GdR "Information et communication quantique" Juillet 2000
www.iota.u-psud.fr/ GdR-IQ/

Introduction à l'information quantique

J.-Ph. Poizat et R. Mosseri

1 Introduction

L'information quantique est un nouveau champ de recherche dont l'objectif est de tirer partie des possibilités offertes par la mécanique quantique pour traiter l'information d'une manière plus efficace [1]. Les deux composantes principales en sont d'une part la cryptographie quantique, qui apporte une sécurité accrue par rapport aux systèmes de cryptographie classique, et d'autre part le calcul quantique, pour lequel de nouveaux algorithmes basés sur les principes de la mécanique quantique permettent de diminuer radicalement les temps de calculs nécessaires pour résoudre certains problèmes.

Ces deux composantes sont en fait étroitement liées. En effet, la confidentialité des systèmes de cryptographie à clé publique utilisés actuellement repose sur la difficulté algorithmique supposée de certains problèmes, comme par exemple la décomposition de grands nombres en facteurs premiers. Un ordinateur quantique pourrait justement arriver à factoriser des grands nombres en un temps exponentiellement plus court. D'où la nécessité de développer d'autres méthodes de cryptographie, résistantes à une attaque "quantique", et l'interêt suscité par les possibilités d'un ordinateur quantique.

Cette question de la décomposition rapide en facteurs premiers est emblématique. L'algorithme proposé par P. Shor en 94 [2] a transformé le champ d'activité discret d'un petit nombre de pionniers du calcul quantique des années 80, en une discipline à la croissance explosive dans la période récente. Même les plus pessimistes sur la possibilité de voir un jour se réaliser ce "rêve de théoriciens" s'accordent pour en attendre quelques très beaux résultats, tant au niveau fondamental qu'à celui des applications. Les plus optimistes (et il en faut) s'emploient à répondre aux premiers en suggérant toujours de nouvelles solutions pour contourner les obstacles, comme par exemple les

codes correcteurs d'erreurs quantiques permettant, non d'éliminer, mais de s'accommoder de la décohérence. De ce débat permanent, signe d'un thème bien vivant, émerge un champ multidisciplinaire allant de l'algorithmique quantique à la physique de la matière condensée en passant par l'optique quantique.

L'information quantique concerne des enjeux économiques réels, se rattachant aux défis de la société de l'information, comme par exemple les communications sécurisées avec la confidentialité accrue offerte par la cryptographie quantique. L'information quantique est également un sujet très riche et extrêment stimulant du point de vue fondamental et technologique. Il est certain que ce terrain est propice à l'apparition d'idées nouvelles, sans qu'il soit possible aujourd'hui de prévoir d'où vont venir les solutions.

Un bref aperçu de l'état de l'art dans le domaine de la cryptographie quantique et du calcul quantique est détaillé ci-dessous.

2 Cryptographie quantique

La cryptographie quantique est basée sur le fait qu'un bit d'information est codé sur un seul objet quantique, comme par exemple un seul photon. Or d'après les lois de la mécanique quantique, il n'est pas possible de mesurer un système quantique inconnu sans le modifier. Un espion essayant d'intercepter une communication entre deux parties (traditionnellement nommées Alice et Bob), ne pourra alors pas extraire d'information utile sans être détecté par Alice et Bob. Ces derniers pourront donc partager une clé aléatoire avec une sécurité absolue basée sur les lois de la mécanique quantique.

Les principes théoriques de la cryptographie quantique ont été établis au milieu des années 80. Depuis plusieurs réalisations expérimentales ont démontré la faisabilité de tels protocoles d'échange de clés quantiques [3]. On peut citer la réalisation par le groupe de N. Gisin à Genève d'échange de clés sous le lac de Genève (plusieurs dizaines de km) en utilisant des fibres télécom déjà en place [4]. Plus récemment, le groupe de Los Alamos a démontré la possibilité d'un échange de clé quantique à l'air libre sur plus de 1 km [5]. Cette dernière expérience est un pas important vers la réalisation d'un protocole de cryptographie quantique entre la terre et un satellite.

Il existe deux principaux types de protocoles d'échange de clés quantique. Le plus ancien est basé sur l'envoi de photons polarisés [6] ou modulés

en phase. La sécurité de ce type de protocole repose sur la possibilité de bénéficier d'une vraie source de photons uniques [7]. En effet, jusqu'à présent, toutes les expériences de ce type ont été réalisées avec des impulsions laser très atténuées, dont certaines contiennent quand même plus de 1 photon. Un des sujets de recherche actuels est la réalisation de vraies sources de photons uniques [8, 9, 10, 11]. Le deuxième type de protocole est basée sur la production de paires de photons intriquées [12] et n'a été démontré expérimentalement que très récemment [13, 14, 15].

Si en principe un fonctionnement parfait de ces protocoles conduit à une sécurité absolue, un problème important est de savoir quelle est la sécurité effective dans des conditions réelles de fonctionnement, c'est-à-dire avec des pertes et des erreurs sur les canaux de transmissions. En l'état actuel des connaissances, les avantages relatifs des deux protocoles mentionnés ci-dessus ne sont pas complètement identifiés. Les directions de recherches concernent donc l'amélioration et le contrôle de la sécurité des transmissions ainsi que l'accroissement des débits qui restent encore très faibles (1 kbits/s). Elles vont des preuves mathématiques de sécurité dans des conditions réelles à l'amélioration de l'efficacité quantique de compteurs de photons à la longueur d'onde telecom de 1.5 μm.

On peut également mentionner la possibilité de faire de la communication quantique avec des variables continues [16], en utilisant des techniques reliées à la lumière comprimée et aux mesures quantiques non-destructives en optique.

3 Calcul quantique

3.1 Les principes

Dans un ordinateur quantique le support physique traitant l'information obéit aux lois de la physique quantique. Les bits deviennent des qubits et sont constitués de systèmes à deux niveaux. Un qubit peut être dans une superposition cohérente de ses deux états. Un registre, constitué d'un ensemble de qubits, peut également être dans une superposition cohérente de différents états. En d'autres termes le nombre écrit dans un registre peut prendre plusieurs valeurs à la fois. La manipulation d'un tel registre dans un ordinateur quantique permet l'exploration simultanée de situations correspondant

aux différentes valeurs du registre. Les informations appropriées extraites du calcul tirent alors parti d'effets d'interférence. Le résultat obtenu dépendra alors des différents chemins suivis par les différentes valeurs du registre. Les superpositions quantiques peuvent être non-séparables, c'est-à-dire que seul l'état de l'ensemble du registre est connu sans que l'on puisse déterminer l'état d'un seul qubit. La quantité d'information contenu dans ces états non-séparables (ou intriqués) est exponentiellement plus grande que dans un système classique de même taille. Ce "parallélisme" quantique permet donc l'exploration d'un espace bien plus grand pour un nombre d'opération donné [1, 18].

Il existe pour l'instant deux algorithmes principaux tirant partie des spécificités d'un ordinateur quantique. L'algorithme de Shor permet une amélioration exponentielle pour la factorisation [2], tandis que celui de Grover accélère de façon quadratique la recherche d'un mot dans une liste [19]. La recherche de nouveaux algorithmes passe par l'identification de certains types de problèmes pouvant a priori bénéficier d'une résolution accélérée par un ordinateur quantique. Ce domaine de recherche constitue un défi considérable pour les chercheurs en algorithmique quantique.

La réalisation pratique d'un tel ordinateur doit cependant faire face à des difficultés expérimentales et théoriques énormes et non encore résolues. La difficulté principale est d'arriver à préserver la cohérence quantique pendant toute la durée du calcul. Celà signifie que les qubits, tout en étant couplés entre eux, doivent être complètement découplés du monde extérieur. Plus le nombre de qubits est grand, plus la probabilité que l'un des qubits interagisse avec l'environnement est grande, et donc plus la probabilité que le calcul échoue est grande. Or le nombre de qubits nécessaire à la réalisation d'une tâche utile (plusieurs milliers pour factoriser un nombre de 200 chiffres) est pour l'instant bien au-delà du record actuel de l'intrication de 4 qubits [17].

Une découverte essentielle pour tenter de résoudre le problème de décohérence qui est l'obstacle majeur à la réalisation d'un ordinateur quantique, est l'existence de code correcteurs d'erreurs quantiques [20, 21]. Le principe utilisé est de coder l'état d'un qubit de manière redondante sur une superposition judicieusement choisie de plusieurs qubits. L'altération d'un des qubits de la superposition est alors détectée et corrigée sans extraire d'information sur l'état du qubit initial, ce qui préserve la cohérence quantique du registre. Par contre, les codes correcteurs d'erreurs actuels ne sont efficaces que lorsque les taux d'erreurs sont très faibles (typiquement inférieurs à 10^{-5}).

3.2 Les approches expérimentales

Les approches expérimentales proposées pour la réalisation d'un ordinateur quantique sont nombreuses et variées. Dans un premier temps, il s'agit de réaliser une porte logique élémentaire, c'est-à-dire d'arriver à coupler deux systèmes quantiques de façon suffisament forte pour que l'état de l'un puisse être modifié par l'état de l'autre avant que la décohérence n'entre en jeu. L'étape suivante consiste à augmenter le nombre de qubits en interaction pour construire un vrai ordinateur. Des propositions ont été faites pour cette dernière étape [22, 23], mais la plupart soulève des difficultés technologiques considérables. Ces propositions se rapportant à différents domaines de la physique sont détaillées ci-dessous.

Ions piégés. Un qubit est supporté par un système à deux niveaux formé par l'état fondamental et un niveau électronique excité metastable d'un ion. Plusieurs de ces ions sont piègés et refroidis dans un piège linéaire. La force électrostatique les maintient à distance. Le couplage entre les ions est assuré par des modes de vibration collectifs. Chaque ion est adressable individuellement par un laser. L'éclairement d'un ion à une longueur d'onde bien choisie peut également exciter un mode d'oscillation collectif de tous les ions dans le piège. La valeur du qubit porté par cet ion est alors transférée sur les autres ions. On peut alors réaliser toutes les opérations logiques élémentaires nécessaires à la réalisation d'un ordinateur quantique [24]. Une démonstration expérimentale sur un seul ion a été effectué par un groupe américain [25], et plusieurs groupes dans le monde travaillent actuellement à l'extension de ce type de système à plusieurs ions. Une version améliorée adaptable à un grand nombre d'ions a récemment été proposée théoriquement [23].

Atomes neutres. On peut également mentionner des propositions récentes de pièges périodiques chargés par des atomes froids ou encore des condensats de Bose-Einstein. Les qubits sont constitués par les états de spin de l'état fondamental des atomes dans chaque alvéole du piège. Divers mécanismes d'interaction entre atomes ont été proposés, basés sur la notion de collisions froides [26], ou de couplage dipôle-dipôle [27].

Electrodynamique quantique en cavité - micro-ondes. Le régime de couplage fort obtenu entre un atome de Rydberg et le champ contenu dans une cavité microonde permet d'intriquer les états atomiques et les états du champ. Ce système a permis de réaliser des expériences de démonstration de fonctions élémentaires de traitement quantique de l'information [28, 30], des

tests de la non-localité quantique [31], ou encore des processus de décohérence [29].

Electrodynamique quantique en cavité - optique. Les expériences dans le domaine optique [32] sont moins avancées qu'en microondes. Mais les photons optiques se propagent plus facilement à l'air libre ou dans des fibres, se détectent plus facilement, et apparaissent donc comme plus prometteurs comme candidats à la réalisation d'algorithme quantique simple. Dans la proposition théorique originale, chaque qubit est codé sur deux niveaux stables de l'état fondamental d'un atome. Plusieurs atomes (ou ions) sont situés dans une cavité optique et sont couplés entre eux via le champ électromagnétique de la cavité [33]. Les difficultés expérimentales actuelles sont de contrôler la position d'un atome par rapport aux noeuds et aux ventres de l'onde stationnaire de la cavité [34, 35].

RMN. A l'heure actuelle, le système ayant démontré expérimentalement le calcul quantique le plus sophistiqué (sept opérations logiques sur deux qubits) est basée sur la résonance magnétique nucléaire [36, 37]. Les qubits sont les états de spin nucléaire d'atomes dans une molécule. Ils sont très bien isolés du monde extérieur et ont donc des temps de cohérence long. Chaque spin a sa propre fréquence de résonance et peut dont être manipulé individuellement par une impulsion RF bien choisie. Par ailleurs les spins des différents noyaux de la molécules sont couplés, et la fréquence de résonance d'un spin peut dépendre de l'état des spins voisins. On peut donc ainsi réaliser des transformations conditionnelles des spins, ce qui est l'ingrédient de base des portes quantiques. Il est à noter que les expériences sont faites sur un échantillon macroscopique, c'est-à-dire sur 10^{23} ordinateurs en même temps [38, 39]. Il faut cependant mentionner qu'un débat s'est récemment ouvert sur le fait que ces expériences reposent sur une distribution statistique, qui ne correspondraient pas à une véritable intrication.

Boîtes quantiques. Dans le domaine de l'information quantique, les résultats expérimentaux en physique du solide n'ont pas encore la maturité atteinte en RMN ou en optique quantique. Cependant les capacités technologiques actuelles en nanoélectronique laissent présager des progrès rapides, avec notamment une perspective d'intégration des qubits à grande échelle que n'ont pas ses concurrents. De nombreuses propositions sont apparues récemment pour la réalisation de qubits avec des états électroniques ou des états de spin, notamment avec des boîtes quantiques semi-conductrices. Le contrôle cohérent d'état électronique de boîtes quantiques individuelles a

été démontré [40]. Les recherches s'effectuent dans plusieurs directions. La première étape, outre la réalisation de qubits à partir de différents systèmes à 2 niveaux (nanostructures isolées, nanostructures couplées) [41], consistera à contrôler et effectuer des rotations de qubits. Ceci s'effectuera notamment par adressage individuel optique en utilisant des techniques de champ proche. Une étape primordiale sera d'observer et de contrôler les interactions entre qubits, en insérant par exemple les qubits dans des cavités [42, 43]. Un accent particulier sera également porté sur les effets de cohérence. Dans le domaine de la cryptographie, l'utilisation de nanostructures semi-conductrices comme sources à 1 photon ainsi que les effets non-linéaires pour la génération paramétrique de photons jumeaux seront étudiés.

Nanojonctions. Une nanoélectrode supraconductrice connectée à un réservoir par une jonction Josephson constitue un système à deux niveaux sur lequel il a été possible d'observer des oscillations de Rabi [44]. Les études sur les nanojonctions supraconductrices s'articulent actuellement autour de quatre domaines de recherche : La réalisation de circuits quantiques à base de nanojonctions Josephson, le développement de techniques de mesures des états quantiques, l'analyse de la décohérence [45] et finalement le développement de techniques impulsionnelles précises pour commander les qubits.

L'ordinateur quantique est à l'heure actuelle un Graal dont il est difficile de pronostiquer l'avènement. Mais les défis auxquels il faut faire face amènent à se poser des questions fondamentales comme la transition entre les mondes classiques et quantiques, et à proposer des solutions technologiques radicalement innovantes.

References

[1] C. H. Bennett & D. P. DiVincenzo, Nature, *Quantum information and computation* **404**, 247 (2000).

[2] P. W. Shor, Proccedings of the 35th annual Symposium on the fondations of computer science, p. 124 (IEEE Computer Society Press, Los Alamitos, California, 1994).

[3] J. M. Merolla, Y. Mazurenko, J. P. Goedgebuer, & W. T. Rhodes, *Single-photon interference in sidebands of phase-modulated light for quantum cryptography* Phys. Rev. Lett. **82**, 1656 (1999)

[4] A. Muller, H. Zbinden & N. Gisin, *Quantum cryptography over 23 km in installed under-lake telecom fibre*, Europhysics Lett. **33**, 335 (1996).

[5] W. T. Buttler, R. J. Hughes, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt & C. G. Peterson, *Daylight quantum key distribution over 1.6 km*, Phys. Rev. Lett. **84**, 5652 (2000).

[6] C. H. Bennett & G. Brassard, Proceedings of the International Conference on Computer Systems and Signal Processing, Bangalore, 1984, p. 175.

[7] N. Lütkenhaus, *Estimates for practical quantum cryptography*, Phys. Rev. A **59**, 3301 (1999).

[8] J. Kim, O. Benson, H. Kan & Y. Yamamoto, *A single photon turnstile device*, Nature **397**, 500 (1999)

[9] C. Brunel, B. Lounis, P. Tamarat & M. Orrit, *Triggerred source of single photons based on controlled single molecule fluorescence*, Phys. Rev. Lett. **83**, 2722 (1999).

[10] C. Kurtsiefer, S. Mayer, P. Zarda & H. Weinfurter, *Stable solid state source of single photon*, Phys. Rev. Lett. **85**, 290 (2000)

[11] R. Brouri, A. Beveratos, J.-Ph. Poizat & Ph. Grangier, *Photon antibunching in the fluorecence of individual colored centers in diamond* à paraître dans Opt. Lett.

[12] A. Ekert, *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett. **67**, 661 (1991).

[13] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter & A. Zeilinger, *Quantum cryptography with entangled photons*, Phys. Rev. Lett. **84**, 4729 (2000).

[14] D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglung & P. G. Kwiat, *Entangled state quantum cryptography: eavesdropping on the Ekert protocol*, Phys. Rev. Lett. **84**, 4733 (2000).

[15] W. Tittel, J. Brendel, H. Zbinden & N. Gisin, *Quantum cryptography using entangled photons in energy-time Bell states*, Phys. Rev. Lett. **84**, 4737 (2000).

[16] A. Furusawa, J. L. Sorensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, E. S. Polzik, *Unconditional quantum teleportation*, Science, **282** 706 (1998).

[17] C. A. Sackett et al, *Experimental entanglement of four particles*, Nature **404**, 256 (2000).

[18] John Preskill, *Quantum Information and Computation*, http://www.theory.caltech.edu/people/preskill/ph229/index.html

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

[20] A. Steane, *Multiple particle interference and quantum error correction*, Proc. R. Soc. Lond. A, **452**, 2551 (1996).

[21] A. Calderbank & P. Shor, *Good quantum error-correcting codes exist*, Phys. Rev. A, **Vol. 54**, 1098 (1996)

[22] B. E. Kane *A silicon-based nuclear spin quantum computer*, Nature **393**, 133 (1998).

[23] J. I. Cirac & P. Zoller, *A scalable quantum computer with ions in an array of microtraps*, Nature **404**, 579 (2000).

[24] J. I. Cirac & P. Zoller, *Quantum computation with cold trapped ions*, Phys. Rev. Lett. **74**, 4091 (1995).

[25] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano & D. J. Wineland, *Demonstration of a fundamental quantum logic gate*, Phys. Rev. Lett. **75** 4714 (1995).

[26] D. Jaksch, H.-J. Briegel, J. I. Cirac, C. W. Gardiner & P. Zoller, *Entanglement via cold controlled collisions*, Phys. Rev. Lett. **82**, 1975 (1999).

[27] G. K. Brennen, C. M. Caves, P. S. Jessen & I. H. Deutsch, *Quantum logic gates in optical lattices*, Phys. Rev. Lett. **82**, 1060 (1999).

[28] X. Maître, E. Hagley, G. Nogues, C. Wunderlich, P. Goy, M. Brune, J. M. Raimond & S. Haroche, *Quantum memory with a single photon in a cavity*, Phys. Rev. Lett. **79**, 769 (1997).

[29] S. Haroche, M. Brune & J. M. Raimond, *Experiments with single atoms in a cavity: entanglement, Schrödinger's cats and decoherence*, Phil. Trans. Roy. Soc. **355**, 2367 (1997).

[30] A. Rauschenbeutel, G. Nogues, S. Osnaghi, P. Bertet, M. Brune, J. M. Raimond & S. Haroche, *Coherent operation of a tunable quantum phase gate in cavity QED*, Phys. Rev. Lett. **83**, 5166 (1999).

[31] A. Rauschenbeutel, G. Nogues, S. Osnaghi, P. Bertet, M. Brune, J. M. Raimond & S. Haroche, *Step by step engineered many particle entanglement*, Science **288**, 2024 (2000).

[32] Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi & H. J. Kimble, *Measurement of conditional phase shifts for quantum logic*, Phys. Rev. Lett. **75**, 4710 (1995).

[33] T. Pellizzari, S. A. Gardiner, J. I. Cirac & P. Zoller, *Decoherence, continuos observation and quantum computing: a cavity QED model*, Phys. Rev. Lett. **75**, 3788 (1995).

[34] C. J. Hood, T. W. Lynn, T. W. Doherty, A. S. Parkins & H. J. Kimble, *The atom-cavity microscope : single atoms bound in orbit by single photons*, Science **287**, 1447 (2000).

[35] P. W. H. Pinkse, T. Fisher, P. Maunz & G. Rempe, *Trapping an atom with single photons*, Nature **404**, 365 (2000).

[36] I. L. Chuang, L. M. K. Vandersypen, X. Zhou, D. W. Leung & S. Lloyd, *Experimental realization of a quantum alogorithm*, Nature, **393**, 143 (1998).

[37] I. L. Chuang, N. Gershenfeld & M. Kubinec, *Experimental implementation of fast quantum searching*, Phys. Rev. Lett. **80**, 3408 (1998).

[38] D. G. Cory, A.F. Fahmy & T. F. Havel, *Ensemble quantum computing by nuclear magnetic resonance spectroscopy*, Proc. Natl. Acad. Sci. USA **94**, 1634 (1997).

[39] N. A. Gershenfeld & I. L. Chuang, *Bulk spin resonance quantum computation*, Science **275**, 350 (1997).

[40] N. H. Bonadeo, J. Erland, D. Gammon, D. Park, D. S. Katzer & D. G. Steel, *Coherent optical control of the quantum state of a single quantum dot*, Science **282**, 1473 (1998)

[41] G. Burkard, D. Loss & D. P. DiVicenzo, *Coupled quantum dots as quantum gates*, Phys. Rev. B **59** 2070 (1999).

[42] M. S. Sherwin, A. Immamoglu, & T. Montroy, *Quantum computation with quantum dots and terahertz cavity quantum electrodynamics*, Phys. Rev. A **60**, 3508 (1999).

[43] A. Immamoglu, D. D. Awschalom, G. Burkard, D. P. DiVicenzo, D. Loss, M. Sherwin & A. Small, *Quantum information processing unsing quantum dots spins and cavity QED*, Phys. Rev. Lett. **83**, 4204 (1999).

[44] Y. Nakamura, Yu. Pashkin & J. S. Tsai, *Coherent control of macroscopic states in a single-Cooper-pair box*, Nature **398**, 786 (1999).

[45] J. R. Friedman, V. Patel, W. Chen, S. K. Tolpygo & J. E. Lukens, *Quantum superposition of distinct macroscopic states*, Nature **406**, 43 (2000).