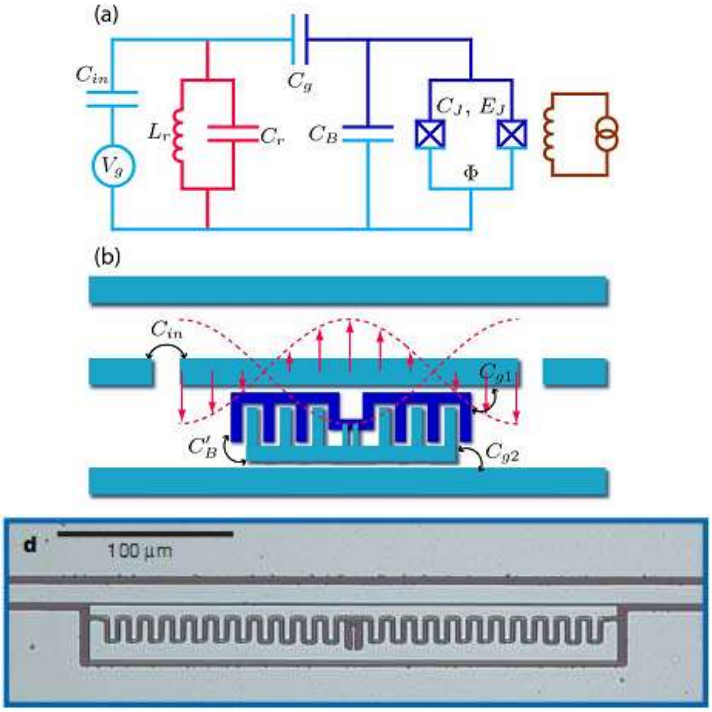


Figure 15 a) et b) Circuit et représentation spatiale schématique du transmon de l'équipe de Yale. Contrairement à un qubit de charge traditionnel, le transmon ne comprend pas un mais deux îlots supraconducteurs, couplés entre eux par deux petites jonctions Josephson et une large capacitance additionnelle C_B. Cette large capacitance explique l'aspect particulier des îlots, en forme de peignes interdigités. Le schéma en b) montre la position du ventre de champ éléctrique de l'onde stationnaire dans le résonateur, situé au niveau des jonctions. c) Image d'un transmon par microscope électronique. Crédit : R. J. Schoelkopf, J. Koch, et al. Phys. Rev. A, 76, 042319 (2007)

Le groupe de Yale est parmi les plus spécialisés dans le couplage de qubits supraconducteurs avec des lignes de transmission micro-ondes, formant des cavités résonantes[73,74]. Dans ces expériences, les modes d'excitations vibratoires des circuits supraconducteurs sont peuplés d'un certain nombre de photons micro-ondes, faisant un lien direct avec le monde de l'optique quantique, et des concepts comme le couplage fort, ou le facteur de Purcell.

En septembre 2007, deux articles spectaculaires étaient publiés simultanément dans le même numéro de la revue Nature. Le premier[75] faisait état d'un dispositif permettant de produire à la demande des photons uniques micro-ondes. Les photons sont produits par émission spontanée d'un qubit transmon, placé dans une cavité résonante micro-onde à la fréquence de 4.68GHz, avec une efficacité d'émission de 38%. Une mesure appelée tomographie, a pu établir une correspondance directe entre l'état du photon émis et l'état du qubit, ce qui un pré requis fondamental pour toute application du dispositif à une manipulation de l'information quantique sur le circuit. L'idée sous jacente à ces recherches est d'aboutir à un 'bus quantique', distribuant l'information entre différents qubits.

Le deuxième article[76] va plus loin dans cette même direction, et entre de plein pied dans les problématiques d'informatique quantique, en apportant un première version du fameux 'bus quantique'. Il démontre en effet un couplage cohérent entre deux qubits, situés à 5mm de distance, de part et d'autre d'une cavité micro-onde résonante. Le circuit, similaire à celui de l'article précédent, comporte deux transmons situés aux ventres du mode électromagnétique résonant à 5.19GHz. Les deux transmons ont des caractéristiques légèrement différentes, ce qui permet d'ajuster leur fréquence de résonance indépendamment à l'aide d'un flux magnétique. Les mesures de l'état des qubits se font par spectroscopie de la transmission de la cavité.

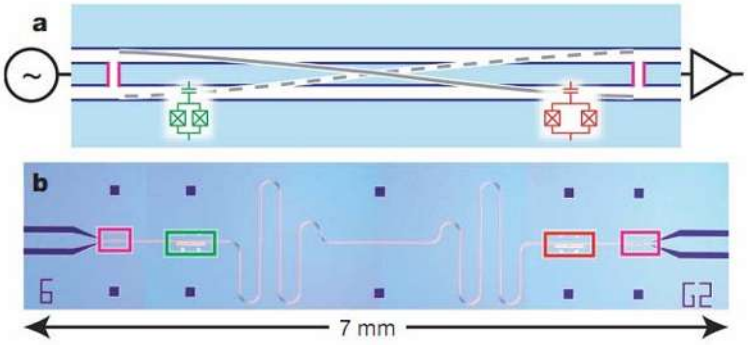


Figure 16 Circuit (a) et image par microscope optique (b) du circuit utilisé par l'équipe de Yale pour coupler deux qubits dans une cavité micro-ondes. Les murs de la cavité sont définis par deux capacitances de couplage (en mauve dans les deux images). Le mode demi-onde (λ/2) est résonant à 5.19GHz,: l'amplitude du champ électrique stationnaire est représentée en gris. Les deux transmons, représentés en vert et rouge, sont situés à deux ventres de champ. Crédits : R. J. Schoelkopf dans J. Majer et al., Nature, 449, 443 (2007)

III.9. Commentaires

A l'issu de l'enquête bibliographique menant à ce dossier, il nous est apparu que les équipes à la pointe des recherches sur les qubits supraconducteurs se situent aux Etats-Unis, en France (CEA), au Japon (NEC), et aux Pays Bas (Université de Delft). Parmi les équipes américaines, celles qui font preuve du plus de dynamisme sont celles des professeurs Schoelkopf et Devoret à Yale, Martinis à UCSB, Clarke à UC Berkeley et Simmonds au NIST.

Les qubits supraconducteurs possèdent des avantages certains, dont une facilité de fabrication grâce à des techniques de lithographie éprouvées issues du monde de la microélectronique, et à l'utilisation de matériaux courants et faciles à manipuler comme l'Aluminium. Les recherches les concernant ont fait des progrès significatifs durant les cinq dernières années. Il y a d'abord eu en 2002 une amélioration notable de l'architecture des qubits de charge, avec l'élimination des principales sources de décohérence, ce qui a permis au groupe Quantronique du CEA d'obtenir des temps de cohérence record, proches de la microseconde. Une certaine prise de conscience des mécanismes essentiels gouvernant le fonctionnement des qubits s'est ensuivie, aboutissant à l'émergence des différentes catégories de qubits : de charge, de flux, de phase, ou intermédiaires charge-flux et charge-phase. A l'aide des qubits de flux, l'équipe de Mooij à Delft est parvenue en 2003 à caractériser temporellement les états de cohérence quantique macroscopique tant recherchés depuis la découverte des SQUIDs. En 2006, l'équipe de J. Martinis à UCSF parvenait à coupler de façon cohérente deux qubits de phase et caractériser le système quantitativement à l'aide de mesures de tomographie. Enfin, en 2007, les équipes de Schoelkopf à Yale et Simmonds au NIST sont parvenues à coupler deux qubits à l'aide d'un bus quantique, tout en maintenant l'intrication des états. Ces avancées récentes marquent un jalon dans les recherches en informatique quantique, et vont certainement relancer l'intérêt que suscitent les qubits supraconducteurs.

Les architectures à qubits supraconducteurs sont très prometteuses pour la réalisation d'un futur ordinateur quantique. Elles présentent l'avantage de la facilité de fabrication sur circuit, ce qui présente toutefois le désavantage d'une plus grande exposition à des interactions décohérentes avec l'environnement que, par exemple, les systèmes à ions piégés. Il s'agira donc dans le futur de continuer à améliorer la cohérence des systèmes supraconducteurs, ainsi que le nombre de qubits couplés. Un autre avantage que présenterait un futur ordinateur quantique à qubits supraconducteurs serait sa facilité d'interfaçage avec l'utilisateur. Les circuits supraconducteurs RSFQ sont très courants et performants pour des applications comme les convertisseurs Analogique-Digital ou Digital-Analogique à très haute fréquence (voir l'entreprise américaine Hypres dans notre rapport de mission sur l'électronique post-CMOS), et feraient une excellente interface entre les parties quantiques et classiques du circuit[77]. L'interface entre le circuit classique RSFQ et l'utilisateur pourrait se faire à l'aide de fibres optiques, lasers semiconducteurs et interupteurs MSM (metal-semiconducteur-metal)[78].

IV. LES BOITES QUANTIQUES SEMICONDUCTRICES

Les matériaux semiconducteurs étant exploités depuis un demi siècle, et s'étant avérés si efficaces et fiables pour réaliser des processeurs de calcul, des mémoires, et des composants optoélectroniques, il est légitime de se demander dans quelle mesure ils pourraient être utilisés pour la réalisation d'un ordinateur quantique. Ces matériaux ont été tellement exploités, notamment par l'industrie de la microélectronique, que les techniques de fabrication mises au point permettent d'en réaliser des miracles de miniaturisation, avec un contrôle et une qualité exceptionnels. Par ailleurs, ils sont si étudiés par la communauté scientifique que leurs propriétés physiques n'ont quasiment plus de secrets pour personne. L'inconvénient, et qu'ils ne permettent pas, contrairement aux matériaux supraconducteurs, d'utiliser une phase macroscopique cohérente : pas de jonction Josephson, de phase supraconductrice faisant office de variable d'état, et in fine, pas de qubit macroscopique. Un qubit semiconducteur devra obligatoirement avoir une taille microscopique (disons nanométrique), et nécessiter des températures ultra-basses (de l'ordre du mK), ce qui évidemment ne facilitera pas son utilisation.

Une des approches les plus prometteuses d'un système de calcul quantique à base de semiconducteurs, proposée initialement en 1998 par Daniel Loss de l'université de Bâle, et David DiVincenzo des laboratoires IBM à Yorktown[79], consiste à piéger des électrons individuels dans des structures appelées 'boîtes quantiques', et à utiliser leur moment magnétique appelé 'spin' comme qubit. Un tel spin individuel possède le gros avantage de n'être couplé essentiellement qu'à un champs magnétique et aux autres spins nucléaires (via l'interaction hyperfine), ce qui lui donne un temps de cohérence atteignant plusieurs millisecondes dans une matrice cristalline sans spin. Cette approche de qubits utilisant des spins en boite quantique, a été adoptée par plusieurs équipes de recherche, dont celles de Lieven Vandersypen à l'université de Delft aux Pays Bas, et celle de Charles Marcus à l'université Harvard, qui sont actuellement les plus en pointe dans ce domaine.

Une boîte quantique semiconductrice est une structure de très petites dimensions (typiquement de quelques nanomètres à quelques microns) pouvant contenir de un à quelques milliers d'électrons. Le point de départ de l'approche utilisée par les équipes de Vandersypen et Marcus consiste à former une telle boîte quantique à l'interface entre deux matériaux ayant des propriétés électroniques différentes, en l'occurrence AlGaAs et GaAs. A cette interface, située typiquement à une centaine de nanomètres de la surface, se forme une fine couche bidimensionnelle (un gaz 2D) d'électrons libres. La qualité des matériaux est souvent suffisante pour que les

électrons puissent se propager dans ce gaz 2D de manière balistique, sur des distances de plusieurs dizaines de microns. La boîte quantique est alors formée en confinant les électrons de cette couche 2D dans les deux directions du plan restantes, touchant ainsi les 3 degrés de liberté du système. Ce confinement latéral est obtenu à l'aide d'électrodes métalliques situées en surface de la structure, qui appliquent une tension négative ayant pour effet de repousser les électrons, et de créer une zone 'déplétée' sous les électrodes (voir figure suivante, haut[80]). En jouant sur la géométrie des électrodes, il est ainsi possible d'aboutir à la formation de boîtes quantiques formées par des électrons piégés au milieu de zones déplétées (voir figure suivante, bas[81]).

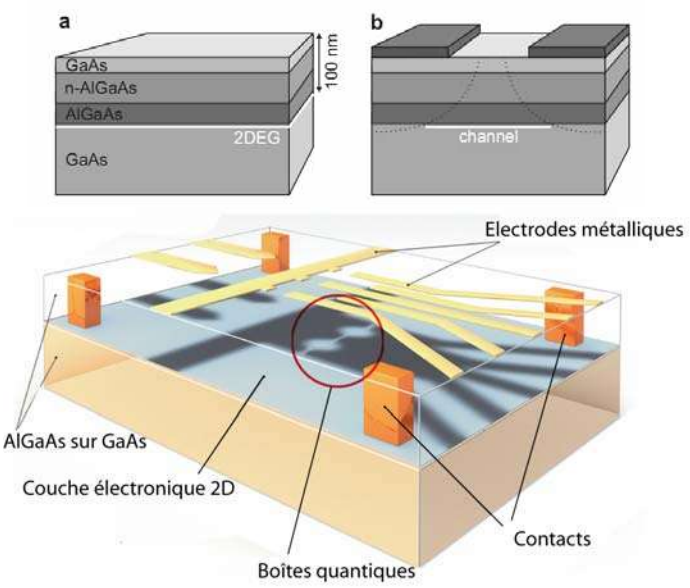


Figure 17 Schéma simplifié de l'hétérostructure utilisée dans les expériences de qubits semiconducteurs du groupe de Vandersypen (Delft). Une couche bidimensionnelle d'électrons libres se forme à l'interface entre l'AlGaAs et le GaAs. L'application d'une tension négative à l'aide d'électrodes en surface crée des zones déplétées (zones ombrées sur la figure du bas) aboutissant à la formation de boîtes quantiques. Crédits : L. Vandersypen, tiré de la thèse de Ronald Hanson (Delft), (image du haut) et de : L. Vandersypen et al. IEEE Spectrum p.42, Septembre 2007 (image du bas).

Toute la difficulté du système consiste à obtenir des boîtes contenant seulement 1 ou 2 électrons, et à pouvoir travailler avec le spin de ces électrons, qui constituera la variable quantique du qubit. Pour qu'un tel système puisse fonctionner un jour comme un ordinateur quantique, il faut qu'il puisse remplir les 5 critères de DiVincenzo (voir paragraphe II.2.1). Nous abordons ces critères dans l'ordre historique où les techniques furent maîtrisées.

IV.1. Initialisation des spins

L'initialisation du système demande d'abord de pouvoir isoler un électron unique par boîte quantique, ce qui fut présenté comme un exploit en 1998[82], mais qui est aujourd'hui considéré comme de la routine[83]. Schématiquement, l'idée est d'appliquer une tension négative aux électrodes situés sur la boîte quantique, jusqu'à ce qu'il n'y reste plus qu'un seul électron. Il s'agit ensuite de pouvoir forcer le spin de cet électron à se mettre dans un des deux états $|0\rangle$ (spin bas) ou $|1\rangle$ (spin haut). C'est cette étape d'initialisation qui détermine la plus forte contrainte sur les températures extrêmement basses du système, qui devra donc être placé dans une enceinte cryogénique complexe, et entouré de bobines supraconductrices, le tout étant évidemment très cher et encombrant. Comme le disait si bien David Di Vincenzo d'IBM, un ordinateur quantique à base de semiconducteurs 'is not going to be a laptop computer'[84].

L'initialisation s'effectue grâce au pompage optique ou, comme c'est le cas pour les expériences du groupe de Delft, à une thermalisation à très basse température (30mK) et à fort champ magnétique (plusieurs Teslas). La thermalisation évite que le spin de l'électron n'oscille dans tous les sens à cause de l'agitation thermique, et le fort champ magnétique lui impose sa direction. Un spin ainsi préparé à une très longue durée de vie, avec un temps de relaxation de l'ordre de la miliseconde[85]. Par ailleurs, en utilisant une technique bien connue « d'écho de spin », on a montré qu'un tel spin possédait un temps de cohérence supérieur à la microseconde (voir les résultats de l'équipe de Harvard plus bas). Les critères 1 et 3 de DiVincenzo sont ainsi satisfaits.

IV.2. Mesure des spins

La mesure du spin d'un électron unique a longtemps été considérée comme difficile à cause de sa si faible interaction avec les champs extérieurs. Des équipes étaient parvenues à contourner cet obstacle à l'aide de techniques optiques ou de microscopes atomiques à force magnétique (MFM), mais pas de technique électronique simple. En 2004, l'équipe de Lieven Vandersypen à l'université de Delft a trouvé une méthode permettant de contourner le problème[86]. Cette méthode mesure le spin indirectement, grâce à une conversion spin-charge, suivie d'une mesure électronique. Plus précisément, les électrodes à proximité de la boîte quantique sont soumises à des impulsions de 5mV pendant 0.5µs. Ces impulsions donnent à l'électron piégé juste assez d'énergie pour s'extraire de la boîte si son spin est bas $|\downarrow\rangle$, mais pas s'il est haut $|\uparrow\rangle$. La raison est qu'en présence d'un champ magnétique $\boldsymbol{B}$, un électron avec un spin bas (antiparallèle au champ) a une plus grande énergie qu'avec un spin haut (parallèle au champ), la différence d'énergie entre les deux états étant donnée par l'énergie Zeeman $\Delta E_Z = g\mu_B B$, qui vaut environ $25\mu eV/T$ dans le GaAs[87]. La présence ou l'absence d'un électron dans la boîte quantique modifie en retour le courant circulant dans un canal nanométrique situé à côté de la boîte. La différence de courant est infime (300pA), mais mesurable à l'aide d'électronique ultrasensible.

Grâce à cette technique ingénieuse, il est ainsi possible de mesurer l'état de spin de l'électron piégé dans la boîte, et ce avec une fidélité de 82%. Il est même possible d'atteindre une fidélité de 99% à l'aide d'électronique encore plus rapide et sensible.

IV.3. Porte quantique d'échange

Pour faire un ordinateur quantique, la manipulation d'un qubit doit pouvoir aboutir à toutes les combinaisons logiques : on doit pouvoir disposer d'une porte quantique universelle. Les théoriciens ont montré (voir le paragraphe II.2.2) que la combinaison de seulement deux portes suffisait à donner une porte universelle : la porte de rotation d'un spin et la porte d'échange (SWAP) de deux spins. La réalisation expérimentale de ces deux portes a été démontrée très récemment par les équipes de Charles Marcus à Harvard et Lieven Vandersypen à l'université de Delft.

La porte *SWAP* de deux qubits a été maîtrisée en 2005 par l'équipe de Charles Marcus[88]. L'expérience utilisait des boîtes quantiques formées à l'interface AlGaAs/GaAs par l'application de tensions négatives dans des électrodes de surface, comme expliqué ci-dessus. Le dispositif est illustré sur la figure suivante, on y retrouve également le principe de mesure électronique 'single-shot' présenté dans le paragraphe précédent. Deux boîtes quantiques sont couplées par un phénomène appelé interaction d'échange[89], qui s'apparente à l'interaction quantique des fonctions d'ondes des électrons dans les deux puits de potentiel correspondant aux deux boîtes. Quand deux électrons sont très proches l'un de l'autre, leurs fonctions d'onde se recouvrent partiellement, et ils peuvent ainsi échanger leur spin. Dans le dispositif, une électrode permet de contrôler le couplage entre les deux boîtes, et la durée de l'échange. Pour une durée bien précise de cette interaction d'échange (360 ps), les deux spins sont précisément échangés (porte *SWAP*). Pour une durée deux fois moindre, les spins sont 'à moitié échangés', c'est-à-dire qu'ils sont dans un état intriqué, ce qui correspond à la porte $\sqrt{SWAP}$.

Dans cette expérience, le temps de déphasage des spins est très faible ($T_2 \approx 10ns$), les spins des électrons dans les boîtes quantiques étant fortement perturbés par les spins des nombreux noyaux atomiques du semiconducteur hôte (un million environ). Une technique bien connue pour augmenter cette durée de cohérence s'appelle l'écho de spin. Elle consiste, après création de la superposition de spins, à attendre une courte durée, puis à appliquer une impulsion de contrôle qui retourne les spins de 180 degrés. On laisse ensuite le système évoluer librement pendant la même durée, et les erreurs accumulées pendant les deux intervalles s'annulent mutuellement. En corrigeant les perturbations des spins de cette manière, la durée de cohérence a pu être étendue à quelques microsecondes, ce qui est alors suffisant pour que l'expérience puisse prétendre au label de porte quantique.

Plus récemment, le groupe de C. Marcus a publié des résultats concernant le développement d'une version beaucoup plus rapide de son dispositif de lecture du qubit[90], la polarisation des spins nucléaires du GaAs par pilotage du qubit de spin[91], et à la transposition de son expérience dans des semi-conducteurs sans spins nucléaires : nanofils de silicium-germanium[92] et nanotubes de carbone.

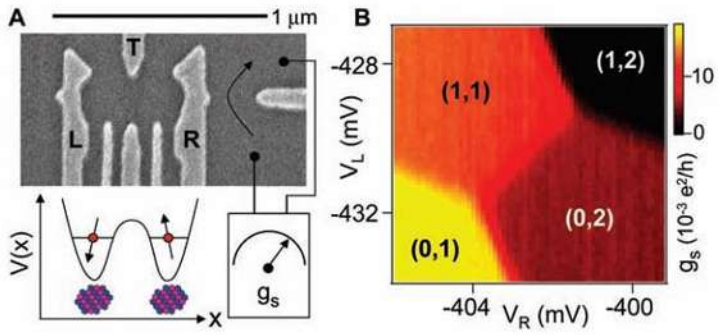


Figure 18 Dispositif utilisé en 2005 par l'équipe de Charles Marcus à Harvard pour générer une porte SWAP entre deux qubits semiconducteurs. (A) Micrographie électronique du dispositif. A l'aide de tensions négatives V_L et V_R, les électrodes L et R contrôlent le nombre d'électrons dans les boîtes quantiques de gauche et de droite. La grille T sert à contrôler le couplage tunnel entre les deux boîtes quantiques. La conductance g_s est sensible principalement au nombre d'électrons dans la boîte de droite. (B) Représentation de g_s en fonction de V_L et V_R, (m,n) indiquant le nombre d'électrons dans la boîte de gauche (m) et droite (n). Crédits : C. Marcus, Harvard, dans J. R. Petta, C et al. Science, 309, 2180 (2005)

IV.4. Porte quantique de rotation

Dans cette recherche de la porte quantique universelle, après la réalisation de la porte SWAP, il restait à réaliser les portes de rotation à un qubit. L'approche la plus classique pour faire tourner un spin est la résonance électronique de spin (ESR)[93], qui fonctionne sur un principe similaire à celui de l'Imagerie par Résonance Magnétique (IRM) utilisée couramment dans les hôpitaux. Elle est basée sur le fait que, placer un spin dans un champ magnétique statique, le fait osciller autours de l'axe du champ, avec une fréquence de précession *f* proportionnelle à l'intensité du champ. Si maintenant, on applique un champ magnétique oscillant, perpendiculaire au champ statique, et oscillant à la même fréquence *f*, le spin subira une rotation selon un axe perpendiculaire à celui du champ statique. Si le spin est initialement aligné avec le champ statique (spin up), il sera ainsi possible de le retourner de 180° (spin down). Toutes les rotations intermédiaires sont également possibles, ce qui permet de réaliser la fameuse porte quantique de rotation à un qubit.

Parvenir à contrôler la rotation d'un spin et à lire son état en utilisant cette technique ESR présente de nombreuses difficultés. La première est qu'il est difficile de générer sur le composant un champ magnétique oscillant avec l'intensité requise (environ 1mT) sans chauffer l'échantillon par effet Joule. La deuxième difficulté concerne la lecture du spin d'un électron unique : le champ magnétique oscillant crée inévitablement des champs électriques parasites qui ont tendance à expulser l'électron de la boîte dans laquelle il est confiné. Pour ces raisons, la résonance magnétique ESR avait déjà été réalisée dans plusieurs expériences, mais jamais dans des boîtes quantiques semiconductrices[94,95], jusqu'à ce qu'en 2006, l'équipe de Lieven Vandersypen à l'université de Delft trouve la bonne configuration du système qui permette de résoudre tous ces problèmes[96].

L'approche du groupe de Vandersypen consiste à utiliser un deuxième électron piégé et bloqué dans une boîte quantique adjacente, et de l'utiliser pour lire l'état de spin du premier électron. Un principe élémentaire de mécanique quantique (principe de Pauli) nous dit que des électrons ayant des spins identiques ne peuvent pas rester ensemble, alors que deux électrons ayant des spins opposés le peuvent. Chaque fois que le spin du premier électron est tourné par ESR, un test est fait pour voir s'il est capable de passer dans la boîte contenant le deuxième électron. Si c'est le cas, c'est que la rotation ESR a été efficace.

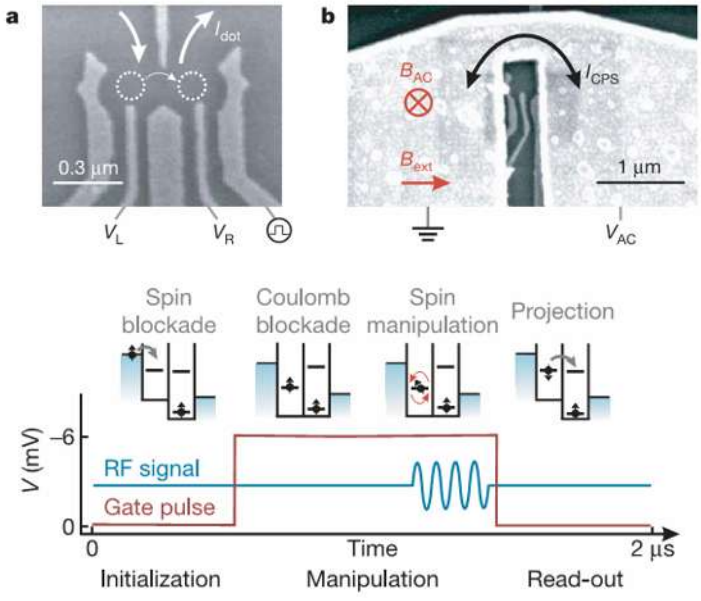


Figure 19 a) Micrographie électronique du composant fabriqué par l'équipe de Lieven Vandersypen pour réaliser la porte quantique de rotation à un qubit. Les électrodes de Ti/Au sont déposées sur une hétérostructure en GaAs/AlGaAs et permettent de former deux boîtes quantiques. Les flèches indiquent le transit des électrons entre les deux boîtes. **b)** Au dessus de la structure montrée en a), et séparée de celle-ci par 100nm de diélectrique, se trouve un circuit électrique CPS (coplanar stripline) permettant de transformer le champ RF en champ magnétique oscillant au niveau des qubits. La direction de ce champ magnétique oscillant B_{AC}, ainsi que celle du champ magnétique statique B_{ext} est indiquée sur la figure. Bas : Schéma montrant le cycle de manipulation et de lecture du spin de l'électron de la boîte de gauche. Crédits : L. Vandersypen dans : F. H. L. Koppens, et al. Nature 442, 766 (2006)

Plus précisément, le composant utilisé est représenté sur la Figure 19. L'électron fixe est situé dans la boîte de droite, avec un spin haut (parallèle au champ magnétique statique B_{ext}). La tension produite sur les différentes électrodes permet d'initialiser le système dans un état $T = |\uparrow\uparrow\rangle$ dit 'triplet', où l'électron de la boîte de gauche possède un spin parallèle à celui de la boîte de droite. Le système est alors bloqué car le principe de Pauli interdit à l'électron de gauche de passer à droite. C'est alors qu'une impulsion RF est appliquée pendant une durée déterminée. A l'aide du circuit CPS montré sur la figure, cette impulsion se transforme en champ magnétique oscillant, dont l'effet est de tourner le premier spin de 180° par effet ESR. Le système se trouve alors dans l'état $S = |\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle$ dit 'singlet', pour lequel il est possible à l'électron de gauche de passer dans la boîte de droite par couplage quantique. La lecture se fait enfin en diminuant la tension de grille de la boîte de droite, qui permet à un des deux électrons de droite de quitter la boîte est d'être détecté par un dispositif de mesure électronique ultra-sensible. S'il n'y a qu'un électron dans la boîte, signe que la rotation ESR n'a pas eu lieu, aucun courant ne sera détecté. L'intensité de courant oscille en fonction de la durée de l'impulsion RF, comme le montre la Figure 20. Il s'agit d'une oscillation Rabi, signe d'un contrôle cohérent de la rotation du spin de l'électron. Comme le suggère la Figure 20, la période d'oscillation varie proportionnellement à l'amplitude de l'impulsion RF (et donc à l'amplitude du champ oscillant B_{AC}), preuve qu'il s'agit bien d'oscillations de Rabi.

Comme on l'a vu, la manipulation du spin à l'aide de champs magnétiques oscillants présente plusieurs difficultés, au premier rang desquelles le chauffage de l'échantillon, les problèmes de lecture et l'encombrement. Très récemment, le groupe de L. Vandersypen a annoncé être parvenu à s'abstraire des champs magnétiques oscillants et à manipuler un spin simplement en appliquant un champ électrique oscillant à l'une des électrodes du dispositif[97]. En plus de la simplicité, ce système permet d'obtenir une bien meilleure sélectivité spatiale, ce qui est important pour adresser localement des spins individuels.

En première analyse, il peut paraître surprenant qu'un champ électrique puisse influer sur un spin magnétique. La théorie de la relativité nous dit cependant qu'aussi bien un électron en mouvement dans un champ électrique, qu'un électron immobile dans un champ électrique variable, ressentent les effets d'un champ magnétique.

Une telle interaction dite 'spin orbite' permet ainsi au spin en question d'être manipulé par le champ électrique oscillant appliqué au dispositif. Ce dispositif a permis de mesurer la transition cohérente entre les états spin-haut et spin-bas, les rotations de 90° s'effectuant en environ 55ns, ce qui est seulement deux fois plus lent qu'avec un pilotage par champs magnétiques oscillants.

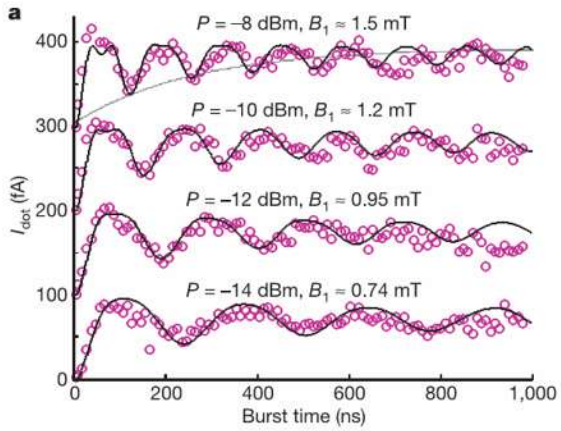


Figure 20 Représentation du courant traversant la boîte quantique de droite du dispositif précédent, en fonction de la durée de l'impulsion RF, et pour plusieurs intensités de l'impulsion RF. Les oscillations de Rabi sont le signe de la rotation cohérente du spin de l'électron. Crédits : L. Vandersypen dans : F. H. L. Koppens, et al. Nature 442, 766 (2006)

IV.5. Commentaires

Depuis la première proposition de DiVincenzo et Loss en 1998, et les premiers dispositifs expérimentaux il y a seulement 5 ans, les recherches sur les qubits semiconducteurs à base de spins électroniques piégés, ont beaucoup progressé. On sait désormais isoler les spins individuels, les initialiser, les manipuler et les lire, le tout avec une bonne précision. Les chercheurs sont également parvenus à coupler à volonté deux spins dans un état de superposition cohérente. Un des premiers défis auquel ils ont été confrontés a été le faible temps de cohérence (environ 10ns) de la superposition ainsi créée. Cette décohérence est due à l'interaction (dite hyperfine) des qubits avec les spins nucléaires des atomes de la matrice cristalline environnante. Une technique un peu artificielle dite d'écho de spin a permis de prolonger ce temps de cohérence au-delà de la microseconde, mais il faudra à l'avenir que les chercheurs se penchent sur cette limitation intrinsèque aux systèmes semiconducteurs. Une possibilité serait d'utiliser des matériaux qui ne possèdent pas de spins nucléaires, comme par exemple le Silicium 28, le Carbone 12, des nanofils de Silicium-Germanium ou des nanotubes de carbone.

La maîtrise de ce problème de décohérence est la première étape dans l'utilisation des qubits semiconducteurs pour la réalisation d'un ordinateur quantique. Les étapes suivantes impliqueront l'intégration de toutes les briques élémentaires dans un système, qu'il faudra étendre de deux qubits à une matrice d'un plus grand nombre de qubits, et qu'il s'agira de manipuler à l'aide d'un ensemble complet de portes quantiques. Dans un premier temps, il faudra cependant trouver un moyen de prouver de façon incontestable l'intrication de deux qubits. Pour cela, la méthode la plus reconnue actuellement est la tomographie d'états dont on a parlé dans le chapitre III.7 sur les qubits supraconducteurs, et qui n'a pas encore été utilisée avec succès sur des qubits semiconducteurs.

V. LES CENTRES NV DANS LE DIAMANT

Nous avons vu dans le chapitre précédent qu'il était possible d'adresser et de contrôler des spins électroniques individuels dans des boîtes quantiques semiconductrices. Les recherches sur ce sujet ont fait des progrès majeurs durant ces dernières années, en révélant l'intrication cohérente de deux spins et l'implémentation de portes quantiques complètes. Un des problèmes toutefois était la faible durée de cohérence des qubits ainsi formés, même s'il était possible d'y remédier de manière artificielle à l'aide de la technique d'écho de spin. Cette décohérence provenait essentiellement de l'interaction hyperfine entre les spins et les moments nucléaires des noyaux environnants. La recherche de matériaux plus adaptés, composés d'atomes ne présentant pas de tels moments nucléaires, a amené les chercheurs à considérer le ^{28}Si, le ^{12}C, des nanofils Si-Ge ou des CNT. Il est apparu récemment que le diamant pourrait être un candidat idéal pour accueillir des spins individuels[98], et en faire des qubits permettant le calcul quantique. Actuellement, plusieurs équipes de recherche américaines travaillent activement sur ce matériau, et ont obtenu des résultats très encourageants. Parmi les équipes les plus en avance, se trouvent celle de David Awschalom à UCSB et Mikhael Lukin à Harvard.

V.1. Introduction aux centres NV

V.1.1. Quelques propriétés du diamant artificiel

Le diamant utilisé dans ces expériences n'est pas celui que l'on trouve en joaillerie. Il est fabriqué artificiellement par une méthode de dépôt en couches minces appelée CVD (Deposition par Vapeur Chimique). Cette méthode utilise des gaz de molécules carbonées (méthane) dont les liaisons covalentes des atomes d'hydrogène sont brisées par des irradiations micro-ondes, ce qui laisse les atomes de carbone libre de se fixer sur la surface du substrat (généralement en Si). Des couches de plusieurs centaines de nanomètres d'épaisseur sont ainsi déposées sur des surfaces de plusieurs cm^2. Ces couches sont formées de diamant extrêmement pur, mais qui se

présente sous forme d'un assemblage de petits cristaux dont les tailles varient du nanomètre au micron selon les conditions de croissance. Pour les expériences qui intéressent l'optique et l'électronique quantique, le système idéal est constitué d'un cristal de diamant unique, suffisamment gros pour posséder une structure cristalline parfaite sur de longues distances.

Une propriété remarquable du diamant est la largeur de sa bande interdite, qui est de 5.5eV, soit environ 5 fois plus large que celle du silicium. Comme dans les semiconducteurs, il est possible d'introduire dans le cristal de diamant des impuretés, dont les niveaux d'énergie discrets se trouvent placés au milieu de la bande interdite. Cependant, étant donné la largeur de cette dernière, certains de ces états peuvent avoir des différences d'énergie comparables avec l'énergie de photons optiques. Il est alors possible de faire fluorescer ces états (en les excitant et désexcitant en continu avec un laser visible bien ajusté) tout en restant dans la bande interdite, et sans jamais passer dans la bande de conduction. Ce procédé de fluorescence en lumière visible d'impuretés isolées dans la bande interdite, a été mis en évidence pour la première fois en 1997 par l'équipe allemande de Wrachtrup à Chemnitz.

V.1.2. Les caractéristiques élémentaires d'un centre NV

Les impuretés que l'équipe de Wrachtrup détectait étaient des « centres NV » (Nitrogen Vacancy). Comme le montre la figure suivante, un centre NV consiste en l'association de deux impuretés dans le cristal de diamant : un atome d'azote N à la place d'un atome de carbone, adjacent à une lacune V, c'est-à-dire à l'absence d'atome (un atome de carbone manquant dans la structure cristalline). Les électrons du centre NV ont des orbites qui couvrent la lacune et l'ensemble des trois atomes de carbone adjacents, mais sans s'approcher de l'atome d'azote. Pour cette raison, le centre NV s'apparente plus à une impureté unique qu'à un ensemble d'impuretés constitué de l'atome N et de la lacune V. C'est cette propriété qui le rend intéressant en calcul quantique, en l'assimilant à un qubit.

Les diamants industriels contiennent des impuretés d'azote, avec des concentrations relativement élevées[99] (10^{19}-10^{20} cm^{-3}). Ces impuretés s'associent naturellement à des lacunes pour donner des centres NV, que l'on trouve en concentration bien moindre (10^{10}-10^{13} cm^{-3}), si bien que certains cristaux de bonne qualité ne possèdent qu'un seul centre NV. La concentration en centres NV peut cependant être augmentée artificiellement par irradiation électronique et recuit.

Les niveaux d'énergie du centre NV, dans son état négativement chargé, sont montrés sur la figure suivante. Ils sont caractérisés par un triplet (3A) de niveaux de basse énergie, dont l'état fondamental $|0\rangle$ est séparé des deux autres niveaux $|\pm1\rangle$ (dégénérés à champ magnétique nul) par une énergie correspondant à 2.88 GHz. Les états excités se présentent également en un triplet (3E) dégénéré à champ magnétique nul. La fluorescence des centres NV intervient entre un des niveaux excités E et un des niveaux de basse énergie A, principalement dans l'état $|0\rangle$. La fréquence de fluorescence est de 1.94eV, soit 639nm, donc de couleur rouge vif. Dans les expériences, les cristaux de diamant sont excités à l'aide de microscopes confocaux qui focalisent la lumière laser sur les défauts à étudier, et qui collectent la lumière de fluorescence émise. Les centres NV apparaissent alors sous forme de points rouge brillants. Comme on l'a dit, il est possible qu'un cristal de diamant ne possède qu'un seul de ces centres.

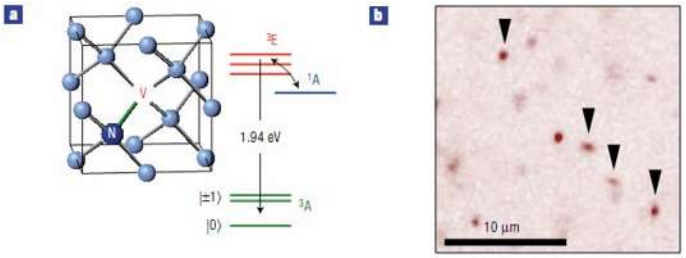


Figure 21 (a) Représentation d'une maille cristalline du diamant comportant un centre NV (un atome d'azote N à la place d'un carbone, situé à proximité d'une lacune V) avec les niveaux d'énergie correspondants. (b) Micrographie optique montrant l'émission de plusieurs centres NV (flèches). Crédits : D. D. Awschalom, UCSB dans : R. J. Epstein et al. Nature physics, **1**, 94-98 (2005)

V.2. Intérêt des centres NV pour le calcul quantique

V.2.1. Source de photons uniques

Les centres NV possèdent plusieurs propriétés très intéressantes en information quantique. La première ne touche pas directement le calcul quantique, mais la discipline cousine qui est la cryptographie quantique. Les centres NV sont en effet capables d'émettre des photons uniques les uns après les autres et à la demande[100,101]. En 2002, l'équipe de Philippe Grangier à l'institut d'optique d'Orsay, démontrait le premier système de cryptographie quantique basé sur une source pulsée à photons uniques[102,103].

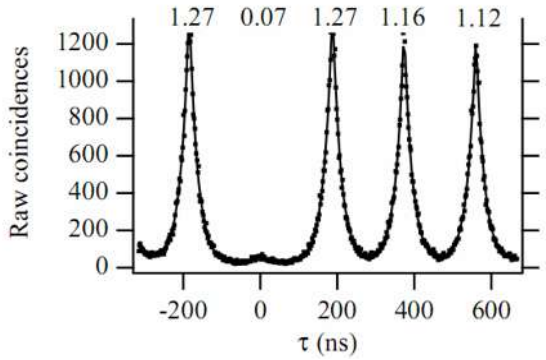


Figure 22 Fonction d'autocorrelation de l'émission de centres NV. La chute à zéro de la fonction pour un délai τ nul indique que le centre NV émet des photons uniques. Crédits : Philippe Grangier, Institut d'optique à Orsay, dans : A. Beveratos, et al. Phys. Rev. Lett. **89** (18), 187901 (2002)

V.2.2. Robustesse vis-à-vis de la décohérence

Une autre propriété, cette fois fondamentale pour le calcul quantique, est que les centres NV possèdent un spin très robuste à la décohérence, qui peut être facilement initialisé et mesuré.

Ce spin NV peut, tout d'abord, être polarisé convenablement à l'aide d'illuminations optiques. Il peut ensuite être mesuré grâce à une propriété remarquable, découverte récemment, qui veut que l'un de ses états ($|0\rangle$ ou $|1\rangle$) fluoresce mieux que l'autre. La méthode de lecture du spin NV repose alors simplement sur une mesure de brillance de la fluorescence.

En outre, les spins NV sont extrêmement stables dans leur environnement cristallin, même à température ambiante. Cette propriété les distingue des spins de tous les autres systèmes à état solide qui requièrent des températures ultra-basses (voir par exemple le chapitre IV sur les qubits à semiconducteurs).

Dans la plupart des matériaux solides, les sources de décohérence d'un spin électronique proviennent du couplage dit 'spin-orbite' (couplant le spin de l'électron avec son mouvement orbital) et surtout du couplage 'hyperfin' (couplant le spin de l'électron avec les spins nucléaires des atomes voisins, voir le chapitre IV). Dans le diamant, le couplage spin-orbite est négligeable, et le couplage hyperfin très faible mais non nul. Ce dernier est limité par le fait que le diamant est composé à 99% d'atomes de carbone ^{12}C dont le spin nucléaire est nul. Le dernier 1% est composé d'atomes de ^{13}C qui possèdent eux un spin ½, constituant ainsi une source de couplage hyperfin et de décohérence des spins NV. Malgré tout, le temps de cohérence de ces spins atteint la valeur intéressante de 50µs à température ambiante[104]. Grâce aux techniques bien maîtrisées d'écho de spin, il est possible de compenser efficacement ce bruit, et d'atteindre des temps de cohérence proches de la milliseconde à température ambiante[98], et même jusqu'à la seconde à des températures cryogéniques[105].

Pour finir, une dernière propriété des centres NV, est la vitesse à laquelle leur spin peut être manipulé. A l'aide de radiations RF amenées sur le centre NV à l'aide de guides d'ondes intégrés, l'état du spin peut être modifié en environ 10ns. Sachant que le temps de cohérence atteint 1ms grâce aux techniques d'écho de spin, il est ainsi possible d'opérer environ 100,000 opérations sur le spin avant qu'il ne décohére. On est bien au-delà des 10,000 opérations données en première estimation par le 3ème critère de DiVincenzo. Les spins de centres NV ont donc des temps de cohérences suffisamment longs pour satisfaire ce critère.

V.2.3. Les premières portes quantiques

Contrairement aux expériences de cryptographie quantique, qui se contentent d'un seul centre NV utilisé comme source de photons uniques, le calcul quantique nécessite de pouvoir coupler plusieurs qubits pour réaliser l'intrication quantique. Dans une première étape, les chercheurs du groupe de David Awschalom à UCSB se sont penchés sur le couplage de deux spins, dont l'un appartient à un centre NV et l'autre à une impureté d'azote (sans lacune)[99,106,107]. Ce dernier est appelée « spin sombre » (dark-spin) car l'impureté ne possède pas les propriétés de fluorescence du centre NV, et reste invisible en photoluminescence. Lorsqu'un centre NV est proche d'une telle impureté d'azote, l'interaction (de nature dipolaire magnétique) entre leurs spins respectifs peut modifier la séparation d'énergie entre les deux niveaux $|0\rangle$ et $|1\rangle$ du spin NV, normalement de 2.88 GHz. Ceci rend possible le basculement conditionné du spin NV par rapport à l'état du spin sombre[98] : l'application d'une impulsion RF à 2.88 GHz faisant basculer le spin NV de l'état $|0\rangle$ à l'état $|1\rangle$ et vice-versa, uniquement si le spin sombre est dans l'état $|1\rangle$. Dans le cas contraire, l'impulsion RF n'a aucun effet sur le spin NV. Un tel basculement conditionné constitue, ni plus ni moins, une porte quantique C_{NOT}.

Par ailleurs, les portes quantiques de rotation à un qubit peuvent être réalisées simplement en appliquant des impulsions RF aux spins. L'adressage de spins individuels s'effectuant à l'aide de canaux de transmission particuliers appelés 'striplines'[98]. Disposant ainsi de la porte C_{NOT} et des rotations à un qubit, il devient possible de réaliser toutes les manipulations quantiques, et de satisfaire au 4ème critère de DiVincenzo.

V.2.4. Réalisation d'un registre quantique

Au lieu des spins sombres, un autre candidat de qubit capable de se coupler utilement aux spins des centres NV, est le spin nucléaire des atomes de ^{13}C. Le couplage dit 'hyperfin' entre ces deux types de spin (qu'on nommera

pour simplifier 'qubit NV' et 'qubit ^{13}C') constitue, comme on l'a vu, la principale source de décohérence des spins de centres NV. L'idée, explorée avec succès par l'équipe de Mikhael Lukin à Harvard, est de mettre à profit ce couplage pour des opérations quantiques contrôlées[108,109]. Il a été possible en particulier de transférer l'état d'un qubit NV sur un qubit ^{13}C et de le relire ensuite avec une grande fidélité, réalisant ainsi une mémoire quantique.

Plus précisément, le couplage d'un qubit NV avec un qubit ^{13}C permet d'implémenter des opérations quantiques conditionnées[109], comme le montre la figure suivante. Lorsque le spin NV est dans l'état $|1\rangle$, l'interaction hyperfine introduit en effet une séparation des états d'énergie $|\uparrow\rangle$ et $|\downarrow\rangle$ du qubit ^{13}C. Il est alors possible de basculer conditionnellement le spin NV par rapport à l'état du spin nucléaire. Sur la figure, ω_L correspond à la fréquence d'oscillation de Larmor des spins nucléaires, qui n'a lieu que si le spin NV est dans l'état $|0\rangle$. Ceci permet de transférer des superpositions quantiques du spin nucléaire sur le spin NV, et entre autres, de pouvoir le lire.

Le spin nucléaire d'un qubit ^{13}C peut ainsi être initialisé avec une fidélité de 85 % à l'aide du qubit NV. Une superposition quelconque des états du qubit NV peut également être copiée sur un qubit ^{13}C, y être stockée, puis relue avec une fidélité de 75%. Le couplage cohérent entre deux ^{13}C a été observé pendant 0.5 ms, et le temps de cohérence d'un qubit ^{13}C (mesuré par une méthode d'écho de spin) dépasse 20 ms. Enfin le qubit ^{13}C décohère en environ 1 µs lorsque le système est irradié par le laser de pompage optique du centre NV[110].

Ainsi, les qubits de spins nucléaires ^{13}C sont bien plus robustes à la décohérence que les qubits NV, et semblent être de bons candidats pour constituer une 'mémoire quantique'. L'équipe de Lukin a même proposé une architecture permettant de construire un répéteur quantique basé sur ce principe. L'existence d'un tel répéteur serait très appréciable en communications quantiques. Il apporterait une solution aux problèmes posés par le transport des qubits sur de longues distances, qui constituent actuellement un frein aux applications de cryptographie quantique.

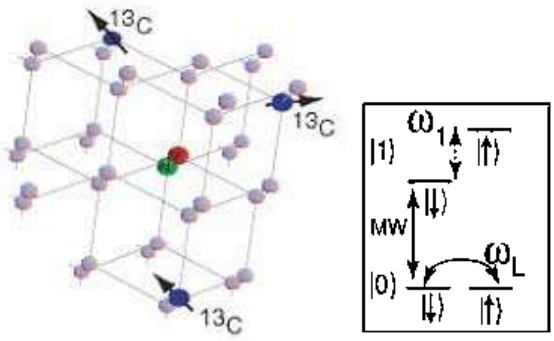


Figure 23 Gauche : Illustration d'un centre NV entouré de plusieurs noyaux ^{13}C avec lesquels il interagit par couplage hyperfin. Droite : Les niveaux $|0\rangle$ et $|1\rangle$ du spin NV sont couplés aux niveaux $|\uparrow\rangle$ et $|\downarrow\rangle$ du spin nucléaire ^{13}C, permettant l'implémentation d'une porte quantique C_{NOT} à deux qubits. Crédits : M. Lukin, Harvard University, dans : M. V. Gurudev Dutt, M. D. Lukin et al., Science, 316, 1312-1316 (2007)

V.2.5. Interactions quantiques à longue distance

Les interactions quantiques qui ont été décrites jusqu'à présent, qu'il s'agisse de couplage avec des spins sombres ou avec des spins nucléaires ^{13}C, sont locales, leur portée ne dépassant pas la maille atomique. Pour que les centres NV puissent interagir à plus longue distance, ils doivent utiliser un vecteur d'interaction différent. Une possibilité serait de faire appel à des photons qui, comme on le sait, ont une portée infinie.

Le diamant artificiel déposé en couches est un matériau qui se prête bien à l'utilisation des photons. En particulier, il est transparent, et peut bénéficier des techniques de microfabrication traditionnelles, permettant de le transformer de manière à ce qu'il ait des propriétés optiques adéquates. On envisage dès lors de créer des composants optiques sur puce, dont les différentes parties seraient connectées par des guides d'ondes gravés directement dans le diamant. L'émission optique des centres NV serait fortement augmentée s'ils étaient situés dans des micro-cavités optiques adéquates. Les progrès de ces dernières années dans la fabrication de telles structures donnent beaucoup d'espoirs[111,112].

L'équipe d'Evelyn Hu à UCSB a récemment montré qu'il était possible de fabriquer des cristaux photoniques dans le diamant épitaxié, de manière à créer une micro-cavité planaire autours d'un centre NV (voir Figure 24). De la même manière, le laboratoire QSR de Hewlett Packard, dirigé par Stanley Williams, est parvenu à coupler des centres NV avec des micro-résonateurs optiques en forme d'anneau (voir Figure 25) dont certains possédaient de forts facteurs de qualité[113].

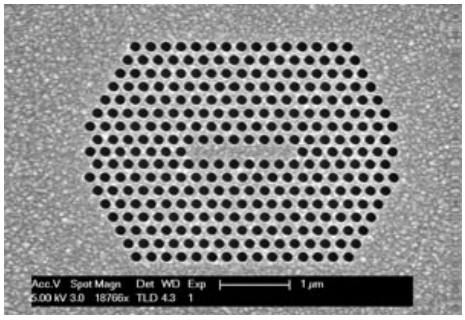


Figure 24 Micrographie électronique d'une structure alvéolaire de cristal photonique créant une micro-cavité planaire dans laquelle se trouve un centre NV. L'idée est d'augmenter le couplage entre le spin du centre NV et les photons du mode résonant dans la cavité. Crédits : Evelyn Hu, UCSB

Figure 25 Couplage de nanocristaux contenant des centres NV (points brillants rouges) avec un microrésonateur optique. Crédits : Stanley Williams, laboratoire QSR, Hewlett Packard.

V.3. Conclusion

L'idée d'utiliser des centres NV dans le diamant pour l'information quantique est très récente, et très prometteuse. Le spin de ces centres forme un qubit qui présente des propriétés particulièrement attractives : il possède de longs temps de cohérence, peut émettre des photons uniques, il est facile à adresser à l'aide d'impulsions RF, et facile à lire grâce à sa forte fluorescence optique sélective. Le couplage local de ce spin avec, soit des spins 'sombres' d'impuretés d'azote, soit des noyaux ^{13}C, permet de réaliser des portes quantiques élémentaires, ainsi que des mémoires quantiques robustes. Enfin, quelques travaux préliminaires montrent qu'il est possible de coupler ce spin efficacement avec des résonateurs optiques, présageant ainsi les transmissions quantiques à plus longue portée.

Un des inconvénients principaux des centres NV réside dans l'absence de contrôle de leur position dans le cristal de diamant. Ils se forment naturellement et avec une distribution spatiale aléatoire. Les travaux présentés ici reposent sur une post-sélection des cristaux qui possèdent les propriétés les plus intéressantes, mais cette démarche présente des limitations évidentes lorsqu'il s'agit de progresser vers de vrais calculateurs quantiques. Des chercheurs à l'université nationale d'Australie, à l'université de Bochum en Allemagne, et au Lawrence Berkeley National Laboratory en Californie, travaillent activement sur ce problème. Ils utilisent des techniques d'implantation ionique permettant d'insérer des ions d'azote aux emplacements voulus. Les cristaux de diamant sont ensuite chauffés à 850°C, permettant aux lacunes de se déplacer, et de finalement rencontrer les impuretés d'azote en formant des centres NV.

L'optique quantique à base de centres NV a donc fait énormément de progrès ces toutes dernières années, et constitue une piste très sérieuse dans la recherche des meilleurs candidats au futur QC. Le fait que de gros industriels comme HP s'y intéressent prouve, s'il en faut, l'intérêt du concept.

VI. LA RÉSONANCE MAGNÉTIQUE NUCLÉAIRE

La résonance magnétique nucléaire (RMN) est une technique spectroscopique étudiant les transitions entre différents niveaux d'énergies (niveaux Zeeman) de noyaux atomiques placés dans un champ magnétique. Initialement, cette technique a été développée par des physiciens, pour tester des modèles de structure nucléaire. Il a fallu peu de temps aux chimistes pour réaliser qu'elle donnait accès à l'environnement chimique des noyaux, les raies spectrales mesurées montrant une dépendance subtile aux propriétés des nuages électroniques entourant les noyaux. Aujourd'hui, la RMN est une technique abondamment utilisée en médecine sous le nom plus commun d'IRM (Imagerie par Résonance Magnétique), en chimie, exploration pétrolière, etc… Elle est unique pour la facilité avec laquelle elle peut être appliquée à des systèmes complexes, et par le degré de sophistication qu'elle a su atteindre. Son succès est dû, en partie, aux longs temps de cohérence des superpositions quantiques, et à l'excellent contrôle expérimental obtenu avec les émissions RF.

VI.1. Motivations

L'idée d'utiliser la RMN pour le calcul quantique fut présentée pour la première fois en 1997 dans deux articles indépendants de trois chercheurs du MIT, Neil Gershenfeld et Isaac Chuang[114] d'une part, et David Cory[115] d'autre part. Ces articles expliquaient, avec quelques différences techniques, la manière d'utiliser un ensemble macroscopique de molécules comme processeur quantique. Au cœur de ce processeur se trouve une molécule individuelle d'une dizaine d'atomes, dont plusieurs possèdent un spin ½. Il s'agit principalement d'atomes d'hydrogène ^{1}H, utilisés couramment dans l'IRM, ou d'atomes de carbone ^{13}C, bien qu'un grand nombre d'autres éléments soient utilisables (^{15}N, ^{14}N ^{19}F,

^{31}P, et plus rarement ^{17}O, ^{29}Si, ^{10}B, ^{11}B, ^{23}Na, ^{35}Cl...). Chacun de ces spins fait office de qubit, que l'on manipule à l'aide des techniques élémentaires de la RMN (voir Chapitre IV) : la molécule est placée dans un intense champ magnétique fixe, et on lui applique des impulsions de durées contrôlées d'un champ magnétique oscillant, dont l'orientation est perpendiculaire au champ fixe.

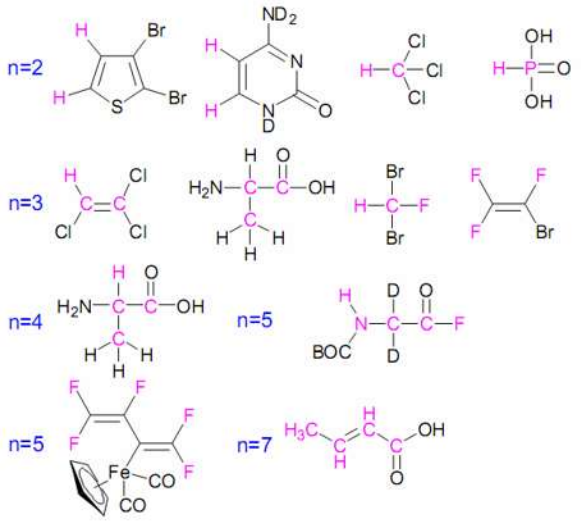


Figure 26 Une sélection de molécules qui ont été utilisées pour le calcul quantique à RMN. Les *n* qubits utilisés pour les calculs sont portés par les atomes illustrés en rose. Dans le cas *n*=7, le groupe méthyl est utilisé comme un seul qubit. Crédits : J. A. Jones, Oxford Centre for Quantum Computation, Oxford, UK dans: '*Quantum computing and Nuclear magnetic resonance*', Phys. Chem. Comm. 11 (2001)

Prenons l'exemple de Gershenfeld et Chuang d'une molécule de (2,3)-dibromothiophene, comportant deux atomes d'hydrogène liés à un même cycle carboné, et ayant chacun un environnement électronique propre dû à différents atomes voisins. Dans un champ magnétique de 4.7T, ces deux atomes ont des fréquences de précession d'environ 200MHz, proches mais pas égales. La différence d'environnement chimique se traduit en effet par une différence de quelques kHz de la fréquence de précession des deux spins. Il est alors possible d'adresser individuellement le spin de chacun des deux atomes en utilisant des impulsions RF ajustées précisément sur l'une des deux fréquences de résonance, permettant de faire tourner un spin sans affecter l'autre.

Le problème est qu'il est extrêmement difficile d'isoler une molécule individuelle, et de lui appliquer efficacement les techniques de RMN. Le signal de résonance est en effet si faible qu'il est pratiquement indétectable. En revanche, avec un ensemble macroscopique de molécules (typiquement, un verre de liquide contenant jusqu'à 10^{20} molécules), les signaux de tous les spins s'additionnent et deviennent détectables. Dans tous les systèmes présentés dans ce dossier, les qubits étaient des objets physiques individuels (le spin d'un électron, un état électronique, un état de phase, un ion…). Dès lors, sachant que l'intrication quantique ne se moyenne pas, n'autorisant pas l'utilisation de la statistique classique, comment extraire un signal quantique utilisable d'un ensemble aussi énorme de molécules quasiment indépendantes ?

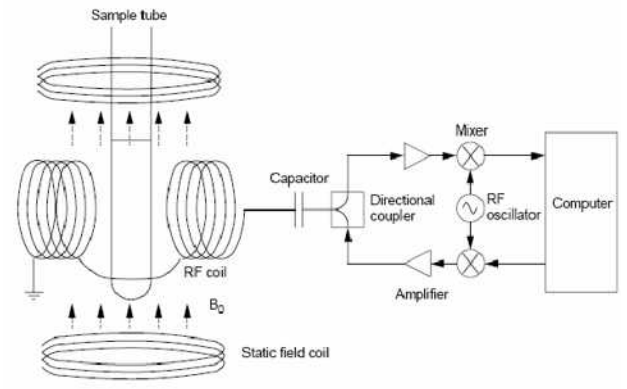


Figure 27 Schéma de principe d'une expérience de calcul quantique à RMN. L'échantillon est placé dans un solénoïde supraconducteur donnant un champ magnétique fixe intense. Des bobines RF sont placés sur le côté pour appliquer des impulsions de champ magnétique oscillant permettant les transformations quantiques. Crédits : S. Schmidt, Duke University, www.ece.duke.edu/~dwyer/courses/ece299.03/presentations/smith_feb21.pdf.

VI.2. Pertinence de la méthode

Pour que la RMN puisse être une technique utilisable dans le cadre du calcul quantique, il faut qu'elle puisse satisfaire à la majorité des critères de DiVincenzo (voir paragraphe II.2.1). Comme nous le faisons dans la plupart des chapitres, reprenons les 5 critères dans leur ordre habituel d'apparition.

VI.2.1. 1er critère : Initialisation des qubits

La première difficulté consiste à initialiser l'ensemble macroscopique des spins à température ambiante dans un 'état pur'. Dans beaucoup de méthodes, ceci est réalisé par un procédé de refroidissement, permettant à tous les qubits de relaxer dans leur état fondamental. Cette approche n'est cependant pas réalisable en RMN, car l'énergie de séparation Zeeman est beaucoup plus petite que l'énergie thermique (kT) à toutes les températures 'raisonnables' (pour lesquelles l'échantillon reste liquide).

Une méthode originale, introduite en 1997 par Gershernfeld et Chuang[114], fait abstraction du refroidissement thermique et renonce également à préparer un état pur. Elle se contente d'un « pseudo état pur », qui permet toutefois de mener à bien les calculs quantique. Sans entrer dans les détails, il s'agit d'obtenir une 'moyenne quantique' en faisant appel à un outil mathématique appelé 'matrice densité' (voir le paragrapheIII.7). A l'équilibre thermique, et sous un fort

champ magnétique statique, les états des différents spins de chaque molécule ont des probabilités d'occupation données par la distribution de Boltzman. Cette dernière dépend de l'énergie des deux états de spin, selon qu'ils pointent dans la direction du champ ou non. La différence entre ces deux états d'énergie (Zeeman splitting) est faible, si bien que leurs probabilités d'occupation sont presque identiques (à un facteur 10^{-6} près), et que la matrice densité ρ de l'ensemble des $\sim 10^{20}$ spins est très proche de la matrice identité *I*. C'est la matrice différence $\Delta = \rho - I$ qui est mise à profit par la méthode et qui est utilisée comme support de l'information quantique. La matrice Δ n'est la matrice densité d'aucun système quantique, et pourtant, comme le montre l'article de Gershernfeld et Chuang, elle se comporte à la manière d'une matrice densité lors des transformations quantiques subies par le système. Elle est une représentation efficace du calculateur quantique.

Plus précisément, la méthode consiste à identifier, dans l'ensemble des 2^N états de spins de la molécule, les états qui ont la même probabilité d'occupation en équilibre thermique. Une série de transformations unitaires permet de grouper ces états dans un ensemble constituant un 'fond thermique' sur lequel les états ayant une population différente peuvent s'exprimer comme des états purs. Ces derniers sont classés à part, dans des blocs séparés de la matrice diagonale Δ, constituant ainsi les pseudo 'états purs' utilisés par les calculs quantiques. L'utilisation de ces états est cependant conditionnée par la lecture de qubits supplémentaires 'ancillae' ayant servi au réarrangement des blocs de la matrice. Pour cette raison, le nombre de qubits utilisables sera inférieur au nombre de spins nucléaires que comportera la molécule en question.

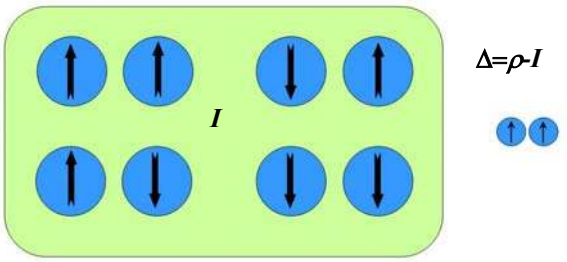


Figure 28 Représentation imagée d'un 'pseudo état pur' à deux qubits. Les quatre états de spin ont quasiment les mêmes probabilités d'occupation, et ne contribuent pas au spectre global. Ils sont rangés dans le fonds thermique représenté par le gros rectangle. Le signal vient d'un faible excès de population pour un des 4 états. C'est ce dernier qui constitue le pseudo état pur.

VI.2.2. 2ème critère : Mesure des qubits

Suivant le principe de fonctionnement général de la RMN, les spins précessent dans le champ magnétique fixe, et leur état peut être mesuré en spectrométrie RF, grâce au nombre macroscopique de molécules dont les signaux s'additionnent. Une subtilité intervient à ce stade.

Il existe en effet deux types de systèmes qui requièrent des techniques de mesure différentes. Dans les systèmes '*hétéronucléaires*', tous les qubits de la molécule sont portés par des atomes différents : par exemple un ^1H et un ^{13}C dans la molécule de chloroforme à deux spins utilisée dans les expériences initiales du groupe de Chuang[116]. Les mesures spectrales sont facilitées car les spins ont des fréquences de résonance bien différentes. L'inconvénient est que la mesure de chaque qubit doit donner lieu à une mesure spectrale propre. En effet, les séparations de Zeeman que l'on cherche à détecter, et qui caractérisent les états des qubits, sont bien plus faibles que les énergies des niveaux en jeu. Comme le montre la Figure 29, mesurer finement les différents niveaux implique que la mesure spectrale soit centrée sur la ligne de résonance de l'atome en question. Caractériser l'état quantique de la molécule revient alors à faire une mesure de tomographie quantique, qui est une procédure très propre mais aussi assez lourde à mettre en œuvre. Ainsi, pour caractériser la molécule de chloroforme à deux qubits, l'équipe de Chuang a dû procéder à un total de 9 mesures. Le nombre de mesures augmentant de façon exponentielle avec le nombre de spin, il est clair que cette technique présente des limitations pratiques.

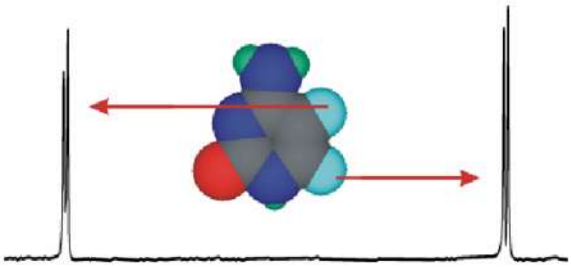


Figure 29 Spectre RMN d'une molécule de cytosine, où deux atomes d'Hydrogène ont été remplacés par des atomes de Deutérium. Les deux groupes de lignes correspondent aux deux atomes, comme indiqué. Le doublet provient du 'couplage J' utilisé pour le calcul quantique. Cette molécule fut utilisée pour la première implémentation d'un algorithme quantique à RMN. Crédits : J. A. Jones, Oxford Centre for Quantum Computation, Oxford, UK dans: '*Quantum computing and Nuclear magnetic resonance*', Phys. Chem. Comm. 11 (2001)

Dans l'autre type de système, dit '*homonucléaire*', tous les atomes portant les qubits sont identiques. Il pourrait s'agir par exemple de la molécule de cytosine utilisant deux noyaux de ^1H. Avec ce type de système, il est possible de lire simultanément l'état de tous les qubits. Sur le spectre RMN centré sur la fréquence de l'atome en question, l'état des différents qubits apparaît à des fréquences de résonance différentes, sous forme de pics positifs pour l'état $|0\rangle$ et de pics négatifs pour l'état $|1\rangle$ (comme on le verra plus loin sur la Figure 32).

VI.2.3. 3ème critère : Durée de cohérence des qubits suffisamment longue

Dans une expérience de RMN, les spins ont de longues durées de cohérence, typiquement de plusieurs secondes pour des échantillons liquides. Avec des matériaux solides, il serait possible d'obtenir des durées de cohérence supérieures, mais ces matériaux ne sont pas utilisables pour le calcul quantique pour plusieurs raisons physiques (élargissement des lignes notamment). L'équipe de Yamamoto à Stanford [117] est ainsi parvenue à atteindre la durée record de 25s dans le cas de cristaux purs de ^{29}Si.

Dans un échantillon liquide, il faut tenir compte du fait que les molécules ont toutes un environnement magnétique différent, influencé par les molécules voisines. Ainsi, les qubits des différentes molécules évoluent tous légèrement différemment, ce qui finit par brouiller très rapidement le signal quantique. Il existe heureusement une méthode standard en RMN qui est très efficace pour résoudre ce problème. Elle porte le nom « d'écho de spin », et consiste à renverser l'évolution libre des spins sans renverser l'effet des portes quantiques, en annulant ainsi les effets de la décohérence. Cette méthode nécessite cependant l'application répétée d'impulsions magnétiques, qui augmente sensiblement la complexité des portes quantiques.

Malgré la relative lenteur d'application des portes quantiques en RMN (quelques ms), un temps de cohérence de quelques secondes suffit à en appliquer plusieurs centaines, ce qui laisse envisager l'implémentation d'algorithmes quantiques relativement élaborés, comme l'algorithme de Shor (voir le paragraphe VI.3).

VI.2.4. 4ème critère : Réaliser toutes les portes quantiques

Une fois que l'ensemble des molécules est préparé dans un pseudo état pur, l'article de Gershernfeld et Chuang montre qu'il est possible de lui appliquer les deux portes quantiques élémentaires qui sont : la rotation à un qubit et la porte C_{NOT}. A l'aide de ces deux portes il est possible d'engendrer toutes les transformations unitaires quantiques, et de satisfaire au 4ème critère.

Si on suppose que le champ magnétique fixe B_0 est orienté selon l'axe Oz, la porte de rotation à un qubit $R_{zA}(\theta)$ (spin noté A) d'un angle θ autour de Oz, est une simple évolution temporelle de durée $t=\theta/\gamma B_0$, γ étant le facteur gyromagnétique du spin. Les rotations $R_{xA}(\theta)$, $R_{yA}(\theta)$ autours de Ox et Oy sont données par l'application d'impulsions de durées déterminées du champ magnétique oscillant B_1, orienté perpendiculairement à B_0 (selon Ox et Oy). Dans le cas d'un système de deux spins en interaction, l'application d'une porte de rotation sur un seul des deux spins peut se faire à l'aide d'une technique appelée 'refocalisation'.

La porte C_{NOT} utilise les non-linéarités de l'interaction des deux spins. Elle peut être implémentée à l'aide d'un changement de phase (rotation des deux spins selon Oz), précédé et suivi par des rotations selon Ox et Oy[114] : $C_{NOT}=R_{yA}(-90)R_{zB}(-90)R_{zA}(-90)R_{zAB}(180)R_{yA}(90)$.

Une autre méthode consiste à tirer parti du 'couplage-J', dit aussi couplage indirect dipôle-dipôle. Il s'agit du couplage entre deux spins nucléaires dû à l'influence des électrons de valence sur le champ magnétique régnant entre les deux noyaux. Comme le montre la figure suivante, le couplage-J entre deux spins nucléaires peut annuler l'influence du champ magnétique RF sur l'un des deux spins : le spin du noyau cible est inversé si et seulement s'il n'y a pas de couplage-J entre les deux noyaux.

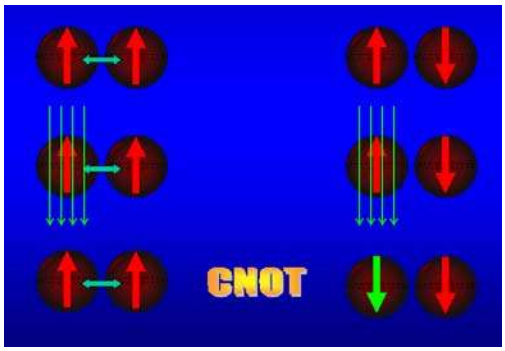


Figure 30 Principe de fonctionnement d'une porte CNOT à deux spins couplés par couplage-J. Crédits : S. Schmidt, Duke University[118].

VI.2.5. 5ème critère : taille du système

L'architecture du système doit être en mesure d'accommoder un grand nombre de qubits. Comme d'habitude, ce critère est toujours le plus difficile à satisfaire, mais ici plus que pour les autres systèmes. Dès son introduction par Gershenfeld et Chuang, la méthode de calcul quantique par RMN a été fortement critiquée pour ses limitations semble-t-il rédhibitoires à fonctionner avec un grand nombre de qubits. Le problème principal vient du fait que le signal mesuré décroît exponentiellement avec le nombre N de spins utilisés, approximativement comme 2^{-N}. En plus de cela, il faut se souvenir que la polarisation du pseudo état pur dérive de la distribution de Boltzman qui, à température ambiante, apporte un facteur 10^{-6} supplémentaire dans l'intensité du signal mesuré.

Dans le tableau extrêmement pessimiste qu'il dresse de la méthode[119], S. Warren de l'université Princeton indique que pour un système idéal de 100 spins, le signal serait 28 ordres de grandeur inférieur à la magnétisation à température ambiante. Pour que le signal ne soit pas ridiculement faible, il faudrait refroidir l'échantillon à des températures $T \ll 1K$, même en présence d'un champ magnétique intense (B_0=14.7T). A ces températures,

l'échantillon ne serait évidemment plus à l'état liquide, les lignes spectrales seraient élargies, et les couplages intermoléculaires compliqueraient énormément les opérations de calcul quantique.

Il est maintenant largement admis que les systèmes de calcul quantique à RMN ne satisfont pas au 5ème critère de DiVincenzo. Le nombre maximal de qubits qu'un tel système sera jamais en mesure d'accueillir devrait certainement ne pas dépasser la dizaine[120,121].

VI.2.6. La question de l'intrication.

Ainsi, les méthodes de calcul quantique à RMN satisfont bien aux 4 premiers critère de DiVincenzo, mais semblent irrémédiablement vouées à ne pas satisfaire le 5ème. Elles ne parviendront donc certainement jamais à construire un véritable ordinateur quantique. Leur intérêt immédiat est cependant d'apporter un moyen pratique de mener à bien quelques algorithmes quantiques simples, et ainsi de faire avancer les recherches en informatique quantique.

Cependant, des doutes ont été émis quant à ce dernier aspect[122]. Selon les critiques, la méthode de calcul quantique à RMN n'aurait même rien de quantique ! Le problème vient du fait que les implémentations à RMN sont basées sur des états mixtes dérivant d'ensembles thermiques (les pseudo états purs). Aux hautes températures auxquelles les expériences sont menées, l'énergie thermique kT est grande comparée à la différence d'énergie Zeeman entre les niveaux des qubits. La matrice densité du système est alors toujours proche de l'état mixte 'maximal'. Il est possible de démontrer qu'un tel état mixte peut être décomposé en produit de plusieurs états, la décomposition n'étant pas unique et pouvant inclure des états intriqués ou non. Il est alors possible de décrire l'état mixte sans faire appel au moindre état intriqué.

La méthode RMN semble ainsi ne pas faire appel à l'intrication qui est pourtant un élément fondamental du calcul quantique. S'agit il donc bien d'un calculateur quantique ? Malgré ces doutes, la situation reste confuse. Certains ont bien tenté de décrire les expériences de calcul quantique à RMN à l'aide uniquement de modèles classiques[123], mais ces tentatives ont échoué. Il a été suggéré par ailleurs que les méthodes à RMN puissent être utilisées pour implémenter la simulation d'autres systèmes quantiques[124]. Même si ces questions théoriques demeurent pour l'instant sans réponse, la RMN a malgré tout fait avancer indéniablement les recherches en informatique quantique, avec des résultats expérimentaux formidables (comme on le verra dans le paragraphe suivant).

VI.3. Perspective historique

La première démonstration expérimentale du calcul quantique à RMN est due à Cory *et al.* du MIT [115]. Leur article de 1997 ne se contente pas d'expliquer les principes de base de la méthode (très similaires à celle de Gershenfeld et Chuang, décrite ci-dessus), mais présente également des expériences simples utilisant deux noyaux de ^{1}H dans une molécule de 2,3-dibromothiophène. Ces expériences démontraient le concept de pseudo état pur et son comportement pendant l'application de portes quantiques simples. Elles n'implémentaient cependant pas de véritable algorithme quantique.

Le premier algorithme quantique à avoir été implémenté sur un système à RMN est celui de Deutsch[125]. Cet algorithme permet de déterminer la parité d'une fonction en une seule évaluation (voir paragraphe II.3.2). Il a été implémenté en 1998 par Jones et Mosca à Oxford, en utilisant les deux noyaux ^{1}H d'une molécule de cytosine dissoute dans de l'eau lourde D_2O (voir Figure 29). Cette démonstration a rapidement été suivie par celle de Chuang *et al.* du MIT [116], utilisant des noyaux de ^{1}H et ^{13}C dans du chloroforme. Toujours en 1998, ces deux groupes parvinrent, en utilisant les mêmes molécules, à implémenter l'algorithme de Grover[126,127].

La période s'étendant entre 1998 et 2001 peut être considérée comme 'l'age d'or' du calcul quantique à RMN[121], tant par la foison des résultats remarquables, que par la vitesse avec laquelle de nouvelles techniques étaient mises au point. Pendant cette période, plusieurs nouveaux algorithmes ont été implémentés : l'algorithme de Deutsch-Jozsa[128,129] (une généralisation de l'algorithme de Deutsch), le comptage quantique[130] (une extension de l'algorithme de recherche quantique de Grover), et un exemple de recherche d'ordre[131] (le calcul quantique certainement le plus complexe effectué jusqu'alors, servant de brique de base à l'algorithme de Shor). Les calculateurs quantiques à RMN ont grandi en taille, avec trois[128], quatre, cinq[129], et sept[132] qubits (voir Figure 26). En addition du calcul quantique, ces systèmes ont été utilisés avec succès dans des expériences de téléportation quantique[133], la correction d'erreurs quantique[134,135], ainsi que les fameux états 'chats de Schrödinger' (voir paragraphe VII.4.5)[132].

En 2001 survenait un événement majeur[136] : la publication par un groupe de chercheurs affiliés à la fois à l'université Stanford et à IBM Almaden, de l'implémentation de l'algorithme de Shor sur une molécule à sept qubits, permettant de factoriser le nombre 15. Le support des qubits était une molécule de fluorine contenant 5 atomes de ^{19}F et deux atomes de ^{13}C (voir Figure 31). L'expérience était effectuée au centre de recherche d'IBM à Almaden (Californie), à l'aide d'un aimant à 11.7T.

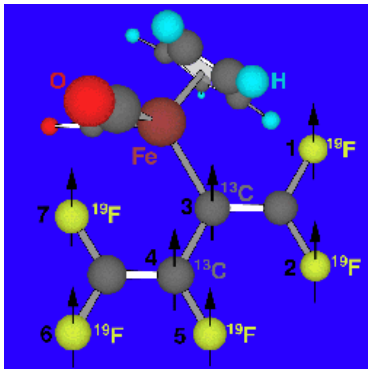


Figure 31 Molécule de fluorine utilisée en RMN par le groupe de Stanford-IBM pour factoriser le nombre 15 à l'aide de l'algorithme de Shor. Cette molécule porte 7 qubits, qui sont les spins des atomes de fluor et de carbone représentés par des flèches. Crédits : IBM Almaden[137]

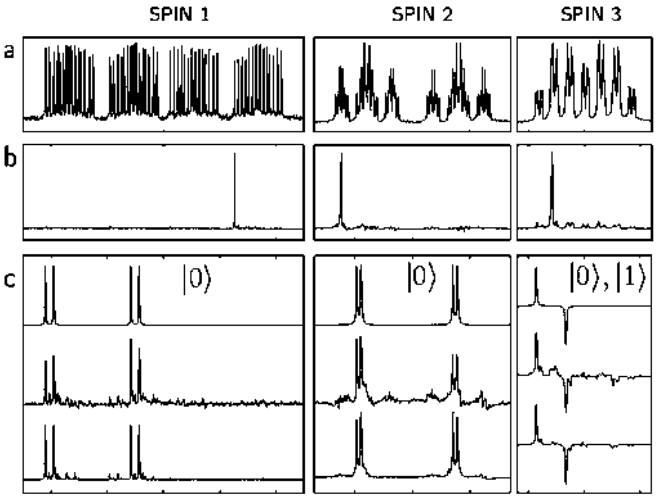


Figure 32 Spectres RMN obtenus dans l'expérience de Stanford-IBM de factorisation du nombre 15. Les spectres du haut (a) correspondent à l'équilibre thermique, après qu'une impulsion RF ait fait basculer les spins $|0\rangle$ (+ $\hat{z}$) et $|1\rangle$ (- $\hat{z}$) dans le plan $\hat{x} - \hat{y}$. L'ensemble de lignes correspond aux différents couplage-J du spin en question avec les autres noyaux. Les états $|0\rangle$ sont donnés par des lignes positives, les états $|1\rangle$ par des lignes négatives. Au centre (b) se trouvent les spectres RMN après préparation de l'échantillon dans un pseudo état pur. En bas (c) se trouve le spectre RMN à la fin de l'algorithme de Shor (ligne du milieu), les lignes du haut et du bas étant des simulations théoriques incluant ou non les effets de la décohérence. Crédits : L. M. K. Vandersypen et al. IBM Almaden and Stanford University, dans L. M. K. Vandersypen, I. L. Chuang et al. , Nature, 414, 883-887 (2001)

A partir de l'état initial de l'ensemble de molécules en équilibre thermique, la préparation du pseudo état pur se faisait en additionnant les effets de 9 expériences d'applications de portes $C_{NOTi,j}$ (C_{NOT} appliquée aux spins i et j) et NOT_i. Chacune de ces expériences étant répétée 4 fois, la préparation exigeait ainsi 36 expériences, qui duraient au total environ 200ms.

Une fois le pseudo état pur préparé, l'algorithme de Shor était implémenté à l'aide d'une séquence d'environ 300 impulsions RF agissant sur les différents spins, et séparées par des intervalles d'évolution libre. La mesure des spins à la fin de la séquence permettait de remonter aux facteurs premiers du nombre 15. La Figure 32 montre quelques uns des spectres RMN obtenus avant et après préparation du pseudo état pur, ainsi qu'à la fin de l'algorithme.

Les "années d'or" du calcul quantique par RMN se terminèrent en 2001 avec ce résultat remarquable, qui fait maintenant parti des anales de la discipline. Depuis, les recherches ont progressé continûment, en se concentrant sur des questions toujours plus subtiles, mais sans qu'aucun résultat d'une envergure équivalente ne soit publié.

VI.4. Conclusion

L'utilisation de la RMN offre une méthode originale de faire des calculs quantiques sur des échantillons macroscopiques comportant un nombre gigantesque de molécules. Les manipulations quantiques se font sur des pseudo états purs qui, contrairement aux autres méthodes exposées dans ce dossier (qubits supra et semi-conducteurs, ions piégés), ne portent pas sur des qubits individuels, mais sur des 'moyennes statistiques' de qubits, qu'il est difficile d'expliciter sans l'appui mathématique de la matrice densité.

Depuis son introduction en 1997, cette méthode a connu rapidement une période d'exaltation qui a duré seulement 3 ans, mais a apporté une importante quantité de résultats remarquables. Cette période s'est terminée sur le chef d'œuvre d'une équipe californienne (Stanford-IBM), qui est parvenu en 2001 à factoriser le nombre 15 à l'aide de l'algorithme de Shor appliqué à une molécule à 7 qubits. Sept ans plus tard, un tel exploit n'a toujours pas été dépassé ni même égalé, bien que les recherches aient continué à progresser en apportant des résultats intéressants.

Les craintes initiales concernant les limitations fondamentales de la méthode semblent malheureusement se vérifier. Ces craintes portaient essentiellement sur la difficulté majeure des systèmes à RMN d'accommoder un grand nombre de qubits. Le signal RMN décroissant exponentiellement avec le nombre de qubits, aller au-delà d'une dizaine de qubits s'avère un défi incroyable. D'autres limitations incluent une inefficacité exponentielle de la préparation des pseudo états purs, le nombre limité d'opérations qui peuvent être appliquées avant décohérence (l'expérience de Standord-IBM opérant à la limite de la décohérence), et les difficultés expérimentales concernant l'implémentation des portes quantiques dans les systèmes multi-spins.

Malgré cette liste déprimante de limitations, la RMN est encore aujourd'hui la seule méthode qui soit parvenue à mener à bien un calcul quantique aussi complexe que l'algorithme de Shor appliqué à 7 qubits. Cependant, il est maintenant largement admis que la RMN aura beaucoup de mal à aller au-delà. Depuis la fin des « années d'or » en 2001, l'intérêt des chercheurs pour la méthode semble être bien retombé.

VII. LES IONS PIEGES

VII.1. Introduction

En 1995, deux physiciens de l'université d'Innsbrück en Autriche, Juan Ignacio Cirac et Peter Zoller, prédisaient qu'une chaîne d'ions maintenue dans le vide par un champ électromagnétique et refroidis à quelques millièmes de degrés Kelvin, pouvait se comporter comme un assemblage de qubits stables[138]. Dans un tel système, les états des qubits correspondent à différents niveaux d'énergie des ions que des faisceaux laser permettent de coupler entre eux, ainsi qu'avec des états de vibration collectifs. L'article de Cirac et Zoller décrivait également la manière théorique de réaliser une porte quantique C_{NOT} avec un tel système. Quelques mois plus tard, l'équipe de David Wineland au NIST (Boulder) en publiait la démonstration expérimentale[139]. A partir de ce moment, les recherches se sont accélérées sur la manière d'utiliser des ions piégés pour réaliser des opérations de calcul quantique, et des résultats remarquables ont vu le jour.

Pendant une période, les systèmes à ions piégés pouvaient être perçus comme trop complexes et délicats, des curiosités de laboratoire en quelque sorte. Les systèmes de qubits 'solides' sur circuits, qu'ils soient semiconducteurs ou supraconducteurs, semblaient être des candidats plus naturels pour former un calculateur quantique, de part leur architecture plus similaire à celle des circuits électroniques classiques. Depuis, la perception a bien évolué, et les systèmes à ions piégés font aujourd'hui parti des candidats les plus prometteurs à l'émergence d'un futur prototype de QC. Actuellement, les équipes les plus en pointe sur ce sujet sont principalement celles de Wineland au NIST (CO), et celle de Rainer Blatt à Innsbrück (Autriche), ainsi que d'autres équipes aux Etats-Unis au LANL à Los Alamos (NM), à l'université du Michigan, au MIT, et ailleurs dans le monde à Barcelone, Garching, Londres, Ontario, Oxford, Ulm.

VII.2. Le piège de Paul

L'essor de cette nouvelle discipline concernant les qubits à ions piégés, tient essentiellement à la maîtrise de techniques expérimentales complexes, développées par le passé pour d'autres raisons. Parmi les pères fondateurs de ces techniques, on peut citer Theodor Hänsch et John Hall (Nobel 2005) pour leurs travaux de métrologie de grande précision utilisant des horloges atomiques, Claude Cohen-Tannoudji des laboratoires Kassler Brossel à Paris, Steven Chu (LBNL, Berkeley) et William Philips (NIST, Boulder), tous les trois prix Nobel de physique en 1997 pour leurs travaux sur le refroidissement d'atomes par laser, et enfin Wolfgang Paul (Nobel 1989) pour la technique de piégeage des ions qui porte son nom (piège de Paul) qui fut développée dans les années 60.

Le piège de Paul apporte une solution pratique à un problème de physique élémentaire : il est impossible de confiner de manière stable une particule chargée en utilisant uniquement des champs électriques statiques. Le principe du piège est d'utiliser des champs électriques oscillants à des fréquences RF, permettant de stabiliser en moyenne les ions piégés. Le piège de Paul présente deux géométries principales, une tridimensionnelle utilisant des électrodes hyperboliques, et une linéaire qui est celle qui nous intéresse dans le cas présent, et qui est représentée schématiquement sur la figure suivante.

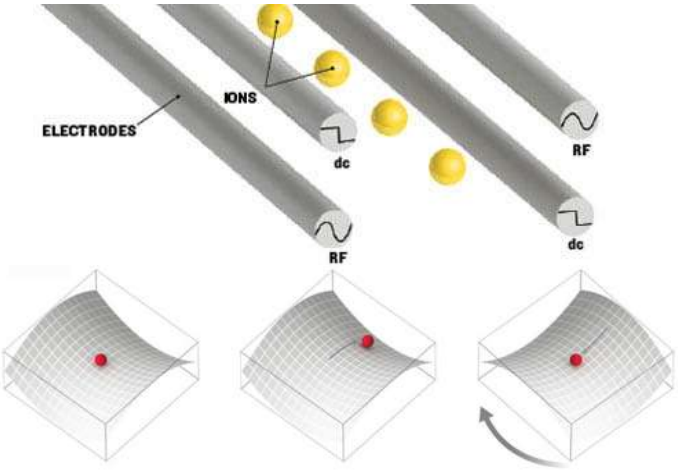


Figure 33 Principe de fonctionnement d'un piège de Paul linéaire. Les ions sont confinés sur une ligne par des champs électromagnétiques générés par quatre électrodes, dont deux produisent un champ électrique continu, et deux produisent un champ alternatif RF. Le potentiel crée a la forme d'une selle de cheval tournant à la fréquence RF, au centre de laquelle les ions sont piégés. Crédits : C. Monroe, NIST Boulder, dans IEEE Spectrum, 37-43, August 2007

Dans une enceinte à vide, quatre longues électrodes sont disposées de manière à former les coins d'une boite rectangulaire. Un champ électrique statique (dc) est appliqué sur deux des électrodes opposées diagonalement, et un champ électrique oscillant à une fréquence RF sur les deux autres. La combinaison de ces champs force les ions à rester confinés le long de la ligne centrale équidistante des 4 électrodes. La raison est la suivante. Si on ne considère que l'action des électrodes RF, les forces électriques agissant sur un ion dérivent à chaque instant d'un potentiel qui a la forme d'une selle de cheval. Cette selle confine dans une direction seulement, celle qui

correspond à une montée de potentiel. L'autre direction est anti-confinante car elle correspond à une chute de potentiel (une particule aurait tendance à tomber). L'astuce du piège provient de l'oscillation du champ RF, qui provoque une rotation permanente du potentiel. Pendant un demi cycle, un ion légèrement décalé par rapport à la ligne centrale se trouve sur la pente montante de la selle, et est poussé vers le centre. En revanche, pendant le deuxième demi-cycle, ce même ion se trouve sur la pente descendante de la selle, et subit une force l'éloignant du centre. Le signal RF est conçu de telle sorte à ce que l'intensité de la première force (vers le centre) soit plus importante que celle de la deuxième, si bien qu'en moyenne, l'ion subit une force de confinement vers la ligne centrale. En réalité, ce confinement se limite au plan médian, équidistant des électrodes RF. C'est là qu'interviennent les deux électrodes dc, qui apportent un confinement supplémentaire dans ce plan médian, ramenant les ions le long de la ligne centrale en les poussant des deux côtés.

Le résultat du piège de Paul est d'aligner les ions le long de la ligne centrale équidistante des quatre électrodes. Comme les ions ont la même charge, ils se repoussent naturellement, phénomène qui peut être utilisé à des fins de codage quantique. En effet, dans ce système, lorsqu'un ion n'est pas figé à l'intersection de plusieurs lasers, il est libre de se déplace le long de la ligne centrale. Interagissant avec les autres ions, comme dans une chaîne de billes reliées par des ressorts, il peut donner à l'ensemble des ions un mouvement de vibration collectif, appelé 'état de vibration'. Cet état est alors susceptible d'agir comme un bus quantique, transférant les uns aux autres, les états quantiques des différents ions.

VII.3. Principe du calcul quantique utilisant des ions piégés

Le piège de Paul et les techniques de refroidissement d'atomes par laser[140,141] constituent les premiers outils permettant d'envisager l'utilisation des ions piégés pour des opérations élémentaires de calcul quantique. Dans sa configuration de base[142], le système consiste en un piège de Paul linéaire à vide poussé (10^{-8} Pa) dans lequel sont confinés plusieurs ions. Chaque ion comporte deux niveaux à longue durée de vie, faisant office d'états orthogonaux du qubit $|0\rangle$ et $|1\rangle$. Il s'agit principalement :

- de deux niveaux hyperfins[iii] de l'état fondamental. Ces états sont extrêmement stables, leur durée de vie étant de l'ordre de mille millions d'années. L'état $|0\rangle$ correspond à un ion où l'électron de valence et le noyau ont des spins opposés, dans l'état $|1\rangle$ les spins sont alignés.

- du niveau fondamental (état $|0\rangle$) et d'un niveau excité de l'ion (état $|1\rangle$), on parle alors de 'qubit optique'.

Dans ce chapitre, nous nous consacrerons principalement aux qubits à niveaux hyperfins, qui sont ceux utilisés par le groupe de David Wineland au NIST.

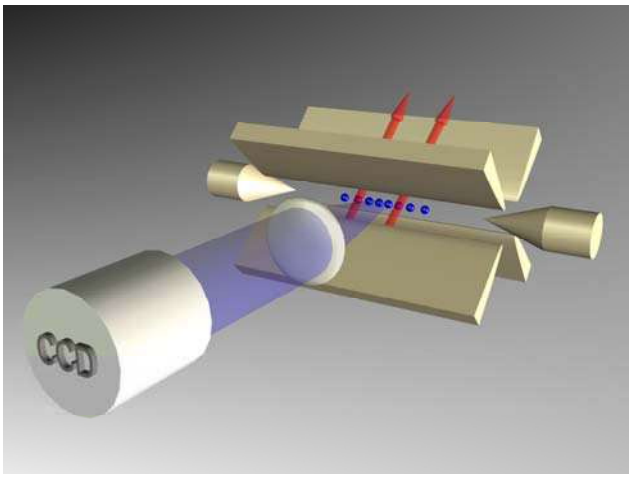


Figure 34 Représentation schématique du dispositif de piégeage d'ions utilisé dans les manipulations de calcul quantique. Crédits : Rainer Blatt, Université d'Innsbrück, http://heart-c704.uibk.ac.at/

Ces ions sont refroidis et manipulés par des lasers accordés sur les fréquences de transition entre les deux niveaux internes (transitions Raman). Typiquement, un même faisceau laser est divisé en plusieurs faisceaux parallèles, qui illuminent chacun un ion différent. Ces faisceaux permettent de manipuler les ions individuellement, et donc de leur appliquer des portes quantiques à un qubit, mais pas plus. Pour obtenir des portes quantiques à deux qubits, il est nécessaire d'avoir une intrication entre plusieurs qubits. C'est là qu'intervient l'idée fondamentale de Cirac et Zoller, d'utiliser le mouvement d'ensemble de la chaîne d'ions.

Comme on le sait, les photons de lumière transportent de l'énergie mais aussi une quantité de mouvement, si bien qu'un faisceau laser interagit avec un ion en lui transférant une certaine impulsion. En outre, les ions se repoussent mutuellement car ils ont la même charge électrique. Par cette interaction, l'impulsion d'un ion est transmise à ses voisins, et de proche en proche, à toute la chaîne. Cette dernière se déplace alors 'en masse', selon certains modes de vibration qui sont quantifiés à cause du confinement du potentiel apporté par le piège de Paul. Ces modes de vibration, ou phonons, correspondent à des états quantiques qui peuvent alors être mis à profit pour réaliser des opérations de calcul quantique.

Pour illustrer cette idée, prenons l'exemple de la réalisation d'une porte quantique C_{NOT} à l'aide de deux ions[143,144]. Un faisceau laser dont la fréquence est bien

[iii] *Provenant de l'interaction du spin du noyau avec le moment magnétique de l'électron*

ajustée peut appliquer une force aux ions, qui dépende de leur état interne. Le faisceau peut ainsi pousser l'ion vers la droite uniquement s'il est dans l'état $|1\rangle$, et n'avoir aucun effet s'il est dans l'état $|0\rangle$. La figure suivante représente schématiquement ce qui se passe dans quatre configurations.

- Si les deux ions sont dans l'état $|0\rangle$, le laser n'a aucun effet sur eux.
- Si les deux ions sont dans l'état $|1\rangle$, ils se déplacent tous les deux vers la droite, mais la distance les séparant n'est pas modifiée. L'état de vibration de l'ensemble des deux ions ne gagne pas d'énergie.
- Si l'ion de gauche est dans l'état $|0\rangle$ et l'ion de droite dans l'état $|1\rangle$, seul l'ion de droite est déplacé, ce qui a pour effet d'éloigner les deux ions. L'état de vibration gagne en énergie.
- Si l'ion de gauche est dans l'état $|1\rangle$ et l'ion de droite dans l'état $|0\rangle$, seul l'ion de gauche est déplacé, ce qui a pour effet de rapprocher les deux ions, et l'état de vibration gagne en énergie. Ce gain est légèrement supérieur que dans le cas précédent, car le couplage électrostatique dû à la configuration du piège n'est pas symétrique : il est plus facile d'éloigner les ions que de les rapprocher.

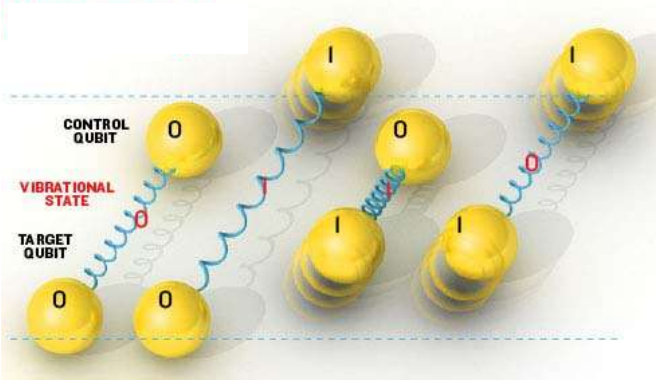


Figure 35 Représentation schématique montrant comment le couplage électrostatique entre deux ions (illustré par des ressorts) peut être mis à profit pour réaliser une porte quantique C_{NOT}. Crédits : C. Monroe, NIST Boulder, dans IEEE Spectrum, 37-43, August 2007

Le résultat de cette opération est d'appliquer une porte C_{NOT} aux deux qubits constitués par l'ion et le mode de vibration : l'état interne de l'ion est inversé uniquement si les ions vibrent. Ceci correspond bien à la table de vérité de la porte C_{NOT} :

$|00\rangle \rightarrow |00\rangle, |01\rangle \rightarrow |01\rangle, |10\rangle \rightarrow |11\rangle, |11\rangle \rightarrow |10\rangle$,

le premier qubit étant le mode de vibration et le deuxième l'état interne de l'ion.

Il ne s'agit ici que d'un exemple de manipulation à deux qubits utilisant les modes quantiques de vibration. La première démonstration expérimentale de la porte C_{NOT} par le groupe de Wineland utilisait un seul ion $^{9}Be^{+}$ dont les deux états hyperfins de l'état fondamental constituaient le qubit cible, et dont les deux premiers états d'oscillation de l'ion dans le piège constituaient le qubit de contrôle. Un autre exemple de porte quantique *controlled-Z* est présenté dans l'article de revue de Steane[1], utilisant deux ions et le mode de vibration entre eux. Cet exemple est similaire à celui qui est présenté ci-dessus, sauf que le résultat est ici un changement de signe de la fonction d'onde et non pas un basculement du qubit cible.

VII.4. Les ions piégés sont-ils de bons candidats pour fabriquer un QC ?

Nous venons de voir que les ions piégés permettent de manipuler des qubits, et de réaliser les portes quantiques élémentaires. L'Annexe XI.4 nous montre, en outre, l'efficacité avec laquelle les groupes de Wineland au NIST et Blatt à l'université d'Innsbrück, ont réalisé les premières expériences de téléportation quantique à l'aide d'ions piégés. Dans le cadre qui nous intéresse, il s'agit maintenant de savoir si ces mêmes ions piégés répondent à la majorité des critères de DiVincenzo qui constituent la définition d'un ordinateur quantique. Les 5 critères sont traités ci-dessous dans le même ordre d'apparition que dans le paragraphe II.2.1.

VII.4.1. Pouvoir initialiser tous les qubits dans un état bien défini (|0000…>) au début du calcul.

Ce premier critère est facile à satisfaire à l'aide d'un faisceau laser, dont la fréquence est précisément ajustée sur l'énergie de transition entre le niveau fondamental hyperfin de l'ion correspondant à l'état $|1\rangle$, et un niveau excité. Lorsque l'ion est dans l'état $|0\rangle$, il n'interagit pas avec le laser et reste dans cet état. En revanche, s'il est initialement dans l'état $|1\rangle$, l'interaction avec le laser l'amène dans l'état excité. Il se désexcite ensuite spontanément dans l'état fondamental, indifféremment dans l'un des deux niveaux hyperfins $|0\rangle$ ou $|1\rangle$. S'il retombe dans l'état $|0\rangle$, le laser n'a alors plus d'influence sur lui, et l'état est initialisé à $|0\rangle$, comme voulu. Si l'ion se désexcite dans l'état $|1\rangle$, il interagit de nouveau avec le laser et le processus d'excitation-désexcitation recommence. Ce processus se répète jusqu'à ce que l'ion finisse par retomber dans l'état $|0\rangle$, ce qui se produit généralement assez rapidement, en moyenne en moins d'une microseconde. L'ion reste alors dans l'état $|0\rangle$, il est initialisé.

VII.4.2. Etre capable de mesurer les qubits à la fin du calcul.

L'état des qubits peut être mesuré efficacement à l'aide du faisceau laser précédent, résonant entre l'état $|1\rangle$ et un niveau excité. Si l'ion est dans l'état $|0\rangle$, il n'interagit pas avec le laser, et rien ne se passe. Si par contre, il est dans l'état $|1\rangle$, il sera excité, et en se désexcitant, émettra un photon de fluorescence. Avec les techniques modernes, la mesure des photons de fluorescence est très efficace. Il est ainsi possible de connaître l'état du qubit avec une précision dépassant 99%, ce qui est remarquable, et constitue un des points forts des qubits à ions piégés.

VII.4.3. Les qubits doivent avoir un temps de décohérence suffisamment long : beaucoup plus long que la durée d'opération d'une porte quantique.

Les niveaux hyperfins des ions utilisés ont de très longues durées de vie, et constituent donc par nature, des qubits robustes vis-à-vis de la décohérence. La principale difficulté expérimentale est de refroidir suffisamment ces ions (à des températures sub-μK), pour qu'ils se maintiennent dans ces états fondamentaux. La source de décohérence du système vient essentiellement du chauffage engendré par le mouvement de vibration des ions, lié aux imperfections de confinement provenant du bruit de tension dans les électrodes. Les premières expériences du groupe de Wineland en 1995 donnaient un taux de décohérence de quelques kHz, compatibles avec des portes quantiques fonctionnant à environ 20kHz. En 2001, ce même groupe mettait au point une méthode de codage d'un qubit à deux ions, permettant de stocker son état dans un sous-espace insensible à la décohérence, et de multiplier par 10 son temps de stockage[145].

En 2004, le groupe de Wineland démontrait le fonctionnement du premier code de correction d'erreur quantique (QEC) utilisant des ions piégés[146]. Cette démonstration faisait appel à 3 qubits donnés par les niveaux hyperfins d'ions $^{9}Be^{+}$. Un seul de ces qubits, dit 'primaire', contenait l'information quantique à préserver, les deux autres qubits, dits 'ancillae', servaient à la correction d'erreurs (voir chapitre II.4). La procédure de correction est la suivante (voir figure ci-dessous): le qubit primaire est codé puis intriqué avec les deux ancillae. Des erreurs sont ensuite appliquées sur l'état intriqué à 3 qubits, sous forme d'une impulsion laser qui induit une inversion de spin aléatoire des qubits. L'état subit ensuite un décodage correspondant à l'opération inverse du codage. L'effet du décodage est de mettre les ancillae dans un état tel, que leur mesure donne directement les erreurs survenues sur les 3 qubits (i.e. ceux dont les spins ont été inversés). Après décodage, les ions sont séparés spatialement et l'état des ancillae est mesuré. Suivant le résultat de la mesure, une opération de correction est appliquée au qubit primaire (*X*, *Y* ou *I*) le remettant dans son état original avant erreur.

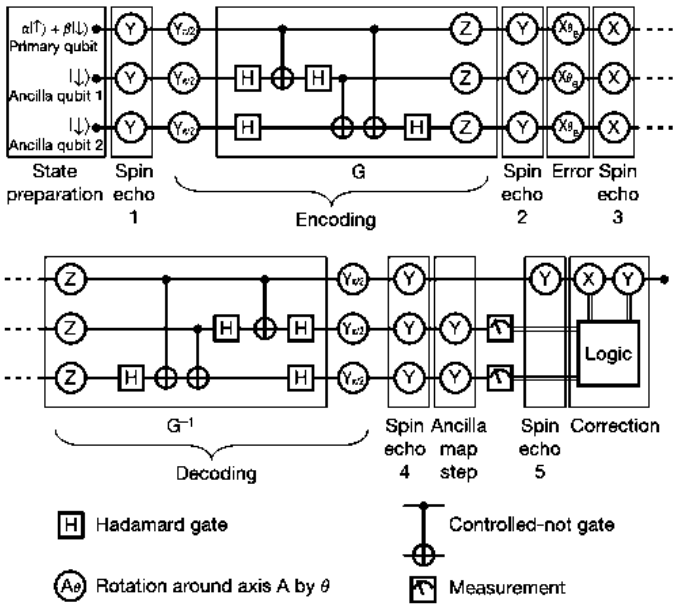


Figure 36 Circuit quantique à ions piégés utilisé en 2004 par le groupe de D. Wineland pour réaliser le premier dispositif à correction d'erreurs quantiques. Trois ions sont utilisés: un qubit primaire et deux ancillae. Crédits : David Wineland, NIST, Boulder, dans : D. J. Wineland et al. Nature **432**, 602-605 (2004)

Les résultats obtenus montraient la possibilité expérimentale de réaliser des QEC à l'aide d'ions piégés. Ils soulignaient toutefois la difficulté de la procédure. L'inconvénient majeur associé à la QEC est le grand nombre d'ancillae nécessaire à sa fiabilité. Pour qu'un QC à base d'ions piégés puisse fonctionner correctement, on estime que, pour chaque qubit de calcul, il faudrait environ une cinquantaine d'ions supplémentaires pour corriger les erreurs qui l'affectent.

En 2006, le groupe de David Wineland, apportait une arme supplémentaire dans la lutte contre la décohérence, en démontrant l'efficacité d'un protocole de purification d'intrication à deux qubits[147]. Ce protocole utilise deux paires intriquées, dont chaque ion est transmis à deux endroits différents. Sur les deux ions reçus à chaque endroit, des portes quantiques sont appliquées, et une communication classique permet de séparer les paires intriquées selon leur degré de fiabilité. Le succès du protocole est de 35%.

VII.4.4. Disposer de suffisamment de portes quantiques pour pouvoir effectuer toutes les opérations quantiques.

Nous savons (voir paragraphe II.2.2) qu'il suffit de disposer de deux portes pour pouvoir effectuer toutes les opérations quantiques : la porte C_{NOT} et la rotation à un qubit. Dès 1995, la porte C_{NOT} a été réalisée par le groupe

de David Wineland (voir ci-dessus). Les opérations de rotations à un qubit, quant à elles, sont effectuées aisément par des transitions Raman stimulées[148], à l'aide de deux faisceaux laser dont la différence de fréquence ('detuning') est égale à la fréquence de transition hyperfine du qubit. Le 4ème critère de DiVincenzo est ainsi satisfait.

En 2003, le groupe de Wineland apportait un outil de plus à la collection de portes quantiques à ions piégés. Il s'agissait d'une porte de changement de phase permettant, entre autres, de limiter la décohérence des qubits, et d'accélérer leurs manipulations[149]. En 2005, ce même groupe démontrait l'implémentation de l'algorithme de transformation de Fourier quantique (QFT), sur un système composé de 3 ions Beryllium[150]. Cet algorithme est utilisé dans celui de Shor, et du logarithme discret (voir chapitre II.3.3), et est au cœur de presque tous les algorithmes quantiques connus ayant une accélération exponentielle par rapport à leurs homologues classiques (c'est dire son importance). Cette implémentation utilisait une version modifiée 'semiclassique' de la QFT, utilisant des séries de mesures de qubits suivies de reconditionnement en phase, et le rendant quadratiquement plus efficace que la version 'totalement cohérente'.

Ainsi, non contents de satisfaire le 4ème critère de DiVincenzo, les systèmes quantiques à ions piégés permettent déjà d'implémenter des algorithmes quantiques assez complexes.

VII.4.5. L'architecture du système doit être en mesure d'accommoder un grand nombre de qubits.

Ce critère est toujours le plus difficile à satisfaire, raison pour laquelle nous ne disposons pas encore de QC. Il est également celui pour lequel les dispositifs à ions piégés ont le plus d'avance par rapport à leurs homologues supra ou semi-conducteurs.

En 2005, l'équipe autrichienne de Rainer Blatt à l'université d'Innsbrück, démontrait l'intrication du nombre record de 8 qubits[151]. Il s'agissait de qubits 'optiques' formés par le niveau fondamental $|0\rangle$ et un niveau excité à longue durée de vie $|1\rangle$ d'ions $^{40}Ca^{+}$. L'intrication provenait de la superposition des 8 états où un ion est dans le niveau fondamental et tous les autres sont excités : $|01...1\rangle + |101...1\rangle + ... + |11...10\rangle$. Cet état intriqué a été caractérisé par une mesure de tomographie quantique (voir paragraphe III.7), permettant de reconstruire sa matrice densité, comme le montre la figure suivante.

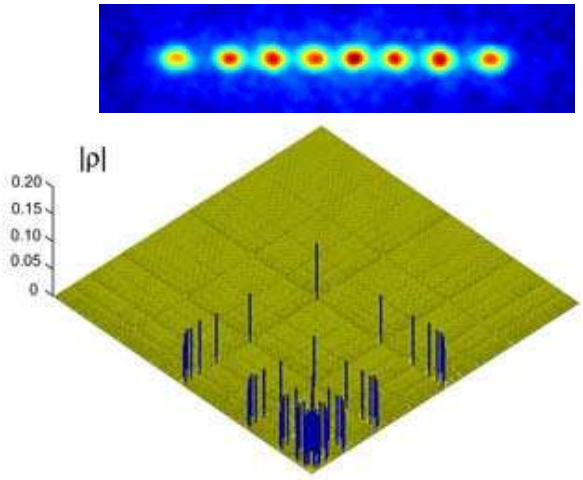


Figure 37 Démonstration en 2005, par le groupe autrichien de R. Blatt, de l'intrication de 8 ions piégés Ca^{+}. Haut : Image optique de la chaîne d'ions. Bas : Matrice densité obtenue par tomographie quantique des états. Crédits : R. Blatt, Université d'Innsbrück, http://heart-c704.uibk.ac.at/.

Toujours en 2005, et dans le même numéro du journal Nature, l'équipe de David Wineland au NIST publiait l'intrication de 6 qubits à ions[152]. L'intrication provenait ici de la superposition de seulement 2 états d'intrication maximale : $|000000\rangle + |111111\rangle$. Dans un tel état intriqué, dit 'chat de Schrödinger', la connaissance de l'état d'un seul qubit révèle immédiatement l'état de tous les autres qubits. Il est ainsi extrêmement fragile, sa cohérence étant perdue après la mesure d'un seul ion. En comparaison, dans l'état intriqué à 8 ions du groupe de Blatt, la mesure d'un ion fait perdre la cohérence de l'ensemble avec une probabilité de seulement 1/8.

En 2006, l'équipe de Wineland progressait encore dans l'augmentation du nombre de qubits, en parvenant à piéger 12 ions, à l'aide d'un piège 'sur circuit', que l'on détaille dans le paragraphe suivant.

VII.5. Les pièges à ions sur circuit

Ainsi, sur les cinq critères de DiVincenzo définissant un QC, les qubits à ions piégés satisfont assez bien aux quatre premiers. Le cinquième, qui concerne le nombre de qubits que le système est capable de gérer, est celui qui pose encore le plus de problèmes. Beaucoup de chercheurs y consacrent des recherches de plus en plus importantes, surtout à partir de l'année 2003, où les quatre premiers critères étaient assez bien résolus. Par exemple, l'équipe d'Innsbrück avait proposé d'utiliser un ion piégé dans une tête mobile, capable d'interagir avec un ensemble d'ions immobiles dans un plan et transporter l'information quantique de qubit en qubit[153]. Nous ne reviendrons pas sur cette approche, qui a été pour l'instant moins fructueuse que celle de l'équipe de David Wineland au NIST, que nous présentons ici. Afin d'augmenter le nombre de qubits que le système est capable de gérer, et donc le nombre d'ions à piéger, l'idée de ce groupe a été

de porter son attention vers les méthodes traditionnelles de la microélectronique classique, comme la photolithographie, afin de réaliser un piège 'sur circuit'.

Dans un ordinateur classique, les bits de données sont stockés sous forme de charges dans des zones mémoire, puis transférés dans la zone processeur sous forme d'impulsions électriques, où elles subissent l'action de plusieurs portes logiques. Enfin, le résultat de la manipulation est de nouveau transféré dans la zone mémoire, et stocké sous forme de charge électrique. De la même manière, un QC devra être en mesure de stocker, manipuler, lire et transférer de l'information quantique. Avec des ions piégés, une façon d'y parvenir est de disposer de plusieurs zones séparées dans l'espace : une consacrée au stockage des ions, une autre à leur manipulation et une autre à la transmission. Typiquement, les trois zones sont des pièges de Paul linéaires, comme ceux exposés ci-dessus, la zone de transmission étant un piège plus long que les autres.

En miniaturisant les pièges de Paul à l'aide des techniques de fabrication de la microélectronique, il est possible de réaliser ces trois zones de stockage, transmission et calcul, sur un circuit électrique semiconducteur. L'architecture la plus simple consiste en deux zones de stockage, reliées à une zone de calcul centrale par deux zones d'interconnexion. Les ions sont déplacés de la première zone de stockage à la zone de calcul en faisant varier la tension électrique des électrodes dc : en renforçant la tension devant un ion et en la diminuant derrière lui, il se retrouve poussé dans la direction voulue. Une fois dans la zone de calcul, les ions subissent les manipulations quantiques désirées (rotations, intrication, changement de phase), au moyen d'impulsions laser de durées bien déterminées. Le résultat du calcul peut alors être lu directement dans la zone de calcul, ou bien les ions peuvent être transférés dans la deuxième zone de stockage à travers une deuxième zone d'interconnexion.

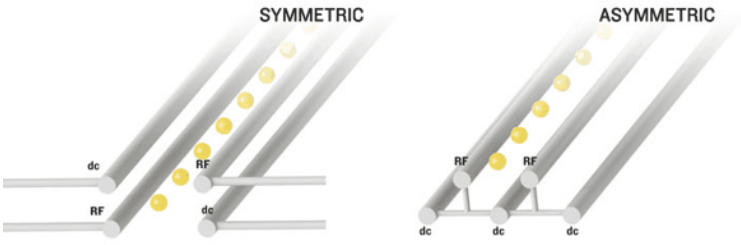


Figure 38 Les pièges à ions sur circuit se présentent principalement sous la forme 'symétrique' ou 'asymétrique'. Les pièges symétriques nécessitent de percer le circuit de part en part, et les ions sont piégés dans la tranche, alors que les pièges asymétriques permettent de piéger les ions au dessus du circuit sans avoir à le percer. Crédits : C. Monroe, NIST Boulder, dans IEEE Spectrum, 37-43, August 2007

Les pièges à ions sur circuits se rangent en deux catégories : les pièges symétriques et asymétriques, comme l'illustre la Figure 38.

Dans la géométrie symétrique, qui est celle utilisée au NIST et à Sandia, les électrodes dc et RF sont positionnées de telle manière à ce que le champ électrique s'annule le long de la ligne située au milieu des deux électrodes RF. Les ions sont piégés dans une tranchée réalisée dans le circuit, qui est bordée des quatre électrodes linéaires. La plupart du temps, la tranchée perce le substrat du circuit de part en part.

Le groupe de David Wineland au NIST utilise un substrat de GaAs percé sur toute son épaisseur au moyen de techniques standard de photolithographie et d'attaques sèches[154,155]. La tranchée mesure 60µm de large pour 1mm de long. Elle est divisée en plusieurs segments, typiquement 6 (voir la Figure 39), chacun disposant de 4 électrodes linéaires qui peuvent être pilotées indépendamment les unes des autres. Ceci permet la manipulation et le transfert des ions d'un segment à l'autre. Par exemple, l'application d'une tension négative sur les électrodes d'un segment permet d'attirer les ions positifs d'un segment voisin, et une tension positive les repousse.

Le problème principal de la géométrie symétrique provient de la finesse des substrats utilisés, qui entraîne une épaisseur réduite de la couche d'isolant séparant les électrodes superposées dc et RF. Avec les tensions élevées qui sont utilisées, ceci peut constituer une sérieuse limitation. Un consortium européen tente d'y apporter une réponse en créant des pièges symétriques contenant des couches d'isolant épaisses.

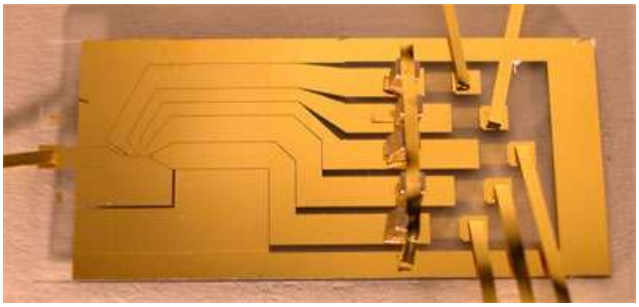


Figure 39 Photographie d'un piège à ions sur circuit fabriqué par le groupe de David Wineland au NIST. Crédits : D. Wineland, NIST, Boulder.

Dans la géométrie asymétrique, les électrodes RF ne sont pas situées symétriquement par rapport aux électrodes dc, et les ions flottent au dessus de la surface du circuit. L'intérêt principal de cette géométrie, est qu'elle évite à la fois le percement du substrat, et un agencement tridimensionnel complexe des électrodes. Le procédé de fabrication utilise ainsi des techniques bidimensionnelles

traditionnelles de la microélectronique, ce qui facilite beaucoup la mise en place d'un réseau de pièges interconnectés. Cette géométrie a été utilisée par le groupe de Wineland (électrodes en or sur un substrat en saphir Al_2O_3), et par les chercheurs des Bell Labs (électrodes en Aluminium et isolant en Silice), pour des applications de spectroscopie de masse portable appliquée à la détection de gaz nocifs.

Cependant, la géométrie asymétrique présente plusieurs inconvénients par rapport à son homologue symétrique. Tout d'abord, le positionnement des électrodes étant différent de celui qui est généralement utilisé dans les pièges de Paul, le piégeage des ions est plus difficile à contrôler, rendant le profil des tensions à appliquer beaucoup plus complexe. Il est également plus difficile de focaliser les faisceaux lasers sur les ions, car la réflexion des faisceaux sur le substrat rend la lecture des qubits délicate. Ne disposant pas ici de tranchée 'vide' comme dans la géométrie symétrique, il faut alors percer des trous à plusieurs endroits dans le substrat.

Qu'il s'agisse de géométrie symétrique ou asymétrique, les contraintes associées à la réalisation de circuits à ions piégés ne sont pas les mêmes qu'en électronique classique, principalement à cause des tensions élevées devant être appliquées. Comparées aux traditionnels 1.5V de la microélectronique, les tensions RF appliquées aux électrodes sont ici de l'ordre de 50 à 300 Volts, à des fréquences allant de 15 à 200 MHz. Il est alors difficile de trouver des matériaux faisant office d'isolant suffisamment robuste, et de dissiper la chaleur générée par les électrodes.

La miniaturisation des pièges à ions sur circuit présente également plusieurs difficultés expérimentales touchant le contrôle du mouvement des ions. La principale concerne l'apparition, sur les électrodes, de champs électriques parasites qui font vibrer et chauffer les ions. Ces champs ont une fréquence d'environ 1MHz, qui entre en résonance avec les modes de vibration des ions dans le piège. Ils sont beaucoup plus importants que prévu, et leur source reste pour l'instant un mystère. Il est possible de limiter leur effet, en abaissant la température des électrodes (passer de la température ambiante à 150K diminue le bruit d'un facteur 10), ou d'éloigner les ions de la surface en créant des pièges plus grands. Les recherches continuent pour comprendre ces bruits et tenter de les supprimer.

VII.6. Perspectives

En 1999 le laboratoire de physique du NIST lançait un des plus importants programmes mondiaux sur l'information quantique nommé 'Quantum Information Program' et incluant des physiciens de renom comme David Wineland, William Philips (prix Nobel de physique en 1997), Raymond Simmonds (voir le chapitre consacré aux qubits supraconducteurs), et des mathématiciens comme Emmanuel Knill. Ce laboratoire a su tirer parti de son expertise sur les ions piégés, acquise pendant des décennies de travaux portant sur les horloges atomiques. Ainsi, le groupe de David Wineland a su rapidement s'imposer comme un des groupes les plus avancés au niveau mondial sur les dispositifs quantiques à ions piégé. Après sa démonstration en 1995 de la première porte $C_{NOT,}$ il a été le premier à démontrer l'intrication de 4 qubits, puis celle des premiers codes correcteurs d'erreurs, de l'implémentation d'algorithmes complexes comme la transformée de Fourier quantique, et enfin la réalisation de pièges sur circuit. Récemment il est parvenu à piéger 12 ions magnésium sur un circuit asymétrique, comme le montre la figure suivante[156].

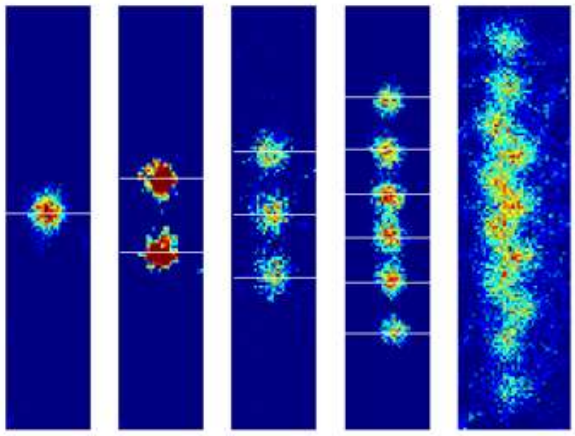


Figure 40 Image montrant 1, 2, 3, 6 et 12 ions magnésium piégés à l'aide d'un dispositif 'sur circuit' du groupe de David Wineland. Au-delà de 6, les ions sont si proches les uns les autres, qu'ils forment une chaîne en zig zag dans le piège de Paul. Crédits : D. Wineland, NIST, Boulder dans : S. Seidelin, et al. Phys. Rev. Lett. 96, 253003 (2006)

Malgré leur difficulté de fabrication et de contrôle, les architectures sur circuit ont permis aux pièges à ions de progresser rapidement dans la course au QC, en autorisant un stockage des ions plus important, et en facilitant leur manipulation. Les équipes de recherche les plus avancées, comme celle de Wineland, s'efforcent désormais d'augmenter encore le nombre d'ions piégés, tout en miniaturisant leurs circuits.

Cette miniaturisation facilite d'une part l'adressage des ions, mais surtout permet une accélération des calculs quantiques. En effet, la vitesse d'opération d'une porte à 2 qubits dépend directement de la fréquence de vibration des ions, elle même proportionnelle à l'inverse de la dimension des électrodes au carré. A l'avenir, la fabrication des pièges devrait pouvoir bénéficier grandement des techniques de micro-fabrication des MEMS. Il restera cependant à résoudre le problème de chauffage des ions dû à leurs vibrations parasites, qui augmente lorsque la taille des électrodes diminue[157].

Les prochaines générations de pièges à ions devraient donc permettre d'accommoder plus de qubits, tout en étant de plus en plus miniaturisés. Cependant,

disposer de nombreux qubits est une chose, parvenir à les manipuler en conservant leur intrication en est une autre. Sur ce point, l'architecture linéaire du piège de Paul risque d'être pénalisante, les ions ne pouvant pas s'entrecroiser, et devant rester dans l'ordre où on les a mis initialement. Pour qu'un tel système puisse évoluer vers le QC, avec plus de qubits et de complexité, il faudra qu'il puisse s'affranchir de cette limitation, en prévoyant des points de jonction à 3 pièges, où les ions pourront bifurquer d'une ligne à une autre. Dans un avenir proche, de telles jonctions devraient être réalisables sans rencontrer normalement de difficulté rédhibitoire, ce qui permettra de réaliser quelques calculs quantiques simples avec quelques dizaines de qubits. Des micropièges contenant 30 à 50 ions devraient être réalisables d'ici 5 à 10 ans[158].

Pour aboutir à une première ébauche de QC, il faudra cependant passer à l'échelle suivante, qui demandera au système de pouvoir gérer plus d'une centaine de qubits[159]. Pour que le système soit suffisamment robuste vis-à-vis de la décohérence, il faudra en outre qu'il soit épaulé de codes correcteurs d'erreurs efficaces. Ceci aura pour effet de démultiplier le nombre d'ions à gérer : il faudra typiquement prévoir 50 ions supplémentaires par qubit, soit plus de 5000 ions au total. Contrôler un réseau de pièges permettant de manipuler avec précision autant d'ions se révèle un défi incroyable. Le dispositif devra comporter quelques 50,000 électrodes dc, qui devront être pilotées indépendamment et avec beaucoup de précision. Plusieurs dizaines, voire centaines de ces électrodes se croiseront en formant des points de jonction. Il faudra également disposer de plusieurs dizaines de lasers pour le refroidissement, la détection et l'opération des portes quantiques. Ces lasers devront être en mesure de garder un alignement très précis avec les ions durant toutes leurs manipulations, à l'aide de miroirs motorisés se déplaçant grâce à des boucles rétroactives. Avec 5000 ions, une telle tâche relève actuellement de l'impossible. Dans le meilleur des cas, en supposant que tous ces défis soient relevés, le contrôle d'un tel QC sera d'une telle complexité qu'il devra faire appel à un puissant ordinateur classique pour fonctionner. L'étape suivante, celle d'un véritable QC universel comportant de l'ordre du million de qubits relève, selon David Wineland d'un « abysse quantique ». Le défi est colossal, même s'il reste purement technologique car aucune objection physique fondamentale n'interdit en effet la réalisation d'un tel QC.

Malgré les difficultés gigantesques qui restent à résoudre avant de pouvoir envisager de construire un QC à l'aide d'ions piégés, les travaux récents ont progressé si vite, avec des résultats si prometteurs, que beaucoup d'espoirs sont permis. Dans tous les cas, les qubits à ions piégés font actuellement parti des meilleurs candidats pour le futur QC. Un sondage portant sur presque 200 personnes (pour la plupart spécialistes du domaine), les place même en tête des candidats avec 30% des voix[160]. Par rapport à leurs concurrents semi ou supraconducteurs, ils possèdent l'avantage d'une grande efficacité de préparation et de lecture, ainsi que de longs temps de cohérence. Ils sont toutefois handicapés par une relative lenteur d'opération des portes quantiques et les difficultés liées à l'architecture linéaire dont on a parlé.

VIII. LES ATOMES FROIDS EN RESEAUX OPTIQUES

VIII.1. Des condensats de Bose Einstein aux réseaux optiques

A cause de leur neutralité électrique, les atomes neutres interagissent moins que les ions avec leur environnement. Ils sont ainsi plus robustes vis-à-vis de la décohérence, ce qui les rend attractifs pour le calcul quantique. Le revers de la médaille est que les techniques de refroidissement et de piégeage sont plus complexes à mettre en œuvre, et ne peuvent pas être miniaturisées sur circuit, comme on l'a vu avec le piège de Paul. Toutefois, ces techniques ont fait énormément de progrès durant ces 10 dernières années, depuis les travaux fondateurs de Claude Cohen-Tannoudji, Steven Chu et William Philips, qui reçurent le prix Nobel de physique en 1997 pour leurs travaux sur le refroidissement d'atomes par laser. En 1995, une étape importante fut franchie avec la mise en évidence d'un condensat de Bose Einstein (BEC) à l'institut JILA à Boulder (institut mixte entre l'université du Colorado et le NIST) et au MIT, ce qui valut le prix Nobel de Physique à Eric Cornell du NIST, Carl Wieman de l'université du Colorado et Wolfgang Ketterle du MIT. Un BEC est un état quantique particulier d'un ensemble d'atomes (2000 atomes de Rubidium dans l'expérience de Cornell et Wieman) à une température tellement basse (20nK en l'occurrence) qu'ils se regroupent tous dans un même état collectif de plus basse énergie, ce qui est autorisé en mécanique quantique par la nature 'bosonique' de ces atomes. En France, le laboratoire Kassler Brossel (LKB) à l'ENS s'est rendu célèbre pour ses travaux sur les BEC, sous l'impulsion de Claude Cohen Tannoudji. Les applications des BEC concernent principalement la métrologie de haute précision, avec les horloges atomiques (projet PHARAO, Christophe Salomon au LKB). Cependant, les progrès réalisés dans le contrôle des BEC sont tels, que de nouvelles applications sont envisagées, en particulier en informatique quantique.

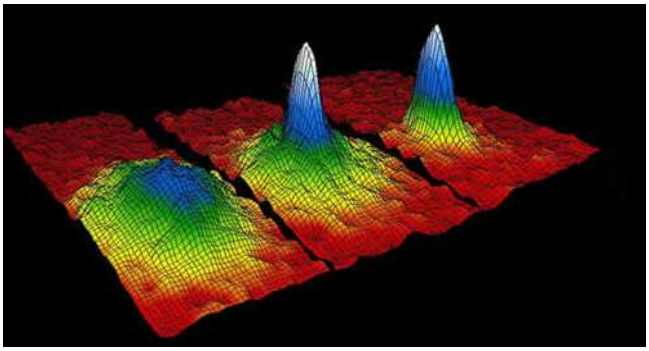


Figure 41 Image du premier condensat de Bose Einstein réalisé en 1995 par l'équipe de Cornell et Wieman au JILA. Crédits : Cornell et Wieman, JILA, http://jilawww.colorado.edu/bec/

Les idées récentes concernant l'utilisation de BEC pour le calcul quantique utilisent des réseaux optiques dans lesquels sont piégés des atomes froids. En Europe, l'équipe la plus en pointe sur ce sujet est celle d'Immanuel Bloch à l'université de Mainz en Allemagne. Aux Etats-Unis, il s'agit du groupe de William Phillips au NIST à Gaithersburg dans le Maryland. Ce dernier confine des atomes de rubidium dans des réseaux optiques dont le potentiel est en forme de 'boîte à œufs' (comme le montre la figure suivante), crées par les ondes stationnaires d'interférences à l'intersection de 4 lasers. Le refroidissement laser des atomes est suffisant pour qu'ils occupent docilement tous les sites de piégeage du potentiel[161]. L'ensemble ressemble alors à un réseau cristallin, raison pour laquelle on l'appelle 'réseau optique'.

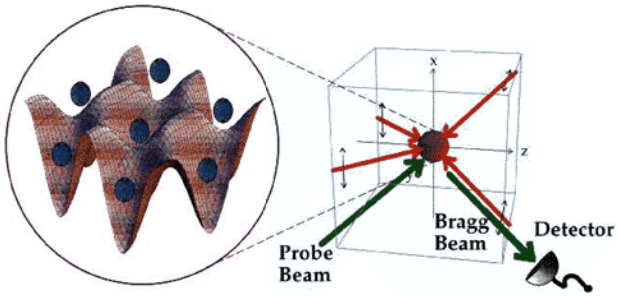


Figure 42 Expérience de piégeage d'atomes froids dans un réseau optique bidimensionnel. Crédits : William Philips, NIST Gaithersburg, http://physics.nist.gov/Divisions/Div842/Gp4/lattices.html

VIII.2. Logique conditionnelle à atomes froids

Nous donnons ici les grandes lignes des idées sous-jacentes à l'utilisation de réseaux optiques à atomes froids pour la réalisation de portes quantiques[162]. Elles sont expliquées en détail dans le cours de Serge Haroche du collège de France[163].

Les qubits sont ici des atomes froids (rubidium par exemple) dans deux sous-niveaux hyperfins de l'état fondamental. Deux atomes dans les deux niveaux $|0\rangle$ et $|1\rangle$ peuvent être piégés dans les puits voisins de deux réseaux optiques unidimensionnels, superposés à un instant initial, et agissant chacun de façon sélective sur un des états $|0\rangle$ ou $|1\rangle$ (couleurs rouges et bleues sur la figure suivante). Il est possible de déplacer ces réseaux de manière à amener les deux atomes dans un même puits, à les laisser interagir pendant un temps défini, avant de les ramener dans leur position initiale. L'interaction aura pour effet de déphaser l'ensemble $|0,1\rangle$, tout en laissant les qubits dans le même état quantique.

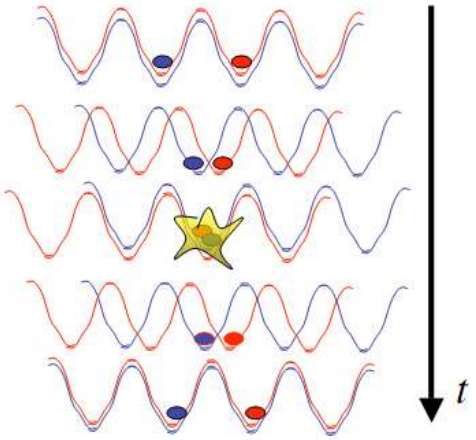


Figure 43 Interaction de deux atomes froids dans deux réseaux optiques superposés, qui sont déplacés de manière contrôlée. Crédits : Serge Haroche, Collège de France, cours 2006-2007

Avec cette technique de déplacement contrôlé de réseaux optiques, il est ainsi possible de construire une porte conditionnelle. L'opération consiste à opérer un aller retour des deux réseaux, vers la gauche s'il s'agit d'un qubit $|0\rangle$, et vers la droite s'il s'agit d'un qubit $|1\rangle$.

- Si l'ensemble des deux qubits (atome de gauche puis atome de droite) est dans l'état $|0,0\rangle$, ils sont tous les deux déplacés vers la gauche sans se rencontrer.
- Dans l'état $|0,1\rangle$, l'atome de gauche est déplacé vers la gauche, et celui de droite vers la droite : ils s'éloignent sans se rencontrer
- Dans l'état $|1,0\rangle$, l'atome de gauche est déplacé vers la droite, et celui de droite vers la gauche : ils se rencontrent et subissent la collision déphasante. L'état devient $e^{-i\varphi}|1,0\rangle$
- Dans l'état $|1,1\rangle$, les deux atomes sont déplacés vers la droite, sans se rencontrer.

Au final, l'opération n'affecte que l'état $|1,0\rangle$ qui subit un déphasage d'un angle φ. Il s'agit bien d'une porte logique conditionnelle.

VIII.3. Intrication de réseaux optiques

Grâce à cette porte logique conditionnelle, on peut construire des états intriqués à 2, 3, puis à *N* atomes, toujours en géométrie 1D. Il est ensuite possible de généraliser à des géométries bi puis tridimensionnelles en translatant les réseaux d'une demi-période λ/2, successivement dans les directions *Ox* et *Oy* (voir figure suivante), puis *Oz*. On peut ainsi obtenir des états dits 'cluster' d'intrication maximale à *N* atomes[164]. Une telle intrication a été mise en évidence dans les expériences du groupe d'I. Bloch[165]. Cette technique d'intrication de réseaux optiques présente toutefois l'inconvénient de devoir déplacer physiquement les atomes. Un résultat équivalent peut être obtenu en laissant les atomes fixes, et en jouant sur des transitions virtuelles entre sites dues à un petit effet tunnel[163].

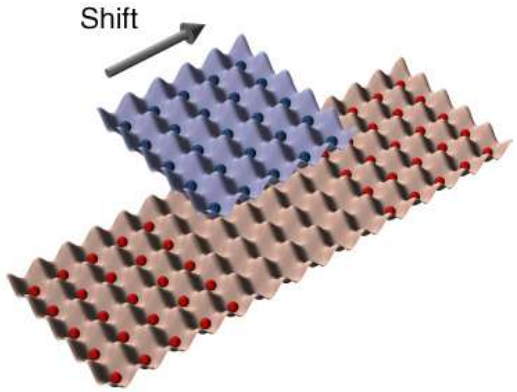


Figure 44 Principe de préparation d'un état intriqué dans un réseau optique bidimensionnel. Les réseaux σ+ et σ- sont déplacés d'une demi-période dans la direction *Ox*, comme montré ici, puis dans la direction perpendiculaire *Oy*. Crédits : I. Bloch, Université de Mainz, http://www.quantum.physik.uni-mainz.de/en/bec/gallery/index.html

VIII.4. Ordinateur unidirectionnel

Grâce à ces réseaux d'atomes intriqués dits 'clusters', Robert Raussendorf et Hans J. Briedel ont imaginé en 2001 un type particulier d'ordinateur quantique appelé « ordinateur unidirectionnel » (one way quantum computer)[166]. Dans un tel QC, l'algorithme est défini par la forme du circuit, et ses étapes de calculs consistent uniquement en des mesures à un qubit, qui s'effectuent dans une seule direction, jusqu'aux qubits finaux qui donnent le résultat.

Le principe de fonctionnement d'un ordinateur unidirectionnel est illustré sur la figure suivante. Le circuit est préparé au début du calcul en intriquant les atomes d'un réseau optique bidimensionnel dans un état 'cluster'. Certains spins atomiques (les qubits) sont mesurés dans la direction *Oz* (hors du plan, symbolisés par les cercles), ce qui 'dessine' le circuit, qui apparait alors en grisé. Le calcul proprement dit consiste alors à mesurer, de gauche à droite, les spins des atomes selon des directions dans le plan *xy* (représentées par les flèches) qui dépendent des résultats des mesures précédentes. Le résultat du calcul est donné par la mesure des spins en bout de chaîne.

Avec un tel QC, les portes quantiques sont caractérisées par des dispositions spatiales particulières. Par exemple, une porte de rotation à un qubit est donnée par 5 atomes consécutifs le long d'une horizontale. Le premier atome est dans l'état initial du qubit. Cet atome, ainsi que les trois suivants, subissent des mesures selon des directions données par les angles d'Euler de la rotation, et le dernier atome se retrouve dans l'état final de la rotation. Les portes à deux qubits sont obtenues en mesurant des spins le long des maillons verticaux reliant deux chaînes de spin horizontales.

L'originalité de l'ordinateur unidirectionnel, est que l'intrication est réalisée une fois pour toute au début, et est défaite par les mesures au fur et à mesure que le calcul progresse. Un tel processeur n'est pas réversible, contrairement au concept de QC à base de portes quantiques dont on a parlé jusqu'à présent.

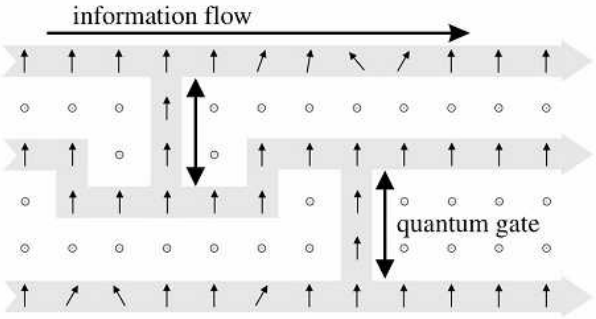


Figure 45 Principe de fonctionnement d'un ordinateur quantique 'unidirectionnel'. L'intrication est réalisée initialement dans un état 'cluster', à la suite de quoi le calcul consiste uniquement en des mesures qui forment le programme de l'ordinateur. Ces mesures 'impriment' le circuit qui apparait ici en grisé. Crédits : R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. 86, 5188 (2001)

VIII.5. Simulateurs analogiques à gaz de Fermi superfluide

Des travaux récents s'intéressent à l'utilisation des atomes froids en vue de construire des simulateurs quantiques analogiques[167]. Contrairement au QC étudié jusqu'à présent, de tels simulateurs ne seraient pas basés sur la programmation d'opérations logiques, mais sur la modélisation de systèmes physiques par des systèmes quantiques contrôlés, ayant la même équation d'évolution. De par leur nature analogique et non-universelle, ces simulateurs s'éloignent du cadre de ce dossier, et nous n'entrerons pas dans les détails.

Dans les années 80, Richard Feynman fut un des premiers physiciens à prôner l'utilité et la puissance des simulateurs quantiques analogiques[168]. Depuis, la route qui a mené aux premiers dispositifs expérimentaux a été

semée d'obstacles. En effet, pour fonctionner en simulateur quantique, le système physique utilisé ne doit contenir aucune impureté, de manière à correspondre exactement au modèle théorique. Les progrès réalisés dans les atomes froids et les BEC dans les années 90 ont apporté quelques premières pistes.

En particulier, en 2005, l'équipe de Ketterle au MIT mettait en évidence un phénomène de superfluidité d'un gaz de Fermi dégénéré[169]. La superfluidité, ou absence de friction dans un liquide, est un phénomène souvent observé avec des particules appelées 'bosons' (hélium superfluide, BEC), mais plus rarement avec des 'fermions', sauf lorsque ces derniers s'assemblent en paires dites 'de Cooper', comme c'est le cas dans la théorie BCS de la supraconductivité. L'expérience de Ketterle mettait à profit le contrôle de la force d'interaction entre deux atomes fermioniques (^{6}Li) à l'aide d'un champ magnétique près de la résonance de Feshbach[170], pour explorer le régime d'interactions intermédiaire entre celui d'un BEC et celui des paires de Cooper de la théorie BCS. Sans entrer dans les détails[167], cette expérience constituait un premier pas vers la réalisation d'un simulateur quantique.

IX. L'OPTIQUE QUANTIQUE

Historiquement, les premières expériences de calcul quantique avec des photons datent de 1997 (équipe de Zeilinger, voir Annexe XI.4), et concernaient la téléportation quantique. Les photons polarisés s'avèrent en effet d'excellents qubits, car ils sont très résistants à la décohérence, et peuvent se propager sur de grandes distances[158]. Leur problème est qu'ils n'interagissent quasiment pas entre eux. Pour cette raison, les expériences de calcul quantique succédant à la prouesse de Zeilinger ont eu tendance à ne plus utiliser de photons polarisés comme qubits, au détriment des autres médiateurs qui ont été étudiés dans ce dossier (ions, atomes, spins etc…). Les photons ont pourtant continué à être utilisé en tant qu'intermédiaires de calcul, d'initialisation, de mesure, ou comme bus quantique. Ils pourraient à l'avenir retrouver une place privilégiée en informatique quantique, grâce aux progrès réalisés dans une discipline qui s'intéresse aux interactions entre atomes et photons : l'optique quantique.

L'optique quantique permet, en effet, de coupler des photons entre eux par l'intermédiaire d'atomes placés dans des cavités résonantes. Les techniques mises en œuvre dans ces expériences sont maintenant très bien contrôlées, notamment par l'équipe de Serge Haroche à l'ENS qui est parmi les plus avancées dans ce domaine[171]. Dans une de ses expériences célèbres, cette équipe est parvenue, en 1996, à observer en direct le phénomène de décohérence dans un système couplant des atomes froids à une double cavité résonante[172].

IX.1. Atomes de Rydberg et cavité supraconductrice

Au cœur de ces expériences d'optique quantique, se trouvent deux systèmes microscopiques en couplage quantique fort : un atome dit de 'Rydberg' et un mode électromagnétique de cavité. Les atomes de Rydberg sont des atomes excités possédant un grand nombre quantique (n>>1), ce qui leur confère de nombreuses propriétés très intéressantes : une très bonne réponse aux champs micro-ondes, une longue durée de vie, et une description physique relativement simple, avec le comportement d'un système quasiment parfait de qubits à deux niveaux. L'exemple que nous retiendrons ici, et qui est couramment utilisé par le groupe de Haroche, est obtenu avec du ^{85}Rb, entre les niveaux n=50 ($|g\rangle$, durée de vie de 30ms) et n=51 ($|e\rangle$).

Le deuxième élément d'une expérience d'optique quantique est un mode de cavité à quelques photons, obtenu dans une cavité micro-onde ultra-réfléchissante. Une telle cavité est constituée typiquement par deux miroirs supraconducteurs refroidis à 0.5K, donnant un mode gaussien de faible volume ($\varnothing$=0.6mm au centre). Les pertes sont si faibles que, dans les expériences du groupe de Haroche, la durée de vie des photons dans la cavité est passée de 0.16ms en 1996, à 130ms dans les dernières expériences[173], un temps qui permettrait au photon de parcourir un dixième de la distance Terre-Lune.

Dans le schéma type d'une expérience du groupe de Haroche (voir figure suivante), la cavité est résonante avec la transition entre les deux niveaux $|g\rangle$ et $|e\rangle$ du ^{85}Rb, soit 51.1GHz. Les atomes de Rydberg sont envoyés un par un à travers la cavité. Leur vitesse est contrôlée par pompage optique laser, ce qui permet d'ajuster leur temps de passage, et donc leur temps de couplage avec le champ. Dans certaines expériences, des impulsions micro-ondes sont appliquées aux atomes avant et après leur passage dans la cavité (R_1 et R_2 sur la figure). Une telle disposition constitue un interféromètre de Ramsey, utile pour étudier l'interaction atome-photon et pour la réalisation de portes quantiques, comme nous le verrons plus loin.

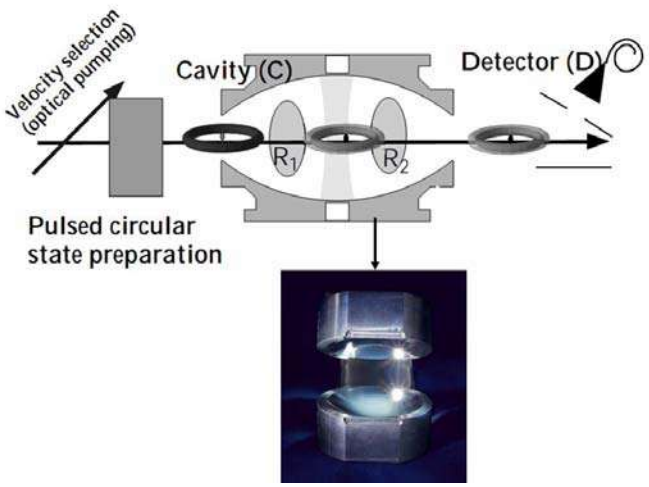


Figure 46 Schéma opératoire d'une expérience d'optique quantique en cavité. La photographie du bas montre la cavité micro-onde à miroirs supraconducteurs, utilisée dans les expériences du groupe de Haroche. Les atomes de Rydberg (anneaux) traversent cette cavité avec une vitesse et un état quantique contrôlés, et sont détectés en sortie après avoir été couplés avec le mode gaussien de cavité (en grisé). R1 et R2 symbolisent des impulsions micro-ondes permettant de transformer le dispositif en interféromètre de Ramsey. Crédits : Serge Haroche, ENS[174]

IX.2. Oscillations de Rabi et intrication

Lorsque la cavité est résonante avec la transition $|g\rangle \rightarrow |e\rangle$ à 51.1GHz, et qu'un atome de Rydberg y est présent, le système atome-cavité est dans un couplage 'fort', et évolue en effectuant des oscillations permanentes dites de Rabi[175]. Supposons que le système atome-cavité soit initialement dans l'état $|e,0\rangle$: l'atome de Rydberg est dans l'état $|e\rangle$ et la cavité est vide de photons. Les oscillations de Rabi font alors évoluer le système entre les états $|e,0\rangle$ et $|g,1\rangle$, comme le montre la figure suivante. En physique classique, ces oscillations correspondraient à des absorptions et émissions répétées de photons par l'atome. Ici, le système évolue en passant par un ensemble d'états intermédiaires, qui sont des états intriqués entre les deux états $|e,0\rangle$ et $|g,1\rangle$. Plusieurs solutions techniques permettent de contrôler cette intrication, en jouant sur le temps de couplage atome-cavité : modification de la vitesse des atomes, ou application d'un champ électrique qui déplace les niveaux de l'atome par effet Stark, et le découple du champ à un instant voulu.

Il est ainsi possible d'appliquer au système une impulsion Rabi de π/2 (voir figure), qui a pour effet de réaliser la superposition cohérente $1/\sqrt{2}\left(|e,0\rangle + |g,1\rangle\right)$. Il est intéressant de noter que cet état intriqué survit après la sortie de l'atome de la cavité. Une impulsion Rabi de π a pour effet de faire passer le système dans l'état $|g,1\rangle$. Elle réalise ainsi la porte *SWAP*, qui échange les états de l'atome et de la cavité. Enfin, une impulsion 2π ramène le système dans l'état initial, avec un atome excité et pas de photon dans la cavité, mais le signe de l'état est inversé, il devient $-|e,0\rangle$. Ces opérations élémentaires constituent les briques de base pour la réalisation de portes quantiques[176].

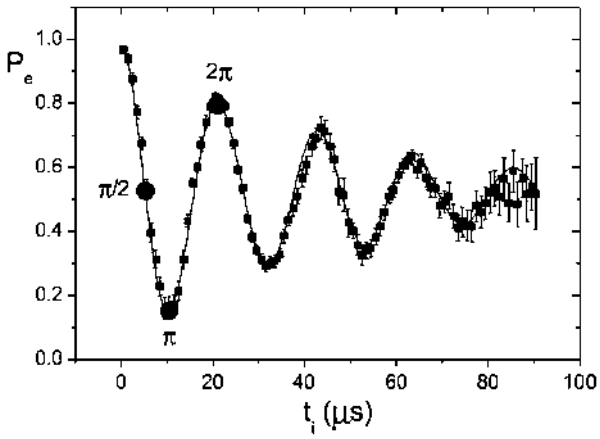


Figure 47 Oscillations quantiques de Rabi d'un système atome-cavité, initialement dans l'état $|e,0\rangle$ et passant périodiquement dans l'état $|g,1\rangle$ et tous les états intermédiaires d'intrication quantique. La courbe a été obtenue en répétant l'expérience de couplage atome-cavité un grand nombre de fois, avec des temps d'interaction t_i différents, et en mesurant la probabilité Pe que l'atome en sortie soit dans l'état $|e\rangle$. Les impulsions Rabi importantes π/2, π et 2π sont indiquées, car elles correspondent à des opérations quantiques élémentaires très utiles (intrication, SWAP et déphasage). Crédits : Serge Haroche, ENS[174]

IX.3. Portes quantique conditionnelles

Une impulsion Rabi de 2π ramène ainsi l'atome et la cavité dans leur état initial, mais modifie la phase de la fonction d'onde du système. Si cette dernière était initialement $|g,1\rangle$, elle change de signe pour devenir $-|g,1\rangle$. En revanche, si le système est initialement dans l'état $|g,0\rangle$, l'atome ne rencontre aucun photon dans la cavité avec lequel se coupler, et il ressort exactement dans le même état. La fonction d'onde du système $|g,0\rangle$ est alors inchangée, et conserve son signe.

Au final, l'impulsion Rabi de 2π a pour effet les opérations suivantes : $|g,0\rangle \rightarrow |g,0\rangle$ et $|g,1\rangle \rightarrow -|g,1\rangle$. Elle constitue ainsi une porte quantique conditionnelle à phase[177], inversant le signe de la fonction d'onde (qubit cible) si et seulement si la cavité contient un photon (qubit de contrôle).

Les portes quantiques conditionnelles à phase ne sont cependant pas suffisantes pour produire l'ensemble des opérations quantiques requises par un QC. Des expériences un peu plus complexes, faisant intervenir l'interféromètre de Ramsey présenté plus haut, permettent de créer des portes quantiques conditionnelles opérant directement sur les états des qubits (photon et atome). En particulier, il a été possible de réaliser la porte C_{NOT} avec le photon dans la cavité comme qubit de contrôle et l'état de l'atome comme qubit cible.

L'expérience utilise un état supplémentaire de l'atome noté *i*, correspondant à n=49 (les états *g* et *e* correspondent à n=50 et 51). L'intérêt de cet état supplémentaire est que la transition $i \to g$ est résonante avec l'interféromètre de Ramsey R_1-R_2, mais pas avec la cavité (résonante sur $e \to g$). Ainsi, la cavité étant réglée sur une impulsion Rabi de 2π, seuls les atomes dans l'état *g* subiront le déphasage de π (changement de signe), à condition que la cavité comporte un photon. Les atomes dans l'état *i* traverseront eux la cavité sans être affecté, quel que soit le nombre de photons présents. Les franges d'interférence Ramsey de la transition $i \to g$ seront donc inversées lorsque le nombre de photons dans la cavité passera de 0 à 1 (voir figure suivante). Avec un choix de phases convenables entre les impulsions Ramsey[163], l'atome en sortie de l'expérience sera détecté dans l'état *g* si la cavité contient 0 photon, et dans *i* si elle contient 1 photon. L'expérience réalise ainsi la porte quantique $C_{NOT} : |g,0\rangle \to |g,0\rangle, |g,1\rangle \to |i,1\rangle, |i,0\rangle \to |i,0\rangle,$ $|i,1\rangle \to |g,1\rangle$. On se limite en pratique aux deux premiers cas, car l'atome est dans l'état $|g\rangle$ lorsqu'il pénètre dans le dispositif.

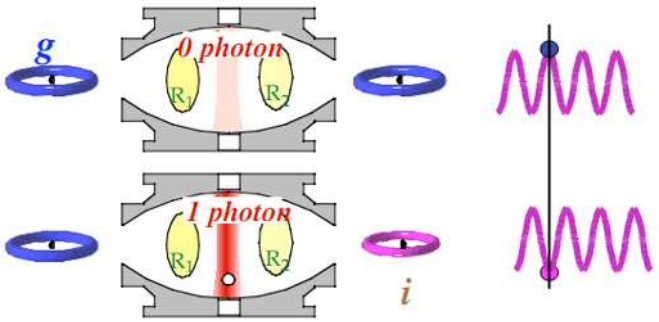


Figure 48 Interféromètre de Ramsey réalisant une porte quantique C_{NOT}, entre le nombre de photons dans la cavité (qubit de contrôle) et l'état quantique de l'atome (qubit cible). Avec une impulsion Rabi de 2π dans la cavité, les franges d'interférence (courbes à droite) sont renversées selon que la cavité contient 0 ou 1 photon. Lorsque le déphasage des impulsions Ramsey est approprié (point sur les courbes), l'atome ressort du dispositif dans l'état $|i\rangle$ (n=49) s'il y a un photon dans la cavité, et dans l'état $|g\rangle$ (n=50) sinon. Crédits : Serge Haroche, ENS, cours du Collège de France (2006-2007).

Cette expérience réalise, en plus de la porte quantique C_{NOT}, un exploit de physique quantique : mesurer un photon sans l'absorber[178,179,173]. L'atome emporte en effet une information sur le champ électromagnétique présent dans la cavité sans que le nombre de photons présents dans cette dernière ne soit affecté. Si, en entrant dans l'appareil, l'atome de Rydberg est dans l'état $|g\rangle$, et qu'en sortant il est mesuré dans l'état $|i\rangle$, cela voudra dire qu'il y avait un photon dans la cavité, et qu'il y est encore. C'est là tout l'intérêt du système : le photon n'est pas détruit par la mesure, et pourra être observé de nouveau plusieurs fois. On parle de mesure non-destructive du champ, ou QND (Quantum Non Destructive).

IX.4. Perspectives

Les progrès réalisés en optique quantique en cavité ont été très importants durant ces dernières années, en particulier dans le groupe de Serge Haroche. L'intrication atome-photon et les phénomènes liés à la décohérence sont maintenant bien compris et maîtrisés[172]. A l'aide d'interféromètres de Ramsey, il est également possible d'intriquer plusieurs atomes entre eux par échange de photons. Des intrications à deux[180], puis trois atomes[181] ont ainsi pu être démontrées expérimentalement. Il est même possible, comme on l'a vu, de réaliser une mesure non-destructive du champ de cavité, permettant entre autres de détecter la présence d'un photon sans l'absorber. Enfin, des dispositifs basés sur les interférences de Ramsey ont mis en évidence les notions même de complémentarité onde-particule[182], chères aux pères fondateurs de la mécanique quantique[iv]. Ces avancées spectaculaires, liées à l'excellente maîtrise obtenue avec le système atome-cavité, rendent la discipline très prometteuse. La réalisation des premières portes quantiques (de phase, puis porte C_{NOT}) est une première étape sur la longue route qui mène à l'ordinateur quantique.

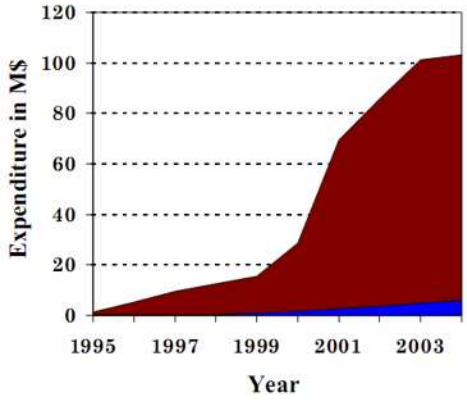
[iv] *Ces dispositifs simulaient l'expérience de pensée de Bohr, dans laquelle un interféromètre de Young comportait une fente mobile permettant de détecter le chemin emprunté par les photons. Le fait de posséder une telle information détruit les interférences, les photons se comportant alors comme des particules.*

X. CONCLUSION

L'ordinateur quantique a pu apparaître un temps comme un calculateur magique, à l'origine de la révolution informatique du prochain millénaire. Ceci a été largement sur-évalué par l'imagination populaire, à cause principalement du mystère planant autours des concepts de mécanique quantique, souvent mal compris et mal interprétés. Il est très peu probable en effet, que le QC supplante intégralement l'ordinateur classique, pour la même raison que la mécanique quantique ne remplace pas la physique classique pour la grande majorité des problèmes quotidiens[1]. Dans le monde macroscopique, personne ne s'aventure en effet dans la résolution de l'équation de Schrödinger pour concevoir un avion ou une voiture. De la même manière, le QC du futur sera réservé à la résolution de problèmes particuliers, pour lesquels le parallélisme quantique apporte un avantage décisif.

En particulier, le QC donne l'espoir de pouvoir un jour résoudre efficacement (en temps polynomial) des problèmes complexes, qui sont insolubles avec des ordinateurs classiques, à cause de l'explosion exponentielle de leur temps de calcul. Des algorithmes quantiques efficaces ont déjà vu le jour, avec la découverte spectaculaire des algorithmes de Shor et de Grover dans les années 90, suivie de la mise au point de nombreuses variantes et améliorations. Malgré leur nombre encore restreint, ces algorithmes quantiques sont théoriquement très efficaces, et apporteront à terme des avantages calculatoires notables. S'ajoute à cela la mise au point de codes correcteurs d'erreur, autorisant une certaine dose de décohérence sans laquelle le QC ne verrait certainement jamais le jour.

Grâce à l'algorithme de Shor, un QC pourra factoriser rapidement de très grands nombres entiers, ce qui rendra caduques les méthodes de cryptage actuelles, basées pour l'essentiel sur la technique RSA. Le gouvernement américain a vite compris les enjeux que cela représentait en termes de sécurité nationale. Il s'est donc engagé très tôt dans la promotion des recherches liées à l'informatique quantique, avec des moyens financiers très importants (voir figure suivante). Les Etats-Unis se sont ainsi rapidement placés à la tête des recherches mondiales dans ce domaine, aussi bien en termes de quantité (publications, nombre d'équipes), que de qualité (percées notables). Les financements américains ont connu une accélération brutale autours de l'an 2000, pour passer à environ 100 millions de dollars en 2004, bien au-delà de ce que pouvaient se permettre les pays concurrents comme le Japon (25 M$), et environ dix fois supérieurs aux dépenses de l'ensemble des principaux pays européens[183] (France, Allemagne, Autriche, Royaume Unis, Pays Bas, Suisse, Danemark et Italie). En 2004, la DARPA avait proposé un projet ambitieux, appelé FOQUS (Focused Quantum Systems), visant à développer un QC capable de factoriser un nombre à 128 bits. Ce projet n'a cependant jamais été approuvé par le gouvernement. Après son abandon, les financements fédéraux ont été revus à la baisse, et n'ont toujours pas retrouvé le niveau exceptionnel qu'ils avaient atteint en 2004.



	Financements 2004 en M$
US	100
Japon	25
Europe	10
Australie	5
Chine	4
Corée	1.3

Figure 49 Haut : Financements fédéraux américains en informatique quantique jusqu'en 2004. La zone bleue représente les financements du NIST. Bas : Financements public en informatique quantique, dans les principales zones du monde. Crédits : C. J. Williams, NIST[184].

Sur le front des réalisations expérimentales, les recherches ont beaucoup progressé durant ces dix dernières années. Elles ont fait appel à différentes approches, appartenant à des disciplines scientifiques très variées :

- les qubits supraconducteurs à base de jonctions Josephson,
- les qubits à boites quantiques semiconductrices
- les ions piégés dans le vide,
- les spins nucléaires de molécules en solution, pilotés par résonance magnétique nucléaire,
- Des atomes de Rydberg, des défauts optiques cristallins, ou des cavités résonantes relevant du domaine de l'optique quantique.

L'approche utilisant les circuits supraconducteurs est séduisante, car elle autorise l'utilisation des procédés de fabrication éprouvés de la microélectronique. En outre, elle a permis la réalisation de qubits en utilisant des approches variées (qubits de charge, de phase, de flux ou intermédiaires). Ces qubits sont faciles à initialiser et peuvent être mesurés en 'single shot' avec de bonnes

fiabilités. Certains d'entre eux possèdent des temps de cohérence importants (~µs), d'autres ont été intriqués et ont permis de réaliser les premières portes quantiques. Les sources de bruit sont toutefois encore mal comprises, et les mécanismes de relaxation et de déphasage doivent être mieux quantifiés. Pour progresser sur la longue route qui mène au QC, on attend de cette approche qu'elle puisse, dans la prochaine décennie, démontrer l'intrication d'une dizaine de qubits, avec l'opération des principales portes quantiques et des premiers algorithmes.

Les dispositifs semiconducteurs offrent les mêmes avantages que ceux à base de supraconducteurs, en ce qui concerne les facilités de fabrication, et la possibilité de réaliser des architectures complexes capables à terme d'accueillir un grand nombre de qubits, tout en conservant un bon interfaçage. Les qubits à spins sont suffisamment robustes, bien que les temps de cohérence soient nettement inférieurs à ceux des qubits supraconducteurs. Les dispositifs à semiconducteurs constituent finalement une approche très prometteuse, même s'ils sont pour l'instant moins avancés que leurs homologues supraconducteurs.

Les qubits à ions piégés disposent de temps de cohérence exceptionnels, et sont particulièrement faciles à initialiser. Des techniques efficaces d'intrication et de manipulation ont été mises au point, permettant d'obtenir un nombre record de qubits intriqués (8 à ce jour), de démontrer les principales portes quantiques, quelques algorithmes quantiques simples, et les premiers codes correcteurs d'erreurs. Des microcircuits ont vu le jour, permettant d'espérer la réalisation prochaine de dispositifs encore plus complexes et comportant un nombre toujours supérieur de qubits. Sur le moyen terme, il s'agira d'améliorer les principales sources de décohérence : émission spontanée, bruit laser, fluctuation des champs électriques dans les électrodes.

L'approche utilisant la résonance magnétique nucléaire en solution utilise des macro-molécules comportant un petit nombre (7, voire 10 au maximum) de spins nucléaires, qui forment les différents qubits que l'on manipule à l'aide de la RMN. Cette approche a connu son heure de gloire en 2001, avec la factorisation du nombre 15 grâce à l'algorithme de Shor. Une avancée majeure mais sans suite, principalement à cause du problème de perte de signal lié à l'augmentation du nombre de spins. Ainsi, cette approche ne sera certainement pas à l'origine du futur QC. Elle aura toutefois permis de nombreuses percées théoriques et expérimentales.

Les approches utilisant l'optique quantique bénéficient d'une facilité de manipulation relative des photons, et des importants progrès réalisés en cryptographie quantique et téléportation. Toutefois, même s'il possède de nombreux avantages en termes de polarisation, transmission, interférences, mesures, le photon est une particule sans masse qui est très difficile à garder en mémoire. Pour qu'il soit utile dans un ordinateur quantique, il est nécessaire de le coupler avec des particules matérielles, comme des atomes ou des électrons. Les centres NV du diamant sont ainsi une alternative très intéressante, leur spin constituant un qubit robuste et facile à adresser. L'optique quantique en cavité est également une approche prometteuse. Les phénomènes quantiques en jeu sont bien compris, qu'il s'agisse de l'intrication comme de la décohérence, faisant l'objet de démonstrations expérimentales d'une précision inégalée. L'optique quantique a toutefois encore du chemin à parcourir avant de rattraper les approches précédentes sur la route qui mène au QC. Enfin, les dispositifs à atomes neutres en réseaux optiques constituent une idée théorique intéressante, qui reste à explorer expérimentalement.

Les points forts et faibles des différentes approches expérimentales sont résumés dans le tableau suivant, qui reprend les 5 critères de DiVincenzo[185].

Approche	Calcul Quantique, Critères de DiVincenzo					Connectivité	
	#1	#2	#3	#4	#5	#6	#7
Supraconducteur	▲	▲	●	●	●	●	●
Semiconducteurs	●	●	●	●	●	▼	▼
RMN	●	●	●	▲	▼	▼	▼
Ions piégés	▲	▲	●	▲	●	●	●
Atomes neutres	▲	●	●	●	●	●	●
Optique quantique	▲	▲	●	●	●	●	●

▲ = l'approche est viable, en ayant suffisamment fait ses preuves expérimentales
● = l'approche est viable, mais plus de preuves expérimentales sont requises
▼ = aucune approche viable n'est connue pour l'instant

#1: Capacité d'initialiser les qubits dans un état bien défini
#2 : Capacité de mesurer les qubits avec fiabilité
#3 : Temps de décohérence suffisamment long (beaucoup plus long que le temps d'opération des portes quantiques)
#4 : Disposer d'un jeu universel de portes quantiques
#5 : Capacité d'accommoder un grand nombre de qubits

#6 : Capacité de convertir les qubits fixes en qubits mobiles
#7 : Capacité de transmettre efficacement les qubits mobiles entre plusieurs endroits

Il est certainement trop tôt pour prédire à quoi ressemblera le futur QC, et s'il dérivera ou non d'une des approches évoquées dans ce dossier. Il est très probable

que plusieurs de ces approches n'aboutiront jamais à des applications pratiques. En revanche, les recherches qui auront été menées auront certainement un rôle à jouer important dans l'avènement du QC, et seront à l'origine de résultats fascinants, qui auront peut être des conséquences physiques et des applications inattendues dans d'autres disciplines.

Sur ce sujet, la France dispose d'excellentes équipes de recherche, qui collaborent souvent avec leurs homologues américains, comme c'est le cas par exemple des groupes de Daniel Estève et Michel Devoret à Saclay et Yale. Favoriser ces collaborations est un des objectifs principaux de la Mission pour la Science et la Technologie de l'Ambassade de France aux Etats-Unis. En décembre 2007, elle a organisé une mission exploratoire sur l'électronique 'post-CMOS', lors de laquelle 5 experts français ont pu visiter plusieurs laboratoires américains d'exception, dont ceux de Yale, IBM Yorktown, Harvard, et HP reconnus pour leurs travaux en informatique quantique. Cette mission a donné lieu à un rapport détaillé[110] faisant le point sur la question, et à un nombre important d'échanges directs entre chercheurs desquels pourront germer de nouveaux partenariats.

XI. ANNEXE

XI.1. Le paradoxe EPR, vers une ébauche de processeur quantique

En 1935, le phénomène d'intrication a amené Einstein, Podolski et Rosen, à proposer une expérience de pensée qui violerait les lois de la relativité générale. La résolution de ce paradoxe, appelé EPR, est un résultat fondamental validant les concepts de mécanique quantique, et s'avère très utile pour comprendre les phénomènes impliqués en informatique quantique.

L'expérience de pensée se réduit en essence à une paire de particules intriquées (appelée à juste titre 'paire EPR'), par exemple $1/\sqrt{2}\left(|00\rangle+|11\rangle\right)$, émise par une source, et dont chacune des particules est envoyée séparément à deux destinataires éloignés Alice et Bob. Supposons qu'Alice mesure la particule qu'elle reçoit et trouve l'état $|0\rangle$. Alors la fonction d'onde de l'état intriqué se réduit instantanément à $|00\rangle$, et si Bob mesure l'état de sa particule, il mesurera à coup sûr $|0\rangle$. De même, si Alice mesure $|1\rangle$, Bob mesurera également $|1\rangle$ avec une probabilité de 100%. Il apparaît que si Alice et Bob sont suffisamment éloignés, ceci permettrait de communiquer à des vitesses supérieures à celle de la lumière. C'est le paradoxe EPR.

Pour résoudre ce paradoxe, Einstein, Podolski et Rosen ont suggéré que chacune des particules dispose de degrés de libertés internes qui permettraient de décrire complètement le résultat des mesures, mais qui seraient cachés aux observateurs à cause de notre connaissance imparfaite des lois de la physique. La théorie de ces 'variables cachées' résoudrait le paradoxe, mais porterait un coup à la mécanique quantique, qui ne serait plus qu'une théorie imparfaite utilisant des probabilités pour masquer notre incompréhension du monde.

L'argument a été étudié par le physicien Bell[186,187], qui a révélé une surprise. Supposons que les particules intriquées soient deux photons dans l'état $\left(|\uparrow\rangle|\downarrow\rangle-|\downarrow\rangle|\uparrow\rangle\right)/\sqrt{2}$, où $|\uparrow\rangle$ et $|\downarrow\rangle$ correspondent respectivement aux états de spin 'haut' et 'bas'. Supposons maintenant qu'Alice et Bob fassent leurs mesures le long de deux axes inclinés d'un angle respectivement ϕ_a et ϕ_b par rapport à la verticale. Selon la mécanique quantique, et en accord avec l'expérience, la probabilité de mesurer la même polarisation pour Alice et Bob est $\sin^2\left((\phi_a-\phi_b)/2\right)$. Mathématiquement, il n'y a cependant aucun moyen d'affecter aux deux photons des propriétés locales (c'est-à-dire à chacun des deux photons indépendamment), qui permette de retrouver ce résultat. Il faudrait par exemple que Alice et Bob puissent être certains de mesurer des polarisations opposées (haut et bas) pour $\phi_a=\phi_b$, et que la probabilité de mesurer le même spin soit de $\sin^2(60°)=3/4$ pour $\phi_a-\phi_b=120°$. Or Feynman a montré[188] que ceci est impossible avec une théorie de variables cachées, au grand maximum cette dernière atteignant la valeur 2/3. De manière plus générale, Bell montra que toute théorie de variables cachées prédisait que certaines mesures devaient satisfaire des inégalités, appelées inégalités de Bell.

Il restait à démontrer expérimentalement la violation de ces inégalités de Bell, ce qui fut fait en 1982 par le groupe d'Alain Aspect à l'université d'Orsay[189,190]. Certains groupes allèrent même au-delà, en considérant des systèmes plus complexes qui apportaient des arguments de plus en plus démonstratifs de cette violation. En particulier Greenberger, Horne et Zeilinger[191], préparèrent un système de trois spins dans l'état $\left(|\uparrow\uparrow\uparrow\rangle+|\downarrow\downarrow\downarrow\rangle\right)/\sqrt{2}$ et montrèrent qu'une mesure le long d'un axe horizontal pour deux particules, et le long d'un axe vertical pour la troisième, donnera avec certitude un résultat exactement opposé de celui que donnerait une théorie de variables cachées.

La violation des inégalités de Bell permet d'imaginer des processus physiques qui sont possibles grâce à la mécanique quantique, mais qu'aucun ordinateur classique ne pourrait résoudre. Par exemple, en reprenant l'argument de Feynman, avec plusieurs paires de photons intriqués A et B, et des axes de mesure orientés à 120°,

Alice et Bob sont capables de mesurer des états corrélés dans plus de 70% des cas, ce qui serait impossible en physique classique.

XI.2. Le théorème du non-clonage

Le théorème du non-clonage dit qu'un état quantique inconnu ne peut pas être cloné. En d'autres termes, il est impossible de générer des copies d'un état quantique, à moins que cet état ne soit déjà connu (à l'aide d'une information classique).

La preuve de ce théorème est due à Wootters et Zurek[192], c'est une simple conséquence de la linéarité et de l'aspect unitaire des transformations. Supposons qu'une transformation *U* unitaire soit capable de cloner les états quantiques, de telle sorte que $U|a_0\rangle = |aa\rangle$ pour tout état $|a\rangle$. Pour un état $|b\rangle$ orthogonal à $|a\rangle$, on a également $U|b_0\rangle = |bb\rangle$. Si on considère maintenant $|c\rangle = 1/\sqrt{2}\left(|a\rangle + |b\rangle\right)$, on a également $U|c_0\rangle = |cc\rangle$. Or, par linéarité on voit que :
$U|c_0\rangle = 1/\sqrt{2}\left(U|a_0\rangle + U|b_0\rangle\right) = 1/\sqrt{2}\left(|aa\rangle + |bb\rangle\right)$, ce qui n'est pas égal à $|cc\rangle$ comme on peut le vérifier aisément. Il y a une contradiction, et donc la transformation de clonage *U* n'existe pas.

Il est particulièrement intéressant de noter qu'en lien avec le paradoxe EPR, si le théorème de non-clonage n'était pas vérifié, il serait possible de communiquer plus vite que la lumière. Partant d'un état EPR transmis à Alice et Bob, Bob pourrait en effet utiliser le clonage pour créer plusieurs copies du qubit de la paire qu'il reçoit, et mesurer ces copies dans différentes bases, lui indiquant alors sans ambiguïté si son qubit se trouve dans la base $\left\{|\uparrow\rangle, |\downarrow\rangle\right\}$ ou dans la base $\left\{|\nearrow\rangle, |\nwarrow\rangle\right\}$ (dans le cas de photons intriqués). Alice pourrait alors communiquer avec Bob instantanément en forçant la paire EPR dans une base ou dans l'autre, simplement en mesurant son qubit dans la base souhaitée[193].

XI.3. Le codage super-dense, ou comment utiliser l'intrication comme source d'information

Comme nous allons le voir, des qubits peuvent être utilisés pour enregistrer et transmettre de l'information classique.

Afin de transmettre l'information classique 0101 (un exemple), Alice peut préparer 4 qubits dans l'état $|0101\rangle$ et les transmettre à Bob, qui mesurera chaque qubit dans la base $\left\{|0\rangle, |1\rangle\right\}$ et obtiendra avec une probabilité de 100% l'information classique 0101. Chaque qubit ne permet de communiquer qu'un seul bit classique, rien de bien nouveau.

Tout cela devient beaucoup plus intéressant si Alice et Bob sont chacun en possession d'un membre d'une paire de qubits intriqués EPR, dans l'état $\left(|00\rangle + |11\rangle\right)$ (en oubliant pour simplifier le facteur $\sqrt{2}$). Grâce à cette paire, Alice peut maintenant communiquer à Bob 2 bits classiques, en ne lui envoyant qu'un seul qubit. C'est ce qui s'appelle le codage super-dense. Notons ici que la paire EPR a pu être créée et stockée bien avant la communication souhaitée.

L'idée est due à Wiesner et Bennet des laboratoires IBM à Yorktown[194]. Elle tient au fait que les quatre états $|00\rangle + |11\rangle$, $|00\rangle - |11\rangle$, $|01\rangle + |10\rangle$ et $|01\rangle - |10\rangle$ sont mutuellement orthogonaux (ils forment la base dite de Bell) et peuvent tous être générés à partir du premier par simple application de l'une des transformations {*I, X, Y, Z*} sur un seul des qubits, par exemple celui dont dispose Alice. Il y a quatre possibilités, ce qui peut se coder par deux bits classiques (00, 01, 10 ou 11). Les deux bits classiques qu'Alice désire envoyer à Bob servent donc à choisir celle des transformations {*I, X, Y, Z*} qu'elle applique à son qubit membre de la paire $|00\rangle + |11\rangle$. Alice envoie alors ce qubit transformé à Bob, qui pour retrouver l'information classique doit déduire dans quel état de la base de Bell se trouve la paire EPR. Il lui applique d'abord la porte C_{not} et mesure le second qubit de l'état résultant, ce qui lui permet de distinguer entre $|00\rangle \pm |11\rangle$ et $|01\rangle \pm |10\rangle$. Bob applique ensuite l'opérateur de Hadamar *H* au qubit restant, ce qui lui permet de connaître le signe de la superposition. Au final, Bob est en mesure de savoir dans état de la base de Bell se trouve la paire intriquée, ce qui lui redonne l'information classique à deux bits qu'Alice souhaitait communiquer (pour plus de détails calculatoires, voir la ref.[1]).

Le codage super-dense est difficile à mettre en œuvre, et a donc peu d'utilité pratique comme moyen de communication. Il peut toutefois servir à établir une ligne de communication sécurisée entre Alice et Bob, car seule une personne en possession du deuxième qubit de la paire intriquée pourra accéder à l'information transmise par Alice. Une démonstration expérimentale du phénomène a été proposée par Mattle et al[195].

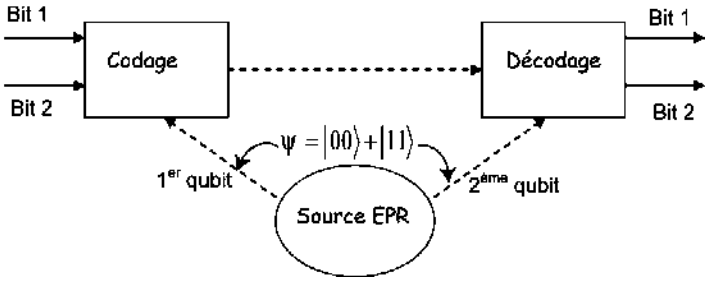


Figure 50: Schéma du protocole utilisé pour le codage super-dense. Alice reçoit deux bits classiques (flèche en trait plein), qu'elle envoie à Bob à l'aide d'un qubit d'une paire EPR (flèches en pointillé) qu'elle code et envoie à Bob. Bob décode le qubit à l'aide de portes quantiques élémentaires et en déduit les deux bits classiques d'Alice.

XI.4. La téléportation quantique

La téléportation quantique montre qu'il est possible de communiquer des qubits en ne transmettant que des bits classiques.

Ceci est loin d'être facile. Supposons en effet qu'Alice désire envoyer un qubit $|\phi\rangle$ à Bob. Si elle connaît son état (par exemple $|0\rangle$), elle peut dire à Bob par un canal classique : « le qubit est dans l'état $|0\rangle$ ». En revanche, si l'état de $|\phi\rangle$ est inconnu, ceci est impossible : Alice ne peut pas savoir sur quelle base mesurer $|\phi\rangle$, chaque mesure le modifie irrémédiablement, et elle ne peut pas le cloner. La seule manière simple de communiquer $|\phi\rangle$ est de l'envoyer physiquement.

La technique de téléportation, imaginée par Bennett des laboratoires IBM[196,197], permet de s'affranchir de l'envoi physique du qubit, et de communiquer son état à l'aide de bits classiques. Elle utilise, comme pour le codage super-dense, une paire EPR $\psi = |00\rangle + |11\rangle$, dont Alice et Bob disposent chacun d'un qubit (Alice le premier et Bob le dernier). Le qubit à transmettre peut s'écrire $|\phi\rangle = a|0\rangle + b|1\rangle$. Alice possède initialement les deux premiers qubits de l'état à 3 qubits : $\phi \otimes \psi = a|000\rangle + b|100\rangle + a|011\rangle + b|111\rangle$ dont elle mesure ses deux premiers qubits dans la base de Bell. Pour ce faire elle opère comme Bob dans le cas du codage super-dense, en appliquant successivement $C_{not} \otimes I$ puis $H \otimes I \otimes I$, après quoi l'état s'écrit :

$$|00\rangle(a|0\rangle + b|1\rangle) + |01\rangle(a|1\rangle + b|0\rangle) +$$
$$|10\rangle(a|0\rangle - b|1\rangle) + |11\rangle(a|1\rangle - b|0\rangle)$$

Alice mesure ensuite les deux premier qubits, ce qui lui donne $|00\rangle$, $|01\rangle$, $|10\rangle$ ou $|11\rangle$ avec égale probabilité. Ce résultat est communiqué à Bob sous forme de deux bits classiques. La mesure a également pour effet de projeter le qubit de Bob dans l'un des états $a|0\rangle + b|1\rangle$, $a|1\rangle + b|0\rangle$, $a|0\rangle - b|1\rangle$ ou $a|1\rangle - b|0\rangle$. Bob peut enfin retrouver le qubit initial $|\phi\rangle = a|0\rangle + b|1\rangle$ en appliquant à son qubit ainsi modifié l'une des opérations $\{I, X, Y, Z\}$, qu'il sait choisir pertinemment grâce à l'information classique des deux bits envoyés par Alice.

Les premières démonstrations expérimentales de la téléportation quantique datent de 1997. Elles utilisaient des photons comme qubits, plus faciles à manipuler que des atomes, mais beaucoup plus difficiles à faire interagir entre eux. Pour pallier ce problème, l'équipe de Francesco Martini à l'université La Sapienza de Rome, utilisait un seul photon comme qubit à téléporter et comme photon EPR (en codant sur deux variables indépendantes comme par exemple l'impulsion et la polarisation), ce qui évitait toute interaction à deux photons lors de la projection d'Alice sur les états de Bell[198]. Une démonstration plus propre est due au groupe d'Anton Zeilinger à l'époque à l'université d'Innsbruck[199], utilisant des photons UV polarisés, et en distinguant bien photon à téléporter et photon EPR. L'intrication était réalisée grâce à la conversion paramétrique d'un crystal non-linéaire, et l'analyse à l'aide de l'interférométrie à deux photons. Par la suite, en 2004, ce même groupe a réalisé la téléportation quantique à travers le Danube[200]. Les photons intriqués étaient envoyés sous le fleuve à l'aide d'une fibre optique, et le signal classique était envoyé par les airs. Du fait de la propagation plus lente des photons dans la fibre, ceci permettait au signal classique d'arriver à temps pour réaliser le décodage des qubits. Toutefois, bien que plus proches du schéma théorique de la téléportation quantique que l'expérience initiale de Martini, ces démonstrations étaient imparfaites car probabilistes, demandant une post-sélection des photons mesurés. C'était le prix à payer pour travailler avec des particules qui interagissent très peu entre elles. Seul le recours à des atomes devait permettre de résoudre ce problème.

La première téléportation quantique à l'aide d'atomes devait attendre 2004, avec deux publications dans le même numéro de la revue Nature, en provenance des groupes de David Wineland au NIST (Boulder, Colorado)[201], et de Rainer Blatt à l'université d'Innsbrück[202]. Les deux groupes utilisaient des techniques assez similaires, avec des pièges de Paul linéaires où des ions étaient piégés (voir chapitre VII). Le groupe d'Innsbrück utilisait trois ions $^{40}Ca^{+}$ séparés de 5µm, manipulés individuellement à l'aide de faisceaux lasers focalisés très précisément. Les manipulations impliquant plus d'un ion (intrication, mesures de Bell) se faisaient au travers des modes de vibration du centre de masse des ions. Le groupe du NIST utilisait des ions $^{9}Be^{+}$ confinés dans un piège linéaire segmenté, ce qui permettait de les manipuler plus facilement et de ne pas avoir recours aux vibrations des centres de masse (voir

paragraphe VII.5). Des potentiels électriques permettaient de faire passer les ions d'un segment à l'autre, et deux lasers étaient utilisés pour implémenter les rotations des qubits. Les deux groupes atteignirent ainsi des fidélités supérieures à 70% dans le protocole de téléportation (78% dans l'expérience de Wineland). On rappelle ici qu'une fidélité supérieure à 2/3 est la preuve que l'intrication est nécessaire au processus de téléportation[188], et que ce dernier ne peut pas s'expliquer à l'aide de variables locales (voir Annexe XI.1).

Ces deux expériences de téléportation utilisant des ions sont d'une importance fondamentale. D'une part elles prouvent expérimentalement la validité du protocole de téléportation sans avoir recours à un traitement post-sélection comme c'est le cas avec les photons. Elles montrent également que la téléportation fonctionne avec de la matière, ce qui permet de préparer à l'avance des paires intriquées et de les conserver. La téléportation peut alors se faire par envoi d'information classique, typiquement à la vitesse de la lumière, et sans envoi de matière, ce qui correspond assez bien à l'image intuitive que l'on se fait d'un processus de téléportation. Enfin, ces expériences sont parmi les premières à mettre en œuvre les techniques efficaces de piégeage d'ions qui sont parmi les plus prometteuses dans la construction des futurs ordinateurs quantiques, comme on le voit dans le chapitreVII.

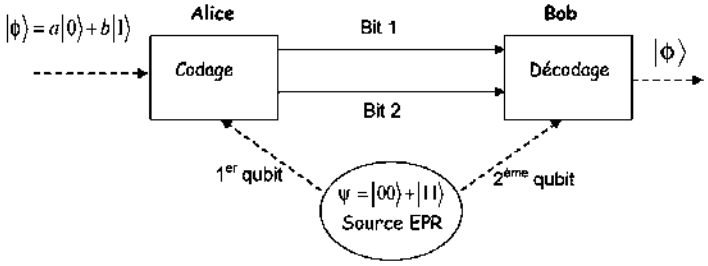


Figure 51: Schéma du protocole utilisé pour la téléportation quantique. Alice désire envoyer à Bob un qubit dont l'état lui est inconnu. Tous les deux disposent d'un état intriqué EPR. Alice utilise une combinaison du qubit inconnu et de son qubit EPR, sur laquelle elle fait agir plusieurs portes quantiques puis en mesure le résultat. Cette mesure a pour effet de transformer le qubit EPR de Bob, et de donner deux bits classiques qu'Alice envoie à Bob par un canal classique. A l'aide de ces deux bits, Bob applique une porte quantique élémentaire à son qubit EPR, ce qui lui redonne l'état du qubit inconnu.

XI.5. La cryptographie quantique

Dans cette revue des principaux concepts utilisés en théorie de l'information quantique, il est difficile de ne pas parler de cryptographie quantique, bien que cette dernière ne fasse pas intervenir directement de transformations d'état (portes quantiques) comme c'est le cas dans les annexes précédentes. La cryptographie quantique vise à permettre à Alice et Bob de communiquer de façon sûre, malgré l'indiscrétion de l'espion Eve. Elle a été introduite pour la première fois par Stephen Wiesner de l'université Columbia au début des années 70, puis reprise 10 ans plus tard par Charles Bennett des laboratoires IBM à Yorktown et Gilles Brassard de l'université de Montréal, et enfin en 1990 par Artur Ekert de l'université d'Oxford.

Nous reprenons ici le protocole d'échange d'une clé quantique développé par Bennett et Brassard en 1984, et appelé à juste titre BB84[203]. Supposons qu'Alice et Bob veuillent convenir d'une clé secrète qui leur permette de crypter leurs messages. Ils communiquent à l'aide d'un canal classique ainsi qu'un canal quantique (par exemple une fibre optique), les deux pouvant être espionnés par Eve, qui reçoit les bits ou qubits (en l'occurrence des photons polarisés) émis par Alice et qu'elle ré-émet à Bob. Comme on peut déjà l'imaginer, ceci est plus facile à réaliser pour les bits classiques que pour les qubits.

Pour chaque qubit envoyé, Alice choisit aléatoirement une des deux bases de polarisation $\{|\uparrow\rangle, |\downarrow\rangle\}$ ou $\{|\nearrow\rangle, |\nwarrow\rangle\}$. Bob mesure les photons qu'il reçoit en choisissant lui aussi une des deux bases aléatoirement. Après que tous les photons aient été transmis, Alice et Bob communiquent sur le canal classique les bases qu'ils ont utilisées. En moyenne ils auront choisi la même base dans 50% des cas. Ils conservent les résultats des mesures correspondant à ces cas, et rejettent les autres. Ces résultats de mesure constituent la clé quantique.

Supposons maintenant qu'Eve mesure l'état des photons transmis et renvoie vers Bob de nouveaux photons avec l'état de polarisation qui aura été mesuré. Elle se trompera de base la moitié du temps, auquel cas elle renverra le photon avec la mauvaise base, et Bob finira par mesurer le mauvais résultat dans 50%*50%=25% des cas. Il suffit alors qu'Alice et Bob communiquent en clair une partie de leur clé quantique pour ce rendre compte de l'espionnage : dans ce cas, environ 25% des résultats de mesure ne seront pas identiques. En revanche, si tous les résultats de mesure sont identiques, supposons qu'il y en ait *n*, la probabilité d'espionnage tombe à $(3/4)^n \simeq 10^{-125}$ pour *n*=500.

Le protocole de cryptage quantique développé par Ekert[204] utilise une autre approche que celle de Bennett et Brassard, impliquant l'utilisation de paires EPR, qu'Alice et Bob mesurent le long de trois axes différents. Afin de prévenir les attaques d'Eve, ils vérifient les corrélations de Bell-EPR dans leurs résultats.

Plusieurs expériences ont vérifié le concept de cryptographie quantique, depuis l'expérience pionnière de Bennett et Brassard[205] qui en a démontré le principe. En 1997, une équipe suisse parvenait à échanger des clés

quantiques sur une distance de 23km sous le lac Léman[206]. En juin 2006, une équipe du NIST à Los Alamos est parvenue à envoyer une clé quantique à travers 148.7 km de fibre optique, en utilisant le protocole BB84, constituant ainsi le record de distance à travers une fibre optique[207]. Sans l'aide d'une fibre optique cette fois, une équipe européenne dirigée par A. Zeilinger est parvenue en 2006 à transmettre une clé quantique entre deux pics des îles Canaries séparés d'une distance de 144km[208,209]. Cette expérience suggère que la transmission de clé quantique vers des satellites est à la portée des technologies actuelles. Le projet QUEST (Quantum Entanglement in Space Experiments) mené par A. Zeilinger, vise à établir des communications quantiques basées sur l'intrication entre la station spatiale internationale et le sol[210].

Il y a actuellement trois compagnies qui proposent des systèmes de cryptographie quantique : id Quantique (Geneve), MagiQ Technologies (New York) et SmartQuantum (France).

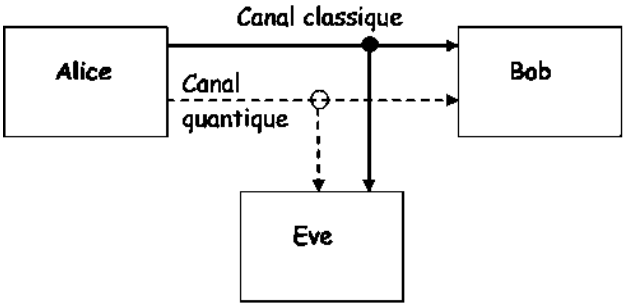


Figure 52 Principe de fonctionnement de la cryptographie quantique. Alice envoie à Bob, via un canal quantique, des qubits préparés aléatoirement dans deux bases différentes. Elle communique ensuite, via un canal classique, les bases utilisées. Les qubits mesurés par Bob selon les bonnes bases constituent la clé quantique. Eve ne peut pas espionner la transmission sans induire un taux élevé d'erreurs dans les mesures de Bob, ce qui peut se détecter.

XI.6. Les portes quantiques fondamentales

Les portes quantiques élémentaires les plus simples et les plus fondamentales sont les quatre transformations ***{I, X, Y, Z}*** **:**

$I : |0\rangle \to |0\rangle, |1\rangle \to |1\rangle$ n'est autre que l'identité,

$X : |0\rangle \to |1\rangle, |1\rangle \to |0\rangle$ est l'inversion appelée NOT,

$Y : |0\rangle \to -|1\rangle, |1\rangle \to |0\rangle$ est une combinaison de *X* et *Z*,

$Z : |0\rangle \to |0\rangle, |1\rangle \to -|1\rangle$ est un changement de phase.

La transformation de **Hadamard**

$H : |0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ joue un rôle fondamental dans plusieurs algorithmes quantiques. Lorsqu'elle est appliquée sur *n* qubits en parallèle, elle permet de générer une superposition de tous les états possibles, qui peuvent être vus comme une représentation binaire des nombres de 0 à 2^n-1 :

$$(H \otimes H \otimes ... \otimes H)|00...0\rangle$$

$$= \frac{1}{\sqrt{2^n}}\left((|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes ... \otimes (|0\rangle + |1\rangle)\right)$$

$$= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n - 1} |x\rangle$$

Cette transformation, qui s'applique aux *n* qubits, est appelée transformation de **Walsh-Hadamard**. Elle est très souvent utilisée au tout début de plusieurs des principaux algorithmes quantiques (Shor, Grover), pour permettre au reste de l'algorithme de pouvoir être effectué en parallèle sur tous les entiers possibles envisagés par le calcul. Cette transformation donne à ces algorithmes la puissance de parallélisme du calcul quantique.

La porte de **Toffoli** (*T*) est la porte Controled-Controled-NOT. Elle agit sur 3 qubits en inversant le troisième si et seulement si les deux autres sont dans l'état $|1\rangle$, ce qui peut s'écrire :

$$|0\rangle \otimes |a,b\rangle \to |0\rangle \otimes |a,b\rangle \text{ et } |1\rangle \otimes |a,b\rangle \to |1\rangle \otimes C_{not}(|a,b\rangle)$$

La porte de Toffoli à trois qubits permet d'engendrer la porte à un qubit NOT et la porte à deux qubits AND (ET). En effet, $T(|1,1,a\rangle) = T(|1,1,-a\rangle)$ ainsi que $T(|a,b,0\rangle) = T(|a,b,a \wedge b\rangle)$, où les notations $|-a\rangle$ et $|a \wedge b\rangle$ correspondent à $NOT(|a\rangle)$ et $AND(|a,b\rangle)$. En d'autres termes, la porte de Toffoli agit sur le troisième qubit $|0\rangle$ pour donner le AND des deux premiers qubits. L'utilisation de 3 qubits est nécessaire pour que l'opération soit unitaire, c'est la seule manière d'autoriser l'opération AND dans le monde du calcul quantique.

Avec les portes NOT et AND on montre qu'il est possible d'engendrer toutes les portes logiques. La porte de Toffoli est ainsi dite 'complète' pour la combinatoire des circuits.

Une autre porte 'complète' pour la combinatoire, est la porte de **Fredkin**, dite aussi 'controlled swap'. La porte d'échange SWAP est donnée d'abord par : $SWAP(|a,b\rangle) = (|b,a\rangle)$.

La porte de Fredkin, notée *F* est alors donnée par :

$F(|0,a,b\rangle) = |0,a,b\rangle$ et $F(|1,a,b\rangle) = |1,b,a\rangle$.

En d'autres termes *F* donne SWAP des deux dernier qubits si le premier qubit est 1, sinon elle les laisse inchangés.

XI.7. Machine de Turing

Le concept de « machine universelle » date des travaux de Church[211] et Turing[212] dans les années 1936. En termes mathématiques, cela s'écrit : $U(d[T],x)=T(x)$, où x est une suite quelconque de bits (input), *T(x)* est le résultat du calcul de la machine de Turing *T* sur *x* (output), *d[T]* est la description de la machine *T* en termes de bits (comment *T* répond aux bits de *x*), et *U* est une machine de Turing universelle. Il est important de noter qu'une machine de Turing universelle n'engendre pas de ralentissement exponentiel : le nombre d'étapes utilisées par *U* pour simuler chaque étape de *T* n'est que polynomial par rapport à la taille de *d[T]*. Ce théorème, démontré par Turing, a donné lieu à un principe (ou thèse), qui lui n'a pour l'instant pas été prouvé, et qui stipule que « toute fonction qui peut être perçue comme calculable peut être calculée sur une machine universelle de Turing ».

XI.8. Les classes de Complexité

La difficulté des tâches effectuées par un ordinateur peut être classée par le concept de 'complexité'. La complexité d'un problème est déterminée par le nombre d'étapes *s* qu'une machine de Turing doit effectuer pour résoudre le problème à l'aide d'une méthode algorithmique. Dans le modèle de réseau classique utilisé dans les microprocesseurs actuels, la complexité est déterminée par le nombre de portes logiques requises. La quantité d'information nécessaire pour spécifier le problème étant notée *L*, si *s* est une fonction polynomiale de *L*, alors on dit que le problème est de classe '*P*'. Si *s* croit de façon exponentielle avec *L*, le problème est dit '*difficile*', et n'appartient pas à la classe *P*. La classe '*NP*' est définie comme étant celle des problèmes pour lesquels une solution peut être vérifiée en temps polynomial. De toute évidence $P \subset NP$, mais on n'a pas forcément *P=NP*. On pense même plutôt que $P \neq NP$, même si personne n'a pour l'instant été capable de le démontrer. La démonstration de cette inégalité (ou de l'égalité) fait partie des 7 'Millenium Problems' et serait récompensée par le 'Clay Mathematics Institute of Cambridge' du fameux prix d'un million de dollars.

Il existe une classe supplémentaire de problèmes, dits '*NP complets*'. Il s'agit de problèmes dont une solution efficace apporterait une solution efficace à tous les autres problèmes *NP*. Dans cette classe se trouve par exemple le problème de coloriage d'une carte avec seulement 3 couleurs. Aucun algorithme n'a pour l'instant été trouvé, permettant de résoudre efficacement (en temps polynomial) un tel problème *NP complet*. Si c'était le cas, ces différentes classes n'existeraient plus, car tout problème *NP* (et *NP complet*) serait ramené à un problème *P*, et on aurait résolu *P=NP*. Cela fait 50 ans que certains des meilleurs mathématiciens cherchent un tel algorithme, et le fait qu'ils n'aient rien trouvé incite à penser que $P \neq NP$.

XI.9. L'algorithme RSA

Le problème mathématique de la factorisation en nombres premiers est d'une grande importance pratique, car il est au cœur de la plupart des systèmes de cryptographie, comme celui mis au point par Rivest, Shamir et Adleman (RSA) en 1979[213]. Etant donné un message *M,* sous forme d'un long nombre binaire, il est facile de calculer sa version encryptée $E = M^S \bmod c$, où *s* et *c* sont de grands nombres entiers choisis avec soin, et qui peuvent être rendus publics. Pour décrypter le message, le destinataire calcule $E^t \bmod c$, qui est égal à *M* pour une valeur de *t* que l'on peut déduire facilement de *s* et des facteurs premiers de *c*. Le destinataire connaît ces facteurs premiers, notés *c=pq*, qui sont en pratique de grands nombres premiers, et il est ainsi le seul à pouvoir décrypter le message, à moins que quelqu'un ne parvienne à factoriser *c*. En revanche, la clé publique (*c,*s) est connue de tous, et permet d'encrypter les messages à volonté, mais pas de les décrypter.

XI.10. L'algorithme de Grover

L'algorithme quantique de Grover permet de chercher un élément x_0 dans une liste non-structurée$\{x\}$ de taille *N*. Soit *n* le plus petit entier tel que $N \leq 2^n$ éléments, et *P(x)* la fonction de test classique: $P(x)=0$ sauf si $x=x_0$, auquel cas $P(x_0)=0$. L'algorithme commence par utiliser la transformation de Walsh-Hadamart donnant la superposition : $1/\sqrt{2^n}\sum_{x=0}^{n-1}|x\rangle$. Il applique ensuite la porte quantique implémentant *P* à cette superposition, donnant la superposition : $1/\sqrt{2^n}\sum_{x=0}^{n-1}|x,P(x)\rangle$. L'objectif est d'extraire de cette superposition l'élément $|x_0,1\rangle$ pour lequel que $P(x_0)=1$. Comme l'amplitude de cet élément est de $1/\sqrt{2^n}$, une mesure directe de la superposition le révèlera avec une probabilité de seulement 2^{-n}. L'idée de l'algorithme de Grover est alors de modifier la superposition à l'aide de transformations unitaires, afin d'augmenter l'amplitude de l'élément $|x_0,1\rangle$ et de décroître celle des autres $|x,0\rangle$. Une fois que cette transformation a été effectuée, il suffit de mesurer le dernier qubit de la superposition, qui représente *P(x)*. La probabilité de mesurer 1 est alors nettement augmentée, et l'état est projeté sur l'état $|x_0,1\rangle$. La mesure du premier qubit donne alors x_0. Si, en revanche, la mesure de *P(x)* donne 0, alors il faut recommencer l'algorithme au début.

Les transformations unitaires utilisées dans l'algorithme pour augmenter l'amplitude de $|x_0,1\rangle$ sont des inversions quantiques. La première transformation inverse le signe de cette amplitude a_0 en $-a_0$, et ne touche

pas aux autres. La deuxième transformation fait une inversion des amplitudes par rapport à leur valeur moyenne, ce qui a pour effet (dans un premier temps) de doubler l'amplitude a_0 et de ne modifier que le signe des autres. Ces deux inversions sont répétées $\frac{\pi}{4}\sqrt{2^n}$ fois.

Après $\frac{\pi}{8}\sqrt{2^n}$ itérations, le taux d'échec de l'algorithme est de 0.5. Il passe à 2^{-n} au bout de $\frac{\pi}{4}\sqrt{2^n}$ itérations, et retombe à presque 1 après $\frac{\pi}{2}\sqrt{2^n}$ itérations. Ce résultat, bien qu'il puisse paraître surprenant, est en fait assez caractéristique des algorithmes quantiques. Il faut essayer de se représenter ces derniers comme des successions de transformations unitaires, c'est-à-dire des rotations dans un espace complexe. Si l'application répétée de ces rotations permet, dans un premier temps, de rapprocher l'algorithme de l'élément rechercher, elle finit par l'en éloigner si le nombre d'applications est trop grand. Pour qu'un algorithme quantique soit efficace, il faut savoir s'arrêter au bon moment.

XI.11. La jonction Josephson

Tous les circuits quantiques envisagés dans le chapitre III sont basés sur des structures supraconductrices utilisant une ou plusieurs jonctions Josephson. Une jonction Josephson est une structure constituée par deux électrodes supraconductrices, typiquement en Aluminium, séparées par une fine couche (~1nm) de diélectrique isolant faisant office de barrière tunnel (voir figure suivante). Elle joue un rôle fondamental en physique des circuits supraconducteurs à cause de ses propriétés non-linéaires inhabituelles, dues au comportement macroscopique particulier des paires de Cooper.

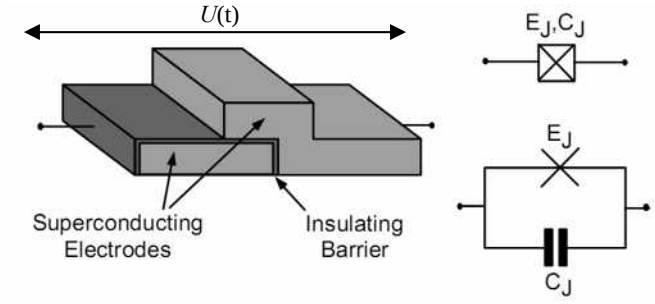


Figure 53 Schéma de principe d'une jonction Josephson, et schéma électrique équivalent. Tiré de la thèse de Audrey Cottet, groupe Quantronique, CEA.

Les équations de base régissant le fonctionnement d'une jonction Josephson sont :

$$U(t) = \frac{\hbar}{2e}\frac{\partial \delta}{\partial t}$$

$$I(t) = I_C \sin\delta(t)$$

où $U(t)$ est la tension aux bornes de la jonction, $I(t)$ est le courant la traversant, I_C est le courant critique de la jonction (le supercourant maximum) et $\delta(t) = (\varphi_2 - \varphi_1)$ est la différence de phase (paramètre d'ordre de Ginzburg-Landau) entre les deux matériaux supraconducteurs. Ce dernier paramètre est utilisé dans beaucoup d'expériences comme variable quantique principale des qubits supraconducteurs.

On distingue deux régimes : si la tension U est nulle, on voit que δ est constant, ainsi que le courant qui est donné par $I = I_C \sin\delta$. C'est le régime appelé DC, la jonction Josephson se comporte comme un court circuit. Si la tension n'est pas nulle, le courant oscille alternativement selon la formule : $I(t) = I_C \sin\left(\frac{2\pi}{\Phi_0}Ut\right)$, où $\Phi_0 = h/2e$ est le quantum de flux magnétique. Il s'agit du régime appelé AC, la jonction Josephson se comporte comme un oscillateur idéal contrôlé en tension, ou si on préfère, comme un convertisseur tension-fréquence. Schématiquement, ce comportement dérive directement de la différence de niveau d'énergie des paires de Cooper de part et d'autre de la jonction, $\Delta E = -2eU$, liée à la relation quantique fondamentale $\Delta E = h\nu$, donnant ainsi la fréquence de couplage $\nu = U/\Phi_0$ du système.

L'énergie de couplage de la jonction Josephson est donnée par $W_J = E_J(1-\cos\delta)$, où l'énergie de la jonction E_J est liée au courant critique par $I_C = (2e/\hbar)E_J$ et est proportionnelle au gap des supraconducteurs divisé par la résistance tunnel dans l'état normal de la jonction.

XI.12. Le SQUID

Un SQUID (Superconducting Quantum Interference Device) est une boucle supraconductrice, dont la propriété principale est de quantifier le flux magnétique. Nous décrivons d'abord le SQUID a une jonction Josephson, qui possède la géométrie la plus simple, et qui est également à la base de nombreux dispositifs en informatique quantique, comme par exemple, le qubit de phase.

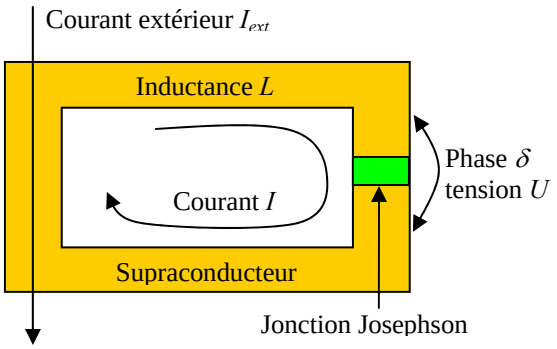


Figure 54 Schéma de principe d'un SQUID à une jonction Josephson, qui est le plus simple circuit quantique à flux.

En utilisant les notations de la figure ci-dessus, les équations de base de la jonction Josephson donnent $U = \frac{\Phi_0}{2\pi}\frac{\partial\delta}{\partial t}$. Or, la loi de l'induction magnétique de Faraday nous dit que : $U = d\Phi/dt$, où Φ est le flux magnétique pénétrant la boucle. Ainsi en intégrant les deux équations on obtient : $\delta = 2\pi\frac{\Phi}{\Phi_0}$, et comme le SQUID est un circuit fermé, bouclé sur lui-même, les phases ϕ_1 et ϕ_2 de part et d'autre de la jonction doivent être égales à un facteur $2\pi n$ près, n étant un entier. Ceci nous donne la loi bien connue donnant la quantification du flux magnétique dans un SQUID : $\Phi = n\Phi_0$

Si maintenant on note Φ_{ext} le flux magnétique crée par le courant extérieur I_{ext}, suivant les notations de la figure, on a : $\Phi = \Phi_{ext} - LI$. Or le courant parcourant la jonction Josephson vaut : $I = I_C \sin\delta$, et avec la relation ci-dessus reliant δ et Φ, on obtient : $\delta + l\sin(\delta) = \delta_{ext}$,où $l = 2\pi LI_C/\Phi_0$ et $\delta_{ext} = 2\pi\Phi_{ext}/\Phi_0$. Selon la valeur du paramètre l, cette équation peut admettre plusieurs solutions. Typiquement, pour un SQUID, $l \approx 1$, et il y a deux solutions stables.

En fixant le flux magnétique extérieur à $\Phi_{ext} = \Phi_0/2$, on peut voir facilement que les deux états seront symétriques, auront le même δ, et donc même flux Φ. En représentant l'énergie du système en fonction de δ_{ext}, on verrait que cette dernière possède deux minima symétriques en 0 et 1, séparés par une barrière de potentiel maximale en ½, à travers laquelle le flux du SQUID peut passer par effet tunnel. Ceci implique que l'état fondamental du SQUID est dégénéré, comportant deux états mixtes séparés par une différence d'énergie ΔE, qui est liée à l'élément de matrice de l'effet tunnel. Finalement, si la cohérence du système peut être maintenue suffisamment longtemps, le flux magnétique oscillera entre les deux états avec la fréquence $\Delta E/2\pi h$.

Dans cet état fondamental dégénéré, le système est dans une superposition quantique de deux états, que l'on appelle cohérence quantique macroscopique (MQC), car il fait intervenir le mouvement macroscopique de milliards d'électrons. La MQC a été démontrée expérimentalement en 2003 par le groupe de Mooij à l'université de Delft, après que de nombreux groupes aient passé une vingtaine d'années en tentatives infructueuses (voir paragraphe III-5 sur les qubits de flux).

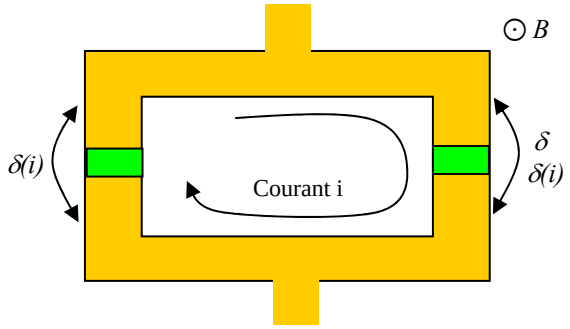


Figure 55 Schéma de principe d'un SQUID à deux jonctions Josephson, utilisé pour les applications de magnétométrie.

Comme expliqué dans le paragraphe III.5 consacré aux qubits de phase, la géométrie de SQUID à une jonction Josephson permet de construire un certain nombre de dispositifs intéressants pour le calcul quantique. Pourtant, la plupart des SQUIDs comportent 2 voire 3 jonctions Josephsons, comme c'est le cas pour le Quantronium, le Transmon et les qubits de flux.

Un SQUID à deux jonctions Josephson (voir figure ci-dessus) fonctionne sur le même principe qu'un SQUID à une jonction. La condition quantique de bouclage de phase est la même, et en ré-écrivant les équations ci-dessus un peu différemment, on obtient : $\delta + 2\delta(i) = 2\pi n$, où $\delta = 2\pi\Phi/\Phi_0$ est toujours la différence de phase part et d'autre d'une jonction causée par le flux magnétique, et $\delta(i)$ est la différence de phase de part et d'autre de chaque jonction causée par le passage du courant i. Lorsque le champ magnétique extérieur B augmente, il en va de même du flux Φ. Via le terme $\delta(i)$, le courant circulant à l'intérieur de la boucle du SQUID doit alors varier pour compenser les variations de δ. Quand c'est possible, il est énergétiquement plus favorable que ce courant circule dans la direction inverse de celle qui augmenterait le flux magnétique. Tous les $\Phi_0/2$, la situation énergétique s'inverse, et le courant change de sens. De manière générale, ce courant est donné par l'expression $i = I_C \sin\left(\frac{\Phi}{\Phi_0}\right)$. Ce comportement peut être attribué à l'interférence des électrons parcourant les deux branches du SQUID.

En résumé, lorsque le champ magnétique extérieur augmente, le courant circulant dans la boucle du SQUID varie en conséquence, avec une périodicité connue. La détection de ce courant permet d'utiliser le SQUID comme un magnétomètre ultra-sensible. Dans ce cas, le SQUID à deux jonctions est qualifié de 'SQUID DC', en référence au courant continu qui circule dans sa boucle. Un SQUID à une jonction peut également être utilisé pour des applications de magnétométrie, en utilisant un courant extérieur RF. Il est alors qualifié de 'SQUID RF', mais il est généralement moins sensible que le SQUID DC à deux jonctions.

En dehors de l'informatique quantique, une des applications les plus prometteuses du SQUID comme magnétomètre concerne la magnéto-encéphalographie utilisant des champs magnétiques extrêmement faibles. En particulier, une équipe du Los Alamos National Laboratory[214] a réalisé récemment une machine d'imagerie à résonance magnétique (IRM) fonctionnant à 46 microteslas (μT), soit à peu près la même intensité de champ magnétique que le champ magnétique terrestre, au lieu de 1.5T pour les machines habituelles. Le faible signal émis par les tissus est détecté par un réseau de SQUIDs. L'intérêt de la machine est d'être beaucoup moins invasive qu'une machine IRM standard, et de couter également beaucoup moins cher, environ $100,000 au lieu de $1,000,000.

XII. REFERENCES

[1] A. Steane, '*Quantum computing*', Reports on Progress in Physics **61**, 2, 117-173 http://xxx.lanl.gov/abs/quant-ph/9708022 (1998)

[2] E. Rieffel and W. Polak, '*An introduction to Quantum Computing for non-physicists*', FX Palo Alto Lab. Report http://arxiv.org/abs/quant-ph/9809016v2 (2000)

[3] Schumacher Quantum Coding, Phys. Rev. A **51**, 2738-2747 (1995)

[4] A. Ekert and R. Jozsa, '*Quantum computation and Shor's factoring algorithm*', Rev. Mod. Phys. **68**, 733 (1996)

[5] T. P. Spiller, '*Quantum information processing : cryptography, computation and teleportation*', Proc. IEEE **84**, 1719 (1996)

[6] D. DiVincenzo, '*Quantum Computation*', Science **270**, 255 (1995)

[7] D. Deutsch, 'Quantum computational networks', Proc. Roy. Soc. Lond. A **425** 73-90 (1989)

[8] D. P. DiVincenzo, in Mesoscopic Electron Transport, eds. Sohn, Kowenhoven, Schoen (Kluwer 1997), p. 657, cond-mat/9612126; "*The Physical Implementation of Quantum Computation*," Fort. der Physik **48**, 771 (2000), http://arxiv.org/PS_cache/quant-ph/pdf/0002/0002077v3.pdf

[9] D. Deutsch, '*Quantum Theory, the Church-Turing principle and the universal quantum computer*', Proc. Roy. Soc. Lond. A **400** 97-117 (1985)

[10] A. Barenco, '*A universal two-bit gate for quantum computation*', Proc. R. Soc. Lond. A **449**, 679-683 (1995)

[11] S. Loyd '*Almost any quantum logic gate is universal*', Phys. Rev. Lett. **75**, 346-349 (1995)

[12] D. DiVincenzo '*Two-bit gates are universal for quantum computation*', Phys. Rev. A **51**, 1015-1022 (1995)

[13] S. Lloyd, '*Universal quantum simulators*', Science **273,** 1073-1078 (1996)

[14] D. Deutsch, '*The Church-Turing principle and the universal quantum computer*', *Proceedings of the Royal Society of London A* **400**, 97 (1985) PDF

[15] D. Deutsch and R. Jozsa, '*Rapid solutions of problems by quantum computation*'. *Proceedings of the Royal Society of London A* **439** 553 (1992)

[16] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca '*Quantum algorithms revisited', Proceedings of the Royal Society of London A* **454**: 339-354 (1998) http://arxiv.org/pdf/quant-ph/9708016

[17] M. E. Hellman, '*The mathematics of public key cryptography*', Scientific American **241**, August 130-139 (1979)

[18] A. J. Menezes, P. C. van Oorschot, and S. Vanstone, '*Handbook of applied cryptography*', CRC Press, Boca Raton (1997)

[19] D. R. Simon, '*On the power of quantum computation*', Proceedings of the 35th Annual Symposium on Foundations of Computer Science (Nov 1994), pp. 124-134 IEEE Computer Society Press. (1994)

[20] P. W. Shor, '*Algorithms for quantum computation : Discrete log and factoring*', in Proceedings of the 35th Annual Symposium on Foundations of Computer Science (Nov 1994), pp. 124-134 IEEE Computer Society Press. (1994)

[21] P. W. Shor, '*Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*', Soc. for Industrial and Appl. Math. Journal on Computing **26**, 5, 1484-1509 (1997)

[22] P. W. Shor, '*Polynomial-Time algorithms for prime factorization and discrete logarithms on a quantum computer*', SIAM Review, **41**, 2 303-332 (1999)

[23] G. H. Hardy and E. M. Wright, '*An introduction to the theory of numbers*' Clarendon Press, Oxford (1979)

[24] C. Miquel, J. P. Paz and Perazzo, '*Factoring in a dissipative quantum computer*', Phys. Rev. A **54** 2605-2613 (1996)

[25] V. Vedral, A. Barenco and A. Ekert, '*Quantum networks for elementary arithmetic operations*', Phys. Rev. A **54** 147-153 (1996)

[26] D. Beckman, A. Chari, S. Devabhaktuni, and J. Preskill, '*Efficient networks for quantum factoring*', Phys. Rev. A **54**, 1034-1063 (1996)

[27] D. Beckman , A. N. Chari, S. Devabhaktuni, and J. Preskill, '*Efficient networks for quantum factoring*', Phys. Rev. A **54**, 1034–1063 (1996)

[28] L. K. Grover, '*Quantum mechanics helps in searching for a needle in a haystack*', Phys. Rev. Lett. **79**, 325-328 (1997)

[29] C. H. Bennett, E. Bernstein, G. Brassard, U. Vazirami, '*Strengths and weaknesses of quantum computing*', SIAM Journal of Comp. **26**, 5, 1515-1523 (1997)

[30] G. Brassard, '*Searching a quantum phone book*', Science **275**, 627-628 (1997)

[31] S. Haroche and J-M Raymond, '*Quantum computing: dream or nightmare*', Phys. Today August 130-139 (1996)

[32] A. M. Steane, '*Multiple particle interference and quantum error correction*', Proc. Roy. Soc. Lond. A **452**, 2551-2577 (1996)
[33] A. R. Calderbank and P. W. Shor, '*Good quantum error-correcting codes exist*', Phys. Rev. A **54**, 1098-1105 (1996)
[34] C. H. Bennett,et al. '*Purification of noisy entanglement and faithful teleportation via noisy channels*', Phys. Rev. Lett. **76**, 722-725 (1996)
[35] D. Deutsch et al. '*Quantum privacy amplification and the security of quantum cryptography over noisy channels*', Phys. Rev. Lett. **77** 2818 (1996)
[36] P. W. Shor, '*Fault tolerant quantum computation*', in Proc. 37th Symp. on Foundations of Computer Science, IEEE Comp. Soc. Press, 56-65 http://arxiv.org/abs/quant-ph/9605011 (1996)
[37] J. Preskill, '*Reliable quantum computers*', Proc.Roy.Soc.Lond. A454 385-410 http://arxiv.org/abs/quant-ph/9705031 (1998)
[38] M. Nielsen and I. Chuang, '*Quantum computation and quantum information*', Cambridge Univ. Press ISBN 0-521-63503-9 (2000)
[39] S. Aaronson, '*The limits of Quantum Computers*', Scientific American, March, 63-69 (2008)
[40] W. M. Kaminski, and S. Lloyd, '*Scalable Architecture for Adiabatic Quantum Computing of NP-Hard Problems'*, Extension of presentation at MQC2 Conference (Napoli, June 2002), http://arxiv.org/abs/quant-ph/0211152
[41] A. deVries, '*A fast quantum search algorithm by controlled measurement and qubit comparison implying the complexity class inclusion NP in BQP'*, http://arxiv.org/abs/quant-ph/0506137 withdrawn (2006)
[42] A. M. Zagonski, S. Savel'ev, and F. Nori, '*Modeling an Adiabatic Quantum computer via an exact map to a gas of particle*s', Phys. Rev. Lett. **98**, 120503 (2007)
[43] J. Timmer, '*A detour into the strange world of quantum computing*', http://arstechnica.com/news.ars/post/20070212-8818.html (February 2007)
[44] C. Lee, '*Using gas to understand adiabatic quantum computing*', http://origin.arstechnica.com/journals/science.ars/2007/03/29/using-a-gas-to-understand-adiabatic-quantum-computing (March,2007)
[45] Tiré de : Grégoire Ithier, '*Manipulation, lecture et analyse de la décohérence d'un bit quantique supraconducteur*', PhD thesis, Université Paris VI, http://www-drecam.cea.fr/drecam/spec/Pres/Quantro/, (2005)
[46] Makhlin Y, Schön G, Shnirman A, '*Quantum-state engineering with Josephson-junction devices',* Rev. Mod. Phys. **73**, 357, (2001)
[47] Audrey Cottet, quantronics group, '*Implementation of a quantum bit in a superconducting circuit*', PhD Thesis, Université Paris VI, http://www-drecam.cea.fr/drecam/spec/Pres/Quantro/ (2002)
[48] Makhlin Y, Schön G, Shnirman A, Nature, **386**, 305 (1999)
[49] V. Bouchiat, D. Vion, P. Joyez, D. Esteve, M. H. Devoret, '*Quantum coherence with a single cooper pair*', Physica Scripta, Vol T76, 165-170 (1998)
[50] V. Bouchiat. '*Quantum fluctuations of the charge in single electron and single Cooper pair devices*.' PhD thesis, Université Paris VI, http://www-drecam.cea.fr/drecam/spec/Pres/Quantro/, (1997)
[51] Nakamura Y, Pashin Yu. A., Tsai J S, '*Coherent control of macroscopic quantum states in a single-Cooper-pair box*', Nature, **398**, 786 (1999)
[52] Vion D, Aassime A, Cottet A, Joyez P, Pothier H, Urbina C, Esteve D, Devoret M H, '*Manipulating the Quantum state of an electrical circuit'*, Science, **296**, 886 (2002)
[53] J. Q. You, J. S. Tsai, F. Nori, '*Scalable quantum computing with Josephson charge qubits'*, Phys. Rev. Lett. Vol. **89**, 19, 197902, (2002)
[54] Yu. A. Pashkin, T. Yamamoto, O. Astafiev, Y. Nakamura, D. V. Averin, J. S. Tsai, '*Quantum oscillations in two coupled charge qubits*', Nature **421**, 823-826 (2002)
[55] T. Yamamoto, Yu. A. Pashkin, O. Astafiev, Y. Nakamura, J. S. Tsai, '*Demonstration of conditional gate operation using superconducting charge qubit*', Nature, **425**, 941-944 (2003)
[56] J. E. Mooij, et al. '*Josephson persistent-current qubit*', Science, **285**, 1036 (1999)
[57] J. R. Friedman, J. E. Lukens et al. '*Quantum superposition of distinct macroscopic states*', Nature **406**, 43-46 (2000)
[58] C. H. Van de Wal, J. E. Mooij et al. '*Quantum superposition of macroscopic persistent-current states*', Science **290**, 773 (2000)
[59] I. Chiorescu, Y. Nakamura, C. J. P. M. Harmans, J. E. Mooij, '*Coherent quantum dynamics of a superconducting flux qubit*', Science **299**, 1869 (2003)
[60] J. B. Majer, J. E. Mooij et al. '*Spectroscopy on two coupled superconducting flux qubits*', Phys. Rev. Lett. **94**, 090501 (2005)
[61] J. H. Plantenberg, P. C. de Groot, C. J . P. M. Harmans, J. E. Mooij, '*Demonstration of a controlled-NOT quantum gates on a pair of superconducting quantum bits*', Nature **447**, 836 (2007)
[62] T. Hime, J. Clarke et al. '*Solid-state qubits with current-controlled coupling*', Science **314**, 1427 (2006)
[63] J. M. Martinis, S. Nam, J. Aumentado, and C. Urbina, '*Rabi oscillations in a large Josephson Junction qubit*', Phys. Rev. Lett. **89**, 11, 117901 (2002)
[64] R. McDermott, J. M. Martinis et al. '*Simultaneous state measurement of coupled Josephson phase qubits*', Science, **307**, 1299 (2005)
[65] I. Siddiqi and J. Clarke, '*Entangled solid-state circuits*', Science, **313**, 1400 (2006)
[66] M. Steffen, J. M. Martinis et al. '*State tomography of capacitively shunted phase qubits with high fidelity'*, Phys. Rev. Lett. **97**, 050502 (2006)
[67] M. A. Sillanpää, J. I. Park and R. W. Simmonds, '*Coherent quantum state storage and transfer between two phase qubits via a resonant cavity*', Nature, **449**, 438 (2007)

[68] Matthias Steffen, J. M. Martinis et al. '*Measurement of the entanglement of two superconducting qubits via state tomography*', Science, **313**, 1423 (2006)
[69] G. C. Stokes, Trans. Camb. Philos. Soc. **9**, 399, (1852)
[70] H. Häffner, R. Blatt et al. '*Scalable multiparticule entanglement of traped ions*', Nature **438**, 643 (2005)
[71] N. Schuch, J. Siewert, '*Natural two-qubit gate for quantum computation using the XY interaction* ', Phys. Rev. A. **67**, 032301 (2003)
[72] J. Koch, T. M. Yu, J. Gambetta, A. A. Houck, D. I. Schuster, J. Majer, A. Blais, M. H. Devoret, S. M. Girvin, R. J. Schoelkopf, '*Charge insensitive qubit design derived from the Cooper pair box*', Phys. Rev. A, **76**, 042319 (2007)
[73] A. Wallraff, R. J. Schoelkopf et al. '*Strong coupling of a single photon to a superconducting qubit using circuit quantum electrodynamics*', Nature, **431**, 162-167 (2004)

[74] D. I. Schuster, M. H. Devoret, R. J. Schoelkopf et al. '*Resolving photon number states in a superconducting circuit*', Nature, **445**, 515-518 (2007)
[75] A. A. Houck, R. J. Schoelkopf, et al.'*Generating single microwave photons in a circuit*', Nature, **449**, 328, (2007)
[76] J. Majer, R. J. Schoelkopf, et al. '*Coupling superconducting qubits via a cavity bus*', Nature, **449**, 443 (2007)
[77] M. F. Bocko, A. M. Herr and M. J. Feldman, IEEE Trans. Appl. Superconductivity **7**, 3638 (1997)
[78] A. Ustinov '*Quantum computing using superconductors*', in *'Nanoelectronics and information technology', p. 46, Rainer Waser Ed., Wiley VCH (2002)*
[79] D. Loss and D. DiVincenzo, '*Quantum computation with quantum dots*', Phys. Rev. A, **57**, 1, 120 (1998)
[80] R. Hanson, '*Electron spins in semiconductor quantum dots*', PhD Thesis, Delft University (2005)
[81] L. Vandersypen, '*Dot to dot design'*, IEEE Spectrum, p42, September 2007
[82] D. G. Austing, S. Tarucha et al. '*Quantum dot molecules'*, Phys. B Cond. Matt. **249-251**, 206-209 (1998)
[83] M. Bayer, A. Forchel et al. '*Coupling and entangling of quantum states in quantum dot molecules*', Science, **291**, 451 (2001)
[84] D. DiVincenzo, '*Prospects for Quantum Computing*', présenté à IEDM (2000)
[85] R. Hanson, et al. '*Zeeman energy and spin relaxation in a one-electron quantum dot*', Phys. Rev. Lett. **91**, 196802 (2003)
[86] J. M. Elzerman, L. M. K. Vandersypen, L. P. Kouwenhoven, et al. '*Single-shot readout of an individual electron spin in a quantum dot*', Nature **430**, 431 (2004)
[87] L. P. Kouwenhoven, D. G. Austing, and S. Tarucha, Rep. Prog. Phys. **64** (6), 701 (2001)
[88] J. R. Petta, C. Marcus, A. C. Gossard et al. '*Coherent manipulation of coupled electron spins in semiconductor quantum dots*', Science, **309**, 2180 (2005)
[89] N. J. Craig, C. M. Marcus, A. C. Gossard et al. '*Tunable nonlocal spin control in a coupled-quantum dot system*', Science **304**, 565 (2004)
[90] D. J. Reilly *et al*, Appl. Phys. Lett. **91**, p. 162101, (2007)
[91] J. R. Petta, et al '*Dynamic Nuclear polarization with single electrons spins*', Phys. Rev. Lett. **100**, 067601 (2008) (disponible gratuitement sur arXiv:0709.0920)
[92] Y. Hu, C. M. Lieber, C. M. Marcus et al. '*Double quantum dot with integrated charge sensor based on Ge/Si heterostructure nanowires*', Nature Nanotechnology **2**, p. 622, (2007)
[93] C. P. Poole, '*Electron spin resonance*' 2nd ed edn, Wiley New York (1983)
[94] M. Xiao, I. Martin, E. Yablonovitch, H. W. Jiang '*Electrical detection of the spin resonance of a single electron in a silicon field-effect transistor*', Nature **430**, 435 (2004)
[95] F. Jelezko, T. Gaebel, I. Popa, A. Gruber, J. Wrachtrup, '*Observation of coherent oscillations in a single electron spin*', Phys. Rev. Lett. **92**, 076401 (2004)
[96] F. H. L. Koppens, L. P. Kouwenhoven, L. M. K. Vandersypen et al. '*Driven coherent oscillations of a single electron spin in a quantum dot*', Nature **442**, 766 (2006)
[97] K. C. Nowack, F. H. Koppens, Yu. V. Nazarov, L. M. K. Vandersypen '*Coherent control of a single electron spin with electric fields*', Science 318, 1430 (2007)
[98] D. D. Awschalom, R. Epstein, and R. Hanson, '*The diamond age of spintronics*', Scientific American, October, pp 84-91 (2007)
[99] R. J. Epstein, F. M. Mendoza, Y. K. Kato and D. D. Awschalom, '*Anisotropic interactions of a single spin and dark-spin spectroscopy in diamond*', Nature physics, **1,** pp 9498 (2005)
[100] A. Beveratos, P. Grangier, et al. '*Room temperature stable single-photon source*',Eur. Phys. J. D **18** (2), 191 (2002) quant-ph/0110176.
[101] G. Messin, F. Treussard, '*Photons uniques et cryptographie quantique*',Images de la physique 2005 (CNRS), pp 118-125 (2005)
[102] A. Beveratos, P. Grangier, et al. '*Single photon quantum cryptography*', Phys. Rev. Lett. **89** (18), 187901 (2002) quant-ph/0206136.
[103] R. Alléaume, P. Grangier, et al. '*Experimental open air quantum key distribution with a single photon source*', New J. Phys. **6**, 92 (2004). quant-ph/0402110
[104] T. A. Kennedy et al. '*Long coherence times at 300K for nitrogen-vacancy center spins in diamond grown by chemical vapor deposition*', Appl. Phys. Lett. **83**, 4190-4192 (2003)
[105] J. Wrachtrup and F. Jelezko, '*Quantum information processing in diamond*', J. Phys.: Condens. Matter **18**: S807-S824 (2006)
[106] T. Kennedy, '*Dark spins come to light*', Nature physics **1**, pp 79-80 (2005)
[107] R. Hanson, D. D. Awschalom et al. '*Polarization and readout of coupled single spins in diamond*', Phys. Rev. Lett. **97**, 087601 (2006)
[108] L. Childress, J. Wrachtrup, M. D. Lukin et al. '*Coherent dynamics of coupled electron and nuclear spin qubits in diamond*', Science **314**, 281-285 (2006)
[109] M. V. Gurudev Dutt, M. D. Lukin et al. '*Quantum register based on individual electronic and nuclear spin qubits in diamond*', Science, **316**, 1312-1316 (2007)
[110] D. Ochoa, S. Deleonibus, E. Dujardin, C. Glattli, D. Mailly and D. Vion, '*L'électronique du futur, au-delà du transistor CMOS*', Rapport de mission, (2008) http://www.bulletins-electroniques.com/rapports/smm08_014.htm
[111] D. Ochoa, R. Herino et al. '*La nanophotonique en Californie*', Rapport de mission, (2007) http://www.bulletins-electroniques.com/rapports/smm07_047.htm
[112] D. Ochoa, R. Herino, R. Allegre, and R. Fayol, '*La nanophotonique aux Etats Unis*', Dossier Sciences Physiques Etats-Unis, (2007) http://www.bulletins-electroniques.com/rapports/2007/smm07_014.htm
[113] K. M. C. Fu, C. Santori, A. Spillane, and R. G. Beausoleil, '*Quantum information processing with diamond nitrogen-vacancy centers coupled to microcavities***',** Proc. SPIE Vol. **6903**, 69030M (2008)
[114] N. Gershenfeld and I. Chuang, '*Bulk spin-resonance quantum computation*', Science **275** 350-356 (1997)
[115] D. G. Cory, A. F. Fahmy and T. F. Havel, '*Ensemble quantum computing by NMR spectroscopy*', Proc. Natl. Acad. Sci. USA **94**, 1634-1639 (1997)
[116] I. Chuang, L. M. K. Vandersypen, X. Zhou, D. W. Leung and S. Lloyd, '*Experimental realization of a quantum algorithm*', Nature **393**, 143-146 (1998)
[117] T. D. Ladd, D. Maryenko, and Y.Yamamoto, '*Coherence time of decoupled nuclear spins in silicon*', Phys. Rev. B **71**, 014401 (2005)
[118] www.ece.duke.edu/~dwyer/courses/ece299.03/presentations/smith_feb21.pdf

[119] S. Warren, '*The usefulness of NMR quantum computing*', Science **277**, 5332, pp. 1688-1690 (1997)
[120] J. A. Jones, '*Nuclear magnetic resonance experiments*', in *The Physics of Quantum Information* (D. Bouwmeester, A. Ekert and A. Zeilinger, Eds.), Springer-Verlag (1999)
[121] J. A. Jones, '*Quantum computing and Nuclear magnetic resonance*', Phys. Chem. Comm. 11 (2001)
[122] S. L. Braunstein et al. '*Separability of very noisy mixed states and implications for NMR quantum computing*', Phys. Rev. Lett., **83**, 1054-1057 (1999)
[123] R. Schack and C. M. Caves, '*Classical model for bulk-ensemble NMR quantum computatio*n', Phys. Rev. A, **60**, 4354-4362 (1999)
[124] E. Knill and R. Laflamme, '*On the power of one bit of quantum information*', Phys. Rev. Lett., **81**, 5672-5675 (1998)
[125] D. Deutsch, '*Three connections between Everett's interpretation and experiment'* in *Quantum Concepts in Space and Time*, R. Penrose and C. J. Isham Eds., Clarendon Press, Oxford, pp. 215-225 (1986)
[126] I. L. Chuang, N. Gershenfeld and M. Kubinec, '*Experimental implementation of fast quantum searching*', Phys. Rev. Lett., **80**, 3408–3411 (1998)
[127] J. A. Jones, M. Mosca and R. H. Hansen, '*Implementation of a quantum search algorithm on a quantum computer*', Nature, **393**, 344–346 (1998)
[128] N. Linden, H. Barjat and R. Freeman, '*An implementation of the Deutsch-Jozsa algorithm on a thre- qubit NMR quantum computer*', Chem. Phys. Lett., **296,** 61-67 (1998)
[129] R. Marx, et al. '*Approaching five bit NMR quantum computing*', Phys. Rev. A, **62**, 012310 (2000)
[130] J. A. Jones and M. Mosca, '*Approximate quantum counting on an NMR ensemble quantum computer',* Phys. Rev. Lett., **83**, 1050-1053 (1999)
[131] L. M. K. Vandersypen, I. L. Chuang et al., '*Experimental realization of an order-finding algorithm with an NMR quantum computer*', Phys. Rev. Lett., **85**, 5452-5455 (2000)
[132] E. Knill, R. Laflamme, R. Martinez and C. H. Tseng, '*An algorithmic benchmark for quantum information processing*', Nature, **404**, 368-370 (2000)
[133] M. A. Nielsen, E. Knill and R. Laflamme, '*Complete quantum teleportation using. nuclear magnetic resonance*',Nature, 396, 52-55 (1998)
[134] D. G. Cory, et al, '*Experimental quantum error correction*', Phys. Rev. Lett., **81**, 2152-2155 (1998)
[135] E. Knill, at al., '*Implementation of the five qubit error correction benchmark',* LANL e-print http://arxiv.org/abs/quant-ph?0101034
[136] L. M. K. Vandersypen, I. L. Chuang et al., '*Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance*', Nature, 414, 883-887 (2001) quant-ph/0112176
[137]http://domino.watson.ibm.com/comm/pr.nsf/pages/news.20011219_quantum.html
[138] J. I. Cirac and P. Zoller, '*Quantum computation with cold trapped ions*', Phys. Rev. Lett. **74**, 4091 (1995)
[139] C. Monroe, D.M. Meekhof, B.E. King, W.M. Itano, and D.J. Wineland, "*Demonstration of a fundamental quantum logic gate*," Phys. Rev. Lett. **75**, 4714 (1995).
[140] Wieman, C., and S. Chu, Eds., J. Opt. Soc. Am. a special issue with many articles on laser cooling (1989)
[141] C.E. Wieman, D.E. Pritchard, and D.J. Wineland, '*Atom cooling, trapping, and quantum manipulation*', Rev. Mod. Phys. **71**, S253-S262 (1999)
[142]A. M. Steane, '*The ion trap quantum information processor*', Appl. Phys. B 64 623-642 (1997)
[143] C. Monroe, '*The trap technique, toward a chip-based quantum computer*', IEEE Spectrum, 37-43, August (2007)
[144] F. Schmidt-Kaler, R. Blatt et al. '*Realization of the Cirac-Zoller controlled-NOT quantum gate*', Nature **422**, 408-411 (2003)
[145] D. Kielpinski, C. Monroe, D. J. Wineland et al. '*A decoherence-free quantum memory using trapped ions*', Science **291**, 1013-1015 (2001)
[146] J. Chiaverini, D.J. Wineland et al. '*Realization of quantum error correction*', Nature **432**, 602-605 (2004)
[147] R. Reichle, D. J. Wineland et al. '*Experimental purification of two-atom entanglement*', Nature **443**, 838-841 (2006)
[148] D. J. Wineland et al. '*Quantum information processing with trapped ions*', Phil. Trans. R. Soc. Lond. A **361**, 1349-1361 (2003)
[149] D. Leibfried, D. J. Wineland et al.'*Experimental demonstration of a robust, high-fidelity geometric two ion-qubit phase gate*', Nature **422**, 412-415 (2003)
[150] J. Chiaverini, D. J. Wineland et al.'*Implementation of the semiclassical quantum Fourier transform in a scalable system*', Science **308** 997-1000 (2005)
[151] H. Häffner, R. Blatt et al. '*Scalable multiparticle entanglement of trapped ions*', Nature **438** 643 (2005)
[152] D. Leibfried, D. J. Wineland et al. '*Creation of a six-atom 'Schrödinger cat' state*', Nature **438** 639 (2005)
[153] J. I. Cirac and P. Zoller, '*A scalable quantum computer with ions in an array of microtraps*', Nature **404**, 579-581 (2000)
[154] D. J. Wineland et al. '*Quantum control, quantum information processing, and quantum-limited metrology with trapped ions*', ICOLS August (2005)
[155] M. A. Rowe et al. '*Transport of quantum states and separation of ions in a dual RF ion trap*', Quant. Inform. Comp. **2**, 257-271 (2002)
[156] S. Seidelin, D. J. Wineland et al. '*Microfabricated surface-electrode ion trap for scalable quantum information processing*', Phys. Rev. Lett. **96,** 253003 (2006)
[157] Q. A. Turchette et al. '*Heating of trapped ions from the quantum ground state*', Phys. Rev. A **61**, 063418-1-8 (2000)
[158] F. Schmidt-Kaler and P. Grangier, '*Les constructeurs de qubits*', Les Dossiers de la Recherche consacrés au monde quantique, p61-64, Novembre (2007)
[159] D. Leibfried, E. Knill, C. Ospelkaus and D. J. Wineland, '*Transport quantum logic gates for trapped ions*', Phys. Rev. A **76**, 032324 (2007)
[160] Site web QubitNews http://quantum.fis.ucm.es/pollBooth.pl?section=&qid=6&aid=-1
[161] P. Rabl, J. I. Cirac, P. Zoller et al., '*Defect-Suppressed Atomic Crystals in an Optical Lattice*', Phys. Rev. Lett. **91**, 110403 (2003)
[162] H. J. Briegel, J. I. Cirac, P. Zoller et al., '*Quantum computing with neutral atoms'*, Journal of Modern Optics, 47, 415 (2000)
[163] Voir le 6ème cours de l'année 2006-2007 http://www.lkb.ens.fr/recherche/qedcav/college/collegeparis.html
[164] H. J. Briegel and R. Raussendorf, '*Persistent Entanglement in Arrays of Interacting Particles*', Phys. Rev. Lett. **86**, 910 (2001)

[165] O. Mandel, I. Bloch et al., '*Controled collisions for multi-particles entanglement of optically trapped atoms*', Nature, **425**, 937 (2003)
[166] R. Raussendorf and H. J. Briegel, '*A one-way quantum computer*', Phys. Rev. Lett. **86**, 5188 (2001)
[167] F. Chevy, '*La preuve par les atomes froids*', Les dossiers de la Recherche, pp 72-77, (Novembre 2007)
[168] R. Feynman, '*Simulating Physics with Computers*', Int. J. Theor. Phys., **21**, 467 (1982)
[169] M. Zwierlein, W. Ketterle et al., '*Vortices and superfluidity in a strongly interacting Fermi gaz*', Nature, **435**, 1047 (2005)
[170] A. Moerdijk B. J. Verhaar, and A. Axelssonet, '*Resonances in ultracold collisions of ^{6}Li, ^{7}Li, and ^{23}Na*', Phys. Rev. A, 51, 4852 (1995)
[171] S. Haroche, '*Quantum Information in Cavity Quantum Electrodynamics: Logical Gates, Entanglement Engineering and 'Schrodinger-Cat States*' Philosophical Transactions: Mathematical, Physical and Engineering Sciences, Vol. **361**, No. 1808, Practical Realizations of Quantum Information Processing, pp. 1339-1347 (2003)
[172] L. Davidovich, M. Brune, J.M. Raimond, S. Haroche, '*Mesoscopic quantum coherences in cavity QED: preparation and decoherence monitoring schemes*', Phys. Rev. A **53**, 1295-1309 (1996)
[173] S. Gleyes, S. Haroche et al. '*Quantum jumps of light recording the birth and death of a photon in a cavity*', Nature, **446**, 297-300 (2007)
[174] http://nobelprize.org/nobelfoundation/symposia/physics/ncs-2001-1/haroche.pdf
[175] M. Brune, J. M. Raimond, S. Haroche et al., '*Quantum Rabi Oscillation: A Direct Test of Field Quantization in a Cavity*', Phys. Rev. Lett. **76**, 1800 (1996)
[176] J. M. Raimond, M. Brune and S. Haroche, '*Manipulating quantum entanglement with atoms and photons in a cavity*', Rev. Mod. Phys. **73**, 565-582 (2001)
[177] A. Rauschenbeutel, S. Haroche et al., '*Coherent Operation of a Tunable Quantum Phase Gate in Cavity QED*', Phys. Rev. Lett. **83**, 5166 (1999)
[178] M. Brune, S. Haroche et al. '*Quantum nondemolition measurement of small photon numbers by Rydberg-atom phase-sensitive detection*', Phys. Rev. Lett. **65**, 976 (1990)
[179] G. Nogues, S. Haroche et al. '*Seeing a single photon without destroying it*', Nature **400**, 239 (1999)
[180] E. Hagley, S. Haroche et al. '*Generation of Einstein-Podolsky-Rosen Pairs of Atoms'*, Phys. Rev. Lett., 79, 1-5 (1997)
[181] A. Rauschenbeutel, S. Haroche et al. '*Step-by-Step Engineered Multiparticle Entanglement'*,Science **288**, 2024-2028 (2000)
[182] B. Bertet, S. Haroche et al. '*A complementarity experiment with an interferometer at the quantum-classical boundary*', Nature **411**, 166 (2001)
[183] 'Quantum information processing and communication', Strategic report on current status, visions and goals for research in Europe, ERA-Pilot – Qurope, (Octobre 2007) http://qist.ect.it/Reports/Content/reports_content.pl
[184] http://qubit.nist.gov/qiset-PDF/Williams.QISET2004.pdf
[185] '*A quantum information science and technology roadmap*', report of the quantum information science and technology experts panel, v. 2.0 Avril 2004, http://qist.lanl.gov/qcomp_map.shtml
[186] Bell J S '*On the Einstein-Podolsky-Rosen paradox*', Physics **1**, 195-200 (1964)
[187] Bell J S '*On the problem of hidden variables in quantum theory*', Rev. Mod. Phys. **38**, 447-52, (1966)
[188] Feynman R P '*Simulating physics with computers*', Int. J. Theor. Phys. **21**, 467-488 (1982)
[189] Aspect A, Dalibard J, and Roger G, '*Experimental test of Bell's inequalities using time-varying analysers*', Phys. Rev. Lett. **49**, 1804-1807 (1982)
[190] Aspect A. '*Testing Bell's inequalities*', Europhys. News. **22**, 73-75 (1991)
[191] Greenberger D. M., Horne M. A. and Zeilinger A. '*Going beyond Bell's theorem*', in Bell's theorem, quantum theory and conceptions of the universe, Kafatos M, ed (Kluwer Academic, Dordrecht) 73-76 (1989)
[192] Wooters W K and Zurek W H, '*A single quantum cannot be cloned*', Nature **299**, 802 (1982)
[193] Glauber R J, in Frontiers in Quantum Optics, Pike E R and Sarker S, eds (Adam Hilger, Bristol) (1986)
[194] Bennett C H and Wiesner S J '*Communication via one- and two-particle operations on Einstein-Podolsky-Rosen states*', Phys. Rev. Lett. **69**, 2881-2884 (1995)
[195] Mattle K, Weinfurter H, Kwiat P G and Zeilinger A, '*Dense coding in experimental quantum communication*' , Phys. Rev. Lett. **76**, 4656-4659, (1996)
[196] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A and Wooters W K, '*Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*', Phys. Rev. Lett. **70**, 1895-1898, (1993)
[197] Bennett C H '*Quantum information and computation*', Phys. Today. **48 10** 24-30 (1995)
[198] D. Boschi, S. Branca, F. De Martini, L. Hardy, S. Popescu, "*Experimental Realisation of Teleporting an Unknown Pure Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels*" Phys. Rev. Lett. **80**, 1121.
[199] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, A. Zeilinger, *Experimental Quantum Teleportation,* Nature **390**, 6660, 575-579 (1997).
[200] Rupert U, Zeilinger A et al. '*Quantum teleportation link accross the Danube*', Nature, **430**, 849 (2004)
[201] M. D. Barrett, J. Chiaverini, T. Schaetz, J. Britton, W. M. Itano, J. D. Jost, E. Knill, C. Langer, D. Leibfried, R. Ozeri, D. J. Wineland, *Deterministic Quantum Teleportation of Atomic Qubits,* Nature **429**, 737 (2004).
[202] M. Riebe, H. Häffner, C. F. Roos, W. Hänsel, J. Benhelm, G. P. T. Lancaster, T. W. Körber, C. Becher, F. Schmidt-Kaler, D. F. V. James and R. Blatt, *"Deterministic quantum teleportation with atoms"***,** Nature **429**, 734 (2004)
[203] C. H. Bennett, G. Brassard, '*Quantum public key distribution reinvented*' SIGACTN : SIGACT News (ACM Special Interest Group on Automata and Computability Theory) 18 (1984)
[204] A. Ekert '*Quantum cryptography based on Bell's theorem*', Phys. Rev. Lett. **67**, 661-663 (1991)
[205] C. H. Bennett and G. Brassard, SIGACT News **20**, 78-82 (1989)
[206] H. Zbinden et al. '*Interferometry with Faraday mirrors for quantum cryptography*', Elect. Lett. **33**, 586-588 (1997)
[207] P. A. Hisket et al. '*Long distance quantum key distribution in optical fiber*', New Journal of Physics, **8** 193 (2006)
[208] R. Ursin, A. Zeilinger et al. '*Free space distribution of entanglement and single photons over 144km*', Nature Physics **3**, 481 - 486 (2007)

[209] T. Schmidt-Manderbach, A. Zeilinger et al. '*Experimental demonstration of free-space decoy-state quantum key distribution over 144km*', Phys. Rev. Lett. **98** 010504 (2007)
[210] '*Quantum communication at ESA: Towards a space experiment on the ISS*', J. Perdigues, A. Zeilinger et al., Conference Proceedings IAC2007, Hydarabath India (2007)
[211] A. Church, '*An unsolvable problem of elementary number theory*', Amer. J. Math. **58**, 345-363 (1936)
[212] A. M. Turing '*On computable numbers, with an application to the Entschneidungsproblem*', Proc. Lond. Math. Soc. Ser. 2 **42**, 230 (1936)
[213] R. Rivest, A. Shamir and L. Adleman, '*On digital signatures and public-key cryptosystems*', MIT Laboratory for Computer Science, Technical Report, MIT/LCS/TR-212 (1979)
[214] IEEE Spectrum, '*A weaker cheaper MRI'*, January 2008, p. 21

XIII. LISTE DES PRINCIPALES EQUIPES DE RECHERCHE

La liste ci-dessous récapitule les principales équipes de recherche, aux Etats-Unis et ailleurs, travaillant sur les différentes disciplines affiliées à l'ordinateur quantique, qui sont étudiées dans ce dossier[v].

SUPRACONDUCTEURS

Averin & Likharev	StonyBrook	USA	Théorie des qubits supraconducteurs
Berggren	MIT	USA	Qubits de flux
Clarke	Berkeley	USA	Qubits de flux
Delsing	Chalmers	USA	Qubits de charge
Devoret	Yale	USA	Qubits de charge
Echternach	JPL	USA	Qubits de charge
Feldman/Bocko	Rochester	USA	Qubits de flux
Han	Kansas	USA	Qubits de flux et qubits de phase à simple jonction
Équipe de Koch	IBM	USA	Qubits de flux
Ladizinsky	TRW, CA	USA	Qubits de flux
Levitov	MIT	USA	Théorie des qubits supraconducteurs
Likharev	StonyBrook	USA	Qubits de charge
Lloyd	MIT	USA	Théorie des qubits supraconducteurs
Lukens, Likharev, & Semenov	StonyBrook	USA	Qubits de flux
Manheimer	LPS, Maryland	USA	Qubits de charge
Martinis	UCSB	USA	qubits de phase à simple jonction
Nori	Michigan and Riken	USA	Théorie des qubits supraconducteurs
Oliver, Gouker	Lincoln Lab	USA	Qubits de flux
Orlando	MIT	USA	Qubits de flux
Schoelkopf	Yale	USA	Qubits de charge
Simmonds	NIST	USA	Qubits de phase
van Harlingen	Illinois	USA	Qubits de flux
Wellstood, Anderson, & Lobb	Maryland	USA	Qubits de flux et qubits de phase à simple jonction
Buisson	Institut Néel, Grenoble	France	Qubits de charge
Esteve	Saclay	France	Qubits de charge
Nakamura	NEC	Japon	Qubits de charge
Tanaka	NTT	Japon	Qubits de flux
Schön, Shnirmann, & Makhlin	Karlsruhe	All.	Théorie des qubits supraconducteurs
Ustinov	Erlangen	All.	Qubits de flux
Wilhelm	Munich	All.	Théorie des qubits supraconducteurs
Kouwenhoven	Delft	Pays Bas	Qubits de charge

[v] '*A quantum information science and technology roadmap*', report of the quantum information science and technology experts panel, v. 2.0 Avril 2004, http://qist.lanl.gov/qcomp_map.shtml

Mooij	Delft	Pays Bas	Qubits de flux
Cosmelli	Rome	Italie	Qubits de flux
Falci	Catania	Italie	Théorie des qubits supraconducteurs
Fazio	Pisa	Italie	Théorie des qubits supraconducteurs
Silvestrini	Naples	Italie	Qubits de flux
Bruder	Bâles	Suisse	Théorie des qubits supraconducteurs
Choi		Corée	Théorie des qubits supraconducteurs

SEMICONDUCTEURS

Awschalom, D.	UC-Santa Barbara	USA	Systèmes de spin à GaAs, systèmes à excitons
Barrett, S.	Yale	USA	ESR dans des composants semiconducteurs
Das Sarma, S.	Maryland	USA	Théorie
Doolen, G.	LANL, Los Alamos	USA	Théorie
Gammon, D.	NRL, Maryland	USA	Spectroscopie à exciton unique
Hammel, P. C.	Ohio State U.	USA	Lecture de spin à force magnétique
Hawley, M.	LANL	USA	Impureté P dans Si
Kane, B.	Univ of Maryland	USA	Impureté P dans Si
Kastner, M.	MIT	USA	Boîtes quantiques GaAs
Levy, J.	Univ. of Pittsburg	USA	Boîtes quantiques Si/Ge
Marcus, C.	Harvard	USA	Fils et Boîtes quantiques GaAs, Nanotubes de Carbone
Raymer, M.	U. of Oregon	USA	Boîtes quantiques en microcavités
Roukes, M.	Caltech	USA	Cantilevers à haute fréquence, et quantiques
Schenkel, T.	LBNL	USA	Impureté P dans Si
Schoelkopf, R.	Yale	USA	Effet tunnel à electron unique en RF et Boîtes de Cooper (CPB)
Schwab, K.	NSA, Maryland	USA	Cantilevers quantiques et CPB
Sham, L. J.	UC-Santa Barbara	USA	Théorie
Steel, D.	U. of Michigan	USA	Excitons et trions en boîtes quantiques
Tucker, J.	U. of Illinois at Urbana-Champaign	USA	Impuretés P dans Si
	U. of Wisconsin consortium	USA	Boîtes quantiques Si/Ge
Webb, R.	Maryland	USA	Boîtes quantiques GaAs
Whaley, B.	UC-Berkeley	USA	Théorie
Yablonovich, E.	UC-Los Angeles	USA	Impuretés P dans Si
Nakamura, Y.	NEC	Japon	Cooper pair box (CPB)
Tarucha, S.	Tokyo	Japon	Boîtes quantiques GaAs
Kotthaus, J.	Munich	All.	Boîtes quantiques GaAs
Kouwenhoven, L.	TU Delft	Pays Bas	Boîtes quantiques GaAs
Pepper, M.	Cambridge	UK	Electrons canalisés dans des ondes acoustiques de surface, impuretés Na dans Si
Rossi, F.	Torino	Italie	Théorie
Ensslin, K.	ETH, Zurich	Suisse	Boîtes quantiques GaAs
Loss, D.	U. of Basel	Suisse	Théorie
Sachrajda, A.	NRC Ottawa	Canada	Boîtes quantiques GaAs, états de bord
Clark, R.	U. of New South Wales	Australie	Impuretés P dans Si

RMN

Cory & Havel	MIT Nuclear Engineering	USA	
Gershenfeld & Chuang	MIT Media Lab	USA	
Knill	Los Alamos	USA	
Laflamme	Waterloo	USA	
Glaser	Munich	All.	
Jones	Oxford	UK	
Kim		Corée	
Kumar	Bangalore	Inde	
Zeng		Chine	

IONS PIÉGÉS

Berkeland, D.	LANL	USA	Sr+
Devoe, R.	Almaden (IBM)	USA	Ba+
Monroe, C.	U. of Michigan	USA	Cd+
Wineland, D.	NIST, Boulder	USA	^{9}Be+, Mg+
Blatt, R.	Innsbruck	Autriche	Ca+
Drewsen, M.	Aarhus	Danemark	Ca+
Gill, P.	NPL, Teddington	UK	Sr+
King, B.	U. Hamilton, Ontario	Canada	Mg+
Steane, A.	Oxford	UK	Ca+
Wunderlich,C.	Hamburg	All.	Yb+
Walther, H.	Max-Planck Institute, Garching	All.	Mg+, In+

ATOMES NEUTRES

Chapman, M. S.	Georgia Tech, Atlanta	USA	Piégeage magnétique et optique
Cirac, J. I.	Max-Planck- Institute, Garching	All.	Théorie
Cote, R.	U. of Connecticut, Storrs	USA	Théorie
Deutsch, I. H.	U. of New Mexico	USA	Théorie
Gould, P.	U. of Connecticut, Storrs	USA	Piégeage optique d'atomes de Rydberg
Jessen, P. S.	U. of Arizona, Tucson	USA	Réseaux optiques
Lukin, M.	Harvard, Massachusetts	USA	Théorie
Phillips, W. D. & Rolston, S. L.	NIST Gaithersburg, Maryland	USA	Réseaux optiques
Saffman, M. & Walker, T. G.	U. of Wisconsin, Madison	USA	Piégeage optique d'atomes de Rydberg
Stamper-Kurn, D.	UC Berkeley, California	USA	Micropièges magnétiques
Weiss, P.	Penn State, State College	USA	Réseaux optiques/ atomes de Rydberg
Williams, C. J.	NIST Gaithersburg, Maryland	USA	Théorie
You, L.	Georgia Tech, Atlanta	USA	Théorie
Grangier, P.	Institut d'Optique, Orsay	France	Piégeage d'atomes uniques
Reichel, J.	LKB, Paris	France	Microcircuits à atomes
Raimond, J. M. Brune, M. & Nogues G.	LKB, Paris	France	Atomes en cavité
Salomon & Chevy	LKB, Paris	France	Gaz de Fermi dégénérés
Dalibard, J.	LKB, Paris	France	BEC

Ertmer, W. & Birkl, G.	U. of Hannover	All.	Piégeage optique avec micro-optiques
Haensch, T. W. & Bloch, I.	Max-Planck-Institute, Garching	All.	BEC/piégeage optique
Meschede, D.	U. of Bonn	All.	Piégeage d'atomes uniques
Reichel, J.	U. of Mainz	All.	Micropièges magnétiques
Schmiedmayer, J.	U. of Heidelberg	All.	Micropièges magnétiques
Zoller, P. & Briegel, H. J.	U. of Innsbruck	Autriche	Théorie
Mølmer, K.	U. of Aarhus	Danemark	Théorie

OPTIQUE QUANTIQUE

Chapman, M.	Georgia Tech	USA	Rb, Ba+
Feld, M.	MIT	USA	Ba
Kimble, J.	Caltech	USA	Cs
Mabuchi, H.	Caltech	USA	Cs
Orozco, L.	U. Maryland	USA	Rb
Stamper-Kurn, D.	UC Berkeley	USA	Rb
Haroche, S.	ENS, Paris	France	Rb (Rydberg)
Kuga, T.	U. of Tokyo	Japon	Rb
Meschede, D.	U. of Bonn	All.	Cs
Rempe, G.	Max-Planck Institute, Garching	All.	Rb
Walther, H.	Max-Planck Institute, Garching	All.	Ca+
Blatt, R.	U. of Innsbruck	Autriche	Ca+
Esslinger, T.	ETH, Zurich	Suisse	Rb

Dossier rédigé par :

Daniel Ochoa
Attaché pour la Science et la Technologie
attache-stic.mst@consulfrance-sanfrancisco.org

Service scientifique du Consulat Général de France à San Francisco
540 Bush St, San Francisco, CA 94108, USA

SCIENCES PHYSIQUES ETATS-UNIS

NANOSCIENCES, MICROELECTRONIQUE, MATERIAUX

Avril 2008

Pour vous abonner gratuitement à :

SCIENCES PHYSIQUES ETATS-UNIS
et être informé en priorité de la disponibilité des prochains numéros, il suffit d'envoyer un courrier électronique à l'adresse:
subscribe.be.etatsunis@adit.fr
Vous recevrez en retour une confirmation d'abonnement.

Directeur de la publication :
Michel ISRAEL

Rédacteurs en chef :
Roland HERINO
Daniel OCHOA

Rédacteurs :
Jean-Baptiste KEMPF
Alban DE LASSUS SAINT-GENIES

SCIENCES PHYSIQUES ETATS-UNIS
est une publication trimestrielle de
la Mission pour la Science et la Technologie
de l'Ambassade de France aux Etats-Unis,
dont la diffusion est assurée par l'ADIT

Vous y trouverez un archivage des anciens numéros et découvrirez aussi les autres publications de la Mission pour la Science et la Technologie

-S&T Presse
-Flash TIC
-Revue santé Etats-Unis
-Revue de l'environnement
-Etats-Unis Espace
-Etats-Unis Microélectronique/ Matériaux
(archives précédant la fusion)

Retrouvez SCIENCES PHYSIQUES ETATS-UNIS ainsi que toute l'actualité technologique aux Etats-Unis et dans le reste du monde sur le site:

http://www.bulletins-electroniques.com/

DOSSIERS ETATS-UNIS SCIENCES-PHYSIQUES

- Janvier 2008 : Molecular electronics in the United States
- Septembre 2007 : Combattre le cancer à l'aide des nanotechnologies.
- Juillet 2007 : L'électronique moléculaire aux Etats-Unis
- Février 2007 : La nanophotonique aux Etats Unis
- Octobre 2006 : Comment maîtriser les risques posés par les nanotechnologies ? L'approche Américaine.
- Juin 2006 : Recherche et Industrie Photovoltaïque (PV) aux Etats Unis
- Février 2006 : Recherche et production industrielle des nanotubes de carbone - Recherche américaine : vers un modèle ouvert basé sur la collaboration
- Octobre 2005 : Nanotechnologies et santé publique - A l'interface du nanomonde - De nouvelles cellules photovoltaïques - Du nouveau dans les semiconducteurs
- Août 2005 : La photolithographie
- Février 2005 : L'électronique grand public aux Etats-Unis
- Juillet 2004 : L'International Roadmap for Semiconductors
- Mai 2004 : Les Nanocomposites aux Etats-Unis

AUTRES RAPPORTS ETATS-UNIS

- Mars 2008 : L'électronique du futur, au-delà du transistor CMOS
- Janvier 2008 : Les Community Colleges aux Etats-Unis
- Janvier 2008 : Le rôle des think tanks dans la définition de la politique scientifique et technologique aux Etats-Unis
- Juin 2007: La nanophotonique en Californie
- Mai 2007: Les pôles d'excellence en recherche environnementale aux Etats-Unis - Volume 1 : les acteurs fédéraux
- Novembre 2006 : Aperçus sur l'énergie aux Etats-Unis
- Mars 2006 : Forum Energie et Nanotechnologie : stockage et distribution
- Janv 2006 : Regards français sur la Silicon Valley
- Janv 2006 : Présence française dans le domaine High Tech dans la region de San Francisco
- Sept 2005 : Les efforts de Recherche et Développement en nanotechnologies aux USA
- Sept 2005 : La Politique Fédérale de R&D en Nanotechnologies aux Etats Unis
- Sept 2005 : Le développement technologique dans la région de San Francisco
- Sept 2005 : Le Devenir des Post-doctorants en Amérique du Nord
- Mars 2005 : La spintronique aux Etats-Unis - Un Aperçu des Recherches
- Jan 2005 : Nanoélectronique – USA