

CALGARY, ALBERTA | JUILLET 2017

# **ATELIER DE L'ICRA SUR LES RÉSEAUX QUANTIQUES**

# SOMMAIRE EXÉCUTIF

Cet atelier de deux jours a réuni des boursiers de l'ICRA du programme Informatique quantique et des chefs de file du milieu universitaire, de l'industrie et du gouvernement pour discuter, à travers la lorgnette de la recherche et du développement, des progrès à ce jour, des obstacles principaux et des possibilités futures relativement au développement de répéteurs quantiques et de leur intégration à des réseaux quantiques à grande échelle. Les présentations, avec conférenciers invités, ont mis l'accent sur les percées scientifiques les plus récentes et sur des problèmes ouverts. Parmi les sujets abordés, notons : applications, protocoles, composants, interfaces et stratégie de création de partenariats avec l'industrie et d'autres parties prenantes.

À la base d'une discussion sur les réseaux quantiques se trouve la perspective que grâce à des efforts considérables de chercheurs universitaires et de joueurs de l'industrie (par exemple, Google, IBM, Microsoft, D-wave), les ordinateurs quantiques (OQ) deviendront réalité dans un proche avenir. Cela scinde les applications des réseaux quantiques en trois catégories : la première cherche à surmonter les problèmes de sécurité créés par les OQ (par exemple, distribution quantique de clés [DQC], partage de secret, etc.), la deuxième cherche à exploiter les capacités exceptionnelles des OQ (comme l'infonuagique quantique, le calcul quantique aveugle, etc.) et la troisième se penche sur l'amélioration des mesures grâce à la mécanique quantique. Dans ces divers contextes, il est important de noter les facteurs suivants : a) les méthodes fondées sur les mathématiques, qui protégeraient la vie privée contre les OQ, suscitent plus de soutien actuellement que la cryptographie quantique et b) la possibilité de lier des unités modulaires de calcul quantique fait déjà l'objet de recherches dans la communauté des OQ, par exemple, pour surmonter les contraintes physiques dans les réfrigérateurs à dilution.

Selon la distance et l'environnement, les liaisons quantiques qui forment un réseau quantique se composent probablement de différents types de canaux, comme des liaisons satellitaires en espace libre et des liens terrestres, ainsi que des liens par fibre optique. Ces dernières années, la capacité des liaisons satellitaires et terrestres a augmenté rapidement et des chercheurs canadiens sont au premier plan de ces avancées. Pour de longues distances, il faut des répéteurs quantiques avec des liaisons par fibre optique, possiblement avec des protocoles différents. Par exemple, des protocoles basés sur des variables discrètes ou continues où chacun comporte des avantages et des défis.

Les composants individuels d'un réseau se trouvent à des niveaux différents de maturité et de qualité. Les sources à photon unique basées sur une conversion paramétrique descendante spontanée d'un mélange à quatre ondes sont extrêmement fiables, mais souffrent d'un compromis entre le débit et la pureté. Les sources à émetteur unique, comme les points quantiques et les centres colorés du diamant, ont évolué rapidement ces dernières années, mais il demeure des problèmes techniques à surmonter, comme l'accroissement de l'efficacité de couplage, de la stabilité spectrale et du rendement. Les sources à émetteur unique haute efficacité qui fonctionnent dans le spectre des télécommunications, quoique hautement souhaitables, restent à démontrer. Comme les points quantiques ont atteint un certain niveau de maturité, le développement de démonstrateurs prêt-à-brancher favoriserait considérablement l'accélération de la mise en œuvre de ces sources dans des bancs d'essai de réseaux quantiques.

La disponibilité de détecteurs supraconducteurs rapides et efficaces – même sur le marché commercial – a éliminé les limitations relatives à la longueur d'onde des photodétecteurs à avalanche utilisés précédemment, facilitant ainsi l'utilisation de photons dans le spectre des télécommunications. L'autre défi à relever est l'incorporation de la détection de degrés de liberté multiplexeurs, par

exemple, des détecteurs à résolution spectrale. Le développement d'une mémoire quantique adéquate – basée à la fois sur des émetteurs uniques (comme des centres NV) et des ensembles (cristaux dopés avec des ions de terres rares) – constitue encore un défi, car aucune mémoire fonctionnelle actuelle ne répond à toutes les valeurs de référence souhaitables pour un répéteur ou un réseau quantique. Les transducteurs quantiques qui établissent un lien entre des états quantiques à encodage optique et des qubits micro-ondes utilisables dans des OQ supraconducteurs constituent le composant le moins mature. Plusieurs approches sont utilisées actuellement et celles qui se fondent sur les oscillateurs nanomécaniques mènent le bal. Toutefois, aucun système n'a encore démontré la transduction au niveau quantique. Il est probable que les transducteurs constitueront le composant le plus limitatif sur le plan de la largeur de bande dans un réseau. Nous notons que les plateformes d'OQ qui se basent entre autres sur des ions piégés et des points quantiques possèdent des transitions optiques et éliminent en conséquence le besoin d'un transducteur.

Un des problèmes organisationnels est qu'il y a trop peu d'incitatifs pour s'attaquer à des problèmes techniques, optimiser les composants pour satisfaire toutes les exigences (ne pas exceller seulement dans une exigence), et développer et analyser des systèmes complets (et intégrés). Pour éliminer cet obstacle, il serait utile de favoriser une plus grande collaboration et la création de bancs d'essai où des chercheurs de compétences différentes peuvent se réunir. De plus, les bancs d'essai sont une bonne façon de mettre en vedette la recherche auprès de l'industrie, des décideurs et du public. Il est important de sensibiliser les gens à la perspective de la création d'emploi et de nouvelles entreprises. Un bon exemple est la nouvelle initiative phare sur les technologies quantiques en Europe (European Quantum Technology Flagship Initiative). L'initiative Quantique Canada, de concert avec les forums connexes, explore actuellement une approche similaire au Canada.

L'industrie peut être une source d'investissements et de marchés pour les technologies mises au point par les chercheurs et servir de levier pour l'établissement de liens entre les chercheurs et les décideurs gouvernementaux. Mais pour que le secteur privé participe au développement des réseaux quantiques, la communauté universitaire de la recherche et l'industrie doivent apprendre à travailler ensemble et favoriser une compréhension mutuelle des objectifs et des problèmes des uns et des autres. Des entités comme le Consortium photonique de l'industrie canadienne pourraient jouer un rôle important, de concert avec des organisations intermédiaires et des bureaux de liaison université-industrie. Il se peut qu'il manque à l'écosystème de financement du Canada un élément pour permettre l'innovation stratégique et d'avant-garde (similaire à DARPA aux É.-U.) ou une entité qui incubera et financera de jeunes entreprises dans l'espace de la technologie quantique. De plus, le gouvernement a un rôle important à jouer comme premier adoptant de nouvelles technologies quantiques, par exemple des liens de communications à protection quantique. Cela offrirait un incitatif au développement d'un écosystème industriel.

Pour faire d'un réseau quantique une proposition véritablement convaincante auprès des décideurs et du public, nous devons formuler une vision grandiose simple et claire comme celle qui a mené à la conquête de la Lune. Cette vision peut présenter un seul objectif clair et captivant, comme La téléportation d'un océan à l'autre, fondée sur des technologies qui recèlent une valeur commerciale et stratégique pouvant susciter l'intérêt de l'industrie et du gouvernement. Comme la protection de la vie privée en ligne revêt de plus en plus d'importance pour le public, nous pourrions aussi utiliser un terme comme la transformation de la cybersécurité. Il importe d'avoir un message qui projette les possibilités envisagées et qui ne se fonde pas sur des termes techniques. Nous devons souligner l'importance d'investir sans tarder et aborder la question de la gestion du risque dans un monde futur où les ordinateurs quantiques seront largement accessibles.

# SOMMAIRE DES SÉANCES EN ATELIER ET DES DISCUSSIONS

## Séance 1 présidée par Ben Sussman avec des présentations de Zac Dutton et Alexandre Blais

Une perspective guide toutes les discussions sur les réseaux quantiques : nous réussirons à construire des ordinateurs quantiques (OQ). Conséquemment, un réseau quantique devrait i) pouvoir mettre en lien de tels OQ et ii) offrir un mécanisme de protection des communications fondé sur des principes physiques qui serait autrement compromis lors de l'utilisation de protocoles de chiffrement vulnérables aux OQ.

Si l'on commence par le deuxième point ii), des réseaux DQC existent déjà à plusieurs endroits. Un défi futur est d'accroître les distances avec les répéteurs quantiques. Il existe différents protocoles et méthodes, mais les progrès dépendent de la résolution de défis techniques associés à l'amélioration du rendement des composants. Il importe de noter qu'il y a actuellement une nette préférence au sein de la communauté des normes cryptographiques pour les protocoles de chiffrement fondés sur les mathématiques (comme le chiffrement à base de réseaux), quoiqu'il est difficile d'imaginer que l'on puisse prouver leur efficacité contre des attaques d'OQ.

En ce qui concerne le premier point i), il faut communiquer plus clairement les arguments en faveur de la mise en réseau. L'argument le plus fondamental est que les ordinateurs quantiques en réseau pourraient se révéler

considérablement plus puissants que des OQ individuels. De plus, un réseau quantique permettrait toute une gamme d'algorithmes quantiques de protection de la vie privée, mais il n'y a pas encore d'arguments convaincants pour expliquer pourquoi quelqu'un en aurait besoin. D'un point de vue pratique, certains chercheurs, comme R.J. Schoelkopf et M. Devoret, C. Monroe et J. Kim, travaillent à des architectures d'OQ modulaires avant tout en raison de la capacité restreinte d'accommoder des qubits supraconducteurs dans un réfrigérateur à dilution ou des ions dans un piège. De tels modules dans un espace réduit (contenant de 10 à 1000 qubits) seraient connectés à l'aide de photons micro-ondes ou optiques, ce qui ouvre la voie à l'interconnexion d'OQ distants.

La discussion qui a suivi cette séance a aussi porté sur la précision des avantages de la connexion d'OQ en réseaux. Quoiqu'il existe des propositions intéressantes pour la détection quantique distribuée, il n'y a pas encore d'arguments convaincants en faveur de la construction d'un réseau quantique. Le secret sera de plus en plus important dans de nombreuses applications de détection. Toutefois, cette question tourne encore une fois autour d'une application de communication protégée.

## Séance 2 sur les protocoles des répéteurs quantiques présidée par Zac Dutton avec des présentations de Christoph Simon et Alexander Lvovsky

Une architecture par liaison quantique dépendra de la distance qu'elle comble. Pour de courtes distances (<500 km), il y aurait des liaisons terrestres directes (peut-être avec des noyaux fiables); pour les distances intermédiaires (500

à 2000 km), il faudrait des répéteurs quantiques (RQ) terrestres; pour les distances nationales et continentales (1000 à 5000 km), il faudrait des satellites en orbite basse terrestre; alors que pour les distances intercontinentales, il

faudrait des satellites géostationnaires ou des architectures de répéteurs quantiques avec des liaisons satellitaires. Comme les liaisons satellitaires requièrent des récepteurs dans des emplacements de faible luminosité (c'est-à-dire, éloignés), il faudrait ajouter des liaisons terrestres (répéteurs) jusqu'à des centres urbains.

Un répéteur quantique (RQ) permet la distribution efficace de l'intrication sur une longue liaison en distribuant d'abord l'intrication sur plusieurs sous-liaisons plus courtes. En ayant recours à l'échange d'intrication, il est possible de partager l'intrication entre les nœuds d'extrémité de toute la liaison. Il y a un certain nombre de distinctions en ce qui concerne les protocoles de RQ.

Une première distinction est de savoir si les erreurs dans les états des qubits transmis - erreurs découlant soit de la perte de qubits pendant la transmission ou pendant une opération éventuelle de purification dans les nœuds - sont corrigées par un signal d'annonce (heralding) (post-sélection) ou à l'aide de codes de correction d'erreurs. La deuxième option est en principe plus rapide, mais requiert de très courtes distances de sous-liaisons, car elle tolère seulement une perte de 50 pour cent entre les nœuds. De plus, cette option nécessite des grilles de qubits haute fidélité. La première option est plus robuste contre les pertes et les erreurs, mais requiert une communication bidirectionnelle et une mémoire quantique avec des durées de stockage comparativement longues.

Une deuxième distinction est de savoir si le protocole utilise i) des variables discrètes (photons uniques) ou ii) des variables continues pour encoder l'information quantique.

i) Un RQ à variables discrètes peut tolérer une assez grande quantité de perte et d'erreurs. Beaucoup de recherches théoriques ont été menées sur le sujet qui fait maintenant l'objet de nombreuses initiatives expérimentales. Pour les protocoles qui utilisent la mémoire quantique, il est possible d'utiliser des systèmes émetteurs-absorbeurs uniques, comme des

atomes neutres dans des cavités à haute finesse, des ions piégés et des centres NV. Il est aussi possible d'utiliser des absorbeurs-émetteurs basés sur des ensembles, comme des vapeurs atomiques chaudes ou froides et des ensembles à l'état solide. Nous présenterons plus en détail les centres NV et les ensembles d'ions de terres rares dopés dans des cristaux dans la séance sur les composants.

ii) Les protocoles à variables continues permettent des mesures de l'état de Bell (Bell-state measurement, BSM) avec une efficacité unitaire. Toutefois, il faut la quasi-perfection en matière de préparation d'état et de mémoire quantique. Différents protocoles existent, comme ceux basés sur des états « chat de Schrödinger » et des états-EPR.

Pour favoriser l'évolution des répéteurs quantiques, il faudrait démontrer la suprématie quantique, c'est-à-dire un cas où le répéteur fait mieux (par ex., sur le plan du débit de clés secrètes) que la meilleure transmission directe de qubits.

Dans la discussion qui a suivi, il a été mentionné qu'un facteur limitatif pour le RQ à variable discrète est le BSM avec une efficacité de 50 pour cent. Il est possible en principe d'augmenter cette valeur à 100 pour cent à l'aide de photons auxiliaires ou, par ex., d'un processeur quantique à base de qubits supraconducteurs. Toutefois, si ce processeur requiert un transducteur pour convertir un qubit à encodage optique en un qubit de processeur, cela pourrait accroître les pertes ou entraîner des limitations de la largeur de bande. Il se peut que différentes configurations de réseau soient optimales pour différentes applications.

Un certain nombre de suggestions ont été formulées sur la façon de couvrir les frais totaux de la construction d'un réseau quantique. Premièrement, il y a la possibilité de faire de l'essaimage d'entreprise grâce aux technologies découlant des recherches, mais avec des applications dans des domaines éventuellement complètement différents (par ex., Montana Instruments et S2-corp à Bozeman, Montana). Deuxièmement, il est possible de réduire les

coûts associés au réseau en exploitant les infrastructures existantes (comme les réseaux de fibre optique) si la coexistence est possible, c'est-à-dire que cela entraîne le moins de perturbations possible pour les infrastructures existantes (par ex., communications classiques). Troisièmement, il faut envisager que le coût de l'échec, c'est-à-dire une violation de la sécurité, pourrait se révéler suffisamment important pour justifier même un système de communications protégées coûteux.

Les défis techniques ne sont pas toujours valorisés au sein de la communauté de la science quantique et cela constitue un obstacle au progrès, car certains problèmes d'optimisation importants ne sont pas résolus. Il est nécessaire de susciter une plus grande collaboration et de plus amples travaux dans l'atteinte d'un but commun. Pour favoriser de tels développements, il serait très utile d'avoir des réseaux quantiques de démonstration financés par le gouvernement.

## Séances 3 et 4 sur les composants présidées par Michal Bajcy avec des présentations de Rob Thew, Dan Dalacu, Paul Barclay, Andy Sachrajda, Daniel Oblak, Charles Thiel et Thomas Jennewein (de la Séance 5)

**Une vaste gamme de composants ont été mentionnés, notamment :** sources, mémoires, canaux et détecteurs/mesures de photons optiques, et processeurs de qubits. Il est possible d'adapter plusieurs des systèmes présentés pour qu'ils fonctionnent comme des composants différents.

**Sources :** On regroupe les sources de photons uniques et intriqués en deux grands types, soit les types probabilistes et déterministes. Dans le type probabiliste, on retrouve la conversion paramétrique descendante spontanée (spontaneous parametric down-conversion, SPDC) et le mélange à quatre ondes (four-wave mixing, FWM) qui excellent en matière de fiabilité, d'accordabilité et d'indiscernabilité des photons émis (tel que requis pour les mesures d'interférence à deux photons dans les répéteurs quantiques). Ces deux méthodes souffrent principalement d'émissions non nulles et de paires de photons multiples qui peuvent être en partie supprimées par divers processus de rehaussement de la mémoire ou de multiplexage.

En tant que source de photons uniques, les points quantiques ont connu des améliorations considérables dans les dix dernières années et, pour une pureté donnée, ils peuvent maintenant atteindre des débits plus élevés comparativement aux sources de photons

uniques annoncés basées sur la SPDC. Un problème important — causé par la diffusion spectrale, l'instabilité de la synchronisation et le couplage avec les phonons — est l'obtention d'une bonne indiscernabilité des photons émis de sources différentes. Finalement, on mentionne rarement quel est le rendement expérimental, c'est-à-dire, quelle fraction des points quantiques testés possède réellement des propriétés similaires à celles présentées dans les articles scientifiques. Des paires de photons intriqués — habituellement en polarisation — peuvent être générées à partir de points quantiques à l'aide d'un processus de relaxation biexcitonique. Les défis à relever dans l'obtention d'états intriqués haute fidélité sont la distribution énergétique de l'échange anisotrope et ceux mentionnés ci-dessus pour l'émission de photons uniques. Ce n'est que récemment qu'une violation de l'inégalité de Bell a été démontrée pour des sources de paires intriquées basées sur les points quantiques.

Les centres colorés du diamant, comme les centres azote-lacune et les centres silicium-lacune, sont aussi des candidats intéressants comme sources de photons uniques. À des températures cryogéniques, les centres colorés affichent des transitions optiques étroites à couplage fort. La collecte efficace de photons dans un mode spatial bien défini a été grandement facilitée par la lentille à immersion

solide. La probabilité d'émissions dans la raie à zéro phonon est faible dans les centres NV, mais plus grande pour les centres SiV. Il est possible d'améliorer la sélection en mode spectral et spatial par l'action de l'effet Purcell sur le couplage d'un centre coloré avec la cavité. D'ailleurs, plusieurs groupes de recherche se penchent sur cette question. Il importe de noter qu'il est possible de concevoir des sources de paires de photons intriqués à partir d'ensembles de sources de photons uniques indiscernables (efficaces) et indépendants.

**Canaux de transmission :** Différents canaux de transmission — par ex., câbles de fibre optique en espace libre — des qubits optiques présentent divers défis pour la collecte et la détection de qubits. Dans un répéteur quantique, l'échange d'intrication se produit en réalisant une mesure de l'état de Bell où les photons en jeu doivent être indiscernables. Conséquemment, en plus de l'indiscernabilité des photons émis par les sources, il faut compenser pour toute perturbation pendant la transmission. Un tel contrôle précis de la polarisation, du chronométrage, de la fréquence et des modes spatiaux a été démontré pour la transmission par fibre optique longue distance, mais demeure un défi pour la transmission en espace libre.

Les liaisons basées sur la transmission en espace libre ne requièrent pas nécessairement de répéteurs, car la perte, en l'absence de l'absorption atmosphérique, n'augmente que quadratiquement (et non pas exponentiellement, comme c'est le cas avec la fibre optique) avec la distance en raison de la divergence du faisceau. Parmi les défis, notons la lumière de fond (que l'on peut éliminer en plaçant des récepteurs terrestres à plus de 20 km environ de tout centre urbain et en exploitant la liaison la nuit), et le mouvement rapide et l'intermittence du satellite (ce qui peut, en partie, être résolu par des systèmes de poursuite d'avant-garde et des satellites géostationnaires, ou un grand nombre de satellites en orbite basse). Les problèmes principaux sont les fluctuations imprévisibles et rapides du mode spatial en raison de la turbulence atmosphérique.

Les systèmes de liaisons satellitaires se divisent en deux catégories : i) configuration descendante où une source de paires de photons sur un satellite fait une transmission à des récepteurs terrestres, entraînant leur intrication, et ii) configuration ascendante, où se fait une mesure de l'état de Bell sur le satellite en tant qu'élément d'une liaison de répéteur quantique ou pour faire une DQC indépendamment d'un appareil de mesure. Toutefois, les chercheurs n'ont pas encore réussi à réaliser expérimentalement une mesure de l'état de Bell avec des photons qui ont voyagé dans des canaux en espace libre.

À l'échelle mondiale, la course spatiale quantique s'intensifie et des groupes chinois et singapouriens ont lancé de l'équipement spatial dans l'espace, et les Chinois ont réussi à établir une liaison descendante quantique avec deux stations terrestres. De plus, plusieurs expériences de validation de principe ont démontré divers aspects d'un système satellitaire. Au Canada, le gouvernement fédéral a annoncé récemment le financement d'un projet de communication satellitaire dont on prévoit le lancement dans trois à quatre ans. La charge utile du satellite est conçue pour une configuration à liaison ascendante ce qui procurera davantage de souplesse pour des études expérimentales. Par exemple, il est possible d'utiliser différents types de sources aux stations terrestres. À long terme, le scénario idéal serait un satellite avec une source intriquée et une mémoire quantique embarquée de longue durée, ce qui permettrait de connecter n'importe quelles deux stations terrestres que survolerait le satellite.

**Détecteurs :** Jusqu'à tout récemment, les détecteurs à photons uniques (single photon detectors, SPD) se basaient habituellement sur des diodes de photodétecteurs à avalanche qui affichent de bonnes propriétés (efficacité et bruit de comptage) dans le spectre visible, mais qui présentent un rendement nettement inférieur pour le spectre des télécommunications, soit 1550 nm. Cela a orienté de nombreuses démonstrations expérimentales et entraîné l'exclusion des

photons de télécommunications des systèmes satellitaires. En raison de l'amélioration considérable et de la commercialisation des détecteurs supraconducteurs, comme les détecteurs TES (transition-edge-sensors) et les détecteurs à nanofils supraconducteurs (superconducting nano-wire detectors, SNPSD), il est possible de détecter efficacement les photons du spectre des télécommunications. Les détecteurs en réseaux de pointe peuvent surmonter certains des autres problèmes, comme l'instabilité de la synchronisation et les temps morts, mais requièrent des systèmes de lecture plus efficaces, comme la lecture multiplex de détecteurs à inductance cinétique (kinetic inductance detectors, KID).

Une autre considération concerne l'architecture de répéteurs quantiques multiplexeurs. Dans ce cas, les détecteurs (et les mesures de l'état de Bell) doivent pouvoir restituer les signaux (démultiplexer) qui arrivent dans des modes différents. Actuellement, les détecteurs réussissent à distinguer avec efficacité seulement les modes temporels (en particulier si les temps morts sont réduits, par ex., en utilisant des réseaux), mais pas les modes dans le domaine spectral. Conséquemment, le démultiplexage doit se produire avant le détecteur, c'est-à-dire par le recours à des filtres spectraux, ce qui ajoute aux pertes et à la complexité.

**Mémoire quantique :** La mémoire quantique fait maintenant partie intégrante de nombreux systèmes. On peut distinguer les mémoires en fonction de leur mode de fonctionnement : i) émission d'un photon qui est intriqué avec l'état (de longue durée) interne de la mémoire ou ii) cartographie réversible d'un signal optique dans son parcours vers la mémoire et à partir de celle-ci. Dans cette séance, les participants ont parlé de deux types de matériaux spécifiques.

Premièrement, les centres colorés du diamant pour le premier type de mémoire ci-dessus sont utilisés actuellement pour tenter de construire un réseau quantique aux Pays-Bas et plusieurs étapes essentielles dans ce processus ont été démontrées ces dernières années. À des

températures cryogéniques, les centres NV ont de longs temps de cohérence de spin (plusieurs secondes à 77 K) et, même à température ambiante, le temps peut être d'environ 30 ms. Un obstacle majeur est la faible efficacité de collecte de la lumière émise (limitée, par exemple, par une faible probabilité d'émissions dans la raie à zéro phonon). Toutefois, comme il a été discuté dans le contexte de sources de phonons uniques, plusieurs initiatives expérimentales portent sur cette question.

Deuxièmement, les cristaux dopés par des ions de terres rares possèdent plusieurs propriétés clés grâce auxquelles ceux-ci se révèlent utiles pour la mémoire quantique et d'autres tâches de traitement quantique. Plus spécifiquement, ils peuvent afficher de très longs temps de cohérence – jusqu'à plusieurs millisecondes avec des transitions optiques et plusieurs heures avec des transitions de spin – ce qui permet un stockage optique transférable à des transitions de spin. L'existence de niveaux avec une longue durée de vie (shelving state) permet l'adaptation spectrale, comme il est nécessaire dans de nombreuses mémoires quantiques avec écho de photon. L'amélioration d'ensemble mène à des probabilités élevées d'absorption de photons, même en l'absence d'une cavité optique, et l'élargissement non homogène donne lieu à de larges bandes passantes de mémoire et à une capacité de stockage multimodale. Toutefois, l'obtention de toutes les propriétés souhaitées dans un seul cristal est difficile et requiert une compréhension détaillée des mécanismes de décohérence et de couplage. Les systèmes à ions de terres rares sont complexes, même en théorie et, de plus, les paramètres du cristal sont influencés par la pureté, les méthodes et les conditions de croissance, l'environnement post-croissance et des facteurs inconnus. Il est nécessaire de mieux comprendre la dynamique de spin, les fonctions d'ondes électroniques et le désordre microscopique dans les cristaux pour adapter et découvrir de meilleurs cristaux à base d'ions de terres rares.

**Processeurs quantiques :** Un OQ se compose de processeurs d'information quantique. De



plus, un processeur quantique permettrait d'effectuer une mesure de l'état de Bell avec efficacité unitaire dans un répéteur quantique — subordonné à la transduction du qubit optique transmis au degré de liberté et à l'espace des paramètres des qubits du processeur.

En plus des processeurs à base de qubits supraconducteurs mentionnés précédemment, d'autres types, comme les ions piégés et les points quantiques (PQ) peuvent être utilisés comme processeurs. Dans les PQ, on a fait la démonstration de tous les composants nécessaires d'un processeur (grilles, interconnexions et lecture), quoique pas de façon optimale dans un même appareil. Un des avantages exceptionnels est la capacité d'interagir directement avec des signaux optiques, éliminant ainsi le besoin d'un élément de transduction supplémentaire. Les chercheurs ont étudié différents systèmes de PQ relativement aux matériaux semi-conducteurs et à l'espace de qubit (PQ simple, états triplets avec points multiples, etc.) dans le porteur (trou ou électron). On a procédé à l'étude des mécanismes d'interconnexion de régions différentes dans un processeur unique relativement aux ondes

acoustiques de surface (transfert spatial), et au couplage de la charge par l'entremise de cavités ou de superpositions quantiques.

La discussion qui a suivi la séance sur les composants s'est penchée sur les mérites et les difficultés de l'intégration des composants, une tâche fastidieuse entreprise par certains groupes de recherche, par ex., J. O'Brien de l'Université de Bristol. L'intégration contribuerait à la fiabilité et à l'évolutivité des appareils de réseaux quantiques et, idéalement, pourrait réduire les pertes découlant des interfaces. Le couplage et le découplage avec des structures microscopiques constituent un défi, quoique certains groupes semblent maîtriser le processus (par ex., O. Painter) et un couplage évanescent aux appareils pourrait atténuer les pertes. Toutefois, une perte supplémentaire associée à la propagation guidée pose problème. Actuellement, le silicium entraîne le moins de perte, mais il n'est pas propice à toutes les longueurs d'onde. Il est clair que de plus amples recherches sont nécessaires afin de cerner les meilleurs matériaux et conceptions pour la mise au point de composants intégrés.

## Séance 5 sur les interfaces présidées par Christoph Simon avec des présentations de Konrad Lehnert et Nikolai Lauk

Dans le contexte des réseaux quantiques, les interférences font référence à la liaison entre les canaux quantiques longue distance et les processeurs quantiques, comme les qubits supraconducteurs micro-ondes. Si le canal prend la forme d'une liaison par fibre optique, la longueur d'onde tourne autour de 1550 nm (spectre des télécommunications), alors que pour une transmission en espace libre, il y a plusieurs « fenêtres » de longueurs d'onde dans l'atmosphère. Conséquemment, l'interface est un transducteur d'information quantique du domaine optique au domaine micro-ondes. Il importe de noter que, en raison du rayonnement thermique, il est impossible de transmettre des signaux micro-ondes en dehors d'un environnement cryogénique. Les transducteurs quantiques doivent préserver

l'état quantique. Il est possible d'analyser ce phénomène relativement aux paramètres de dispersion intrant-extrant où l'on doit démontrer la préservation du nombre et la bidirectionnalité. On a proposé des transducteurs dans plusieurs systèmes, notamment : atomes froids à proximité de circuits supraconducteurs, convertisseurs électro-optiques optimisés, spins micro-ondes et optiques dans des cristaux (par ex., ions de terres rares), appareils optomécaniques piézoélectriques (par ex., AlN), cristaux optomécaniques, conversion paramétrique descendante et membranes semi-conductrices (par ex., SiN).

La transduction par une membrane SiN fonctionne à l'aide de micro-ondes qui agissent sur un circuit résonant comprenant un capaciteur

formé d'une membrane SiN. Conséquemment, les micro-ondes induisent des oscillations mécaniques dans la membrane qui, à son tour, perturbe un champ de cavité quantique qui est réfléchi de la même membrane. En conséquence, l'énergie est transférée dans des bandes de fréquence latérales du champ optique. Dans un réfrigérateur à dilutions de 100 mK, on a démontré une efficacité de conversion de 20 pour cent avec l'ajout de seulement cinq photons de bruit. Le problème principal est le bruit causé par le fort champ de la pompe optique qui pourrait être résolu par une interaction cohérente forte, sans absolument aucune interaction incohérente.

Pour la transduction basée sur un ensemble, les absorbeurs doivent posséder des transitions dans les spectres optiques et micro-ondes, et faciliter le transfert cohérent entre ceux-ci. Parmi les candidats prometteurs pour la transduction à l'aide d'absorbeurs basés sur un ensemble, notons les centres colorés du diamant et les cristaux dopés par des ions de terres rares. Jusqu'à présent, un certain nombre d'expériences sur les deux types de systèmes ont démontré un couplage fort avec des champs micro-ondes. En ce qui concerne les matériaux de terres rares, certains possèdent des transitions dans le spectre des télécommunications et affichent aussi une combinaison d'élargissement large non homogène et d'élargissement étroit homogène. On a exploité ces propriétés dans une proposition de transducteur mettant en jeu des interactions avec échos de photon.

Lors de la discussion sur les interfaces, l'un des premiers commentaires fut que les qubits supraconducteurs sont difficiles à mettre en réseau, car ils ne possèdent pas de transitions optiques et, en conséquence, les transducteurs sont indispensables. Il y a d'autres choix que les qubits supraconducteurs pour les processeurs, mais il ne faut pas ignorer qu'ils constituent présentement le choix de presque tous les grands joueurs commerciaux.

Un autre commentaire a porté sur l'utilité de mettre l'accent sur la création de composants

qui possèdent de bonnes propriétés d'ensemble pour un réseau quantique, plutôt que de miser sur la conception de composants qui pourraient faire mieux que le nec plus ultra en ce qui concerne une propriété donnée ou quelques-unes.

Subséquent, il a été dit que pour faire d'un réseau quantique une proposition véritablement convaincante auprès des décideurs et du public, la communauté de la recherche quantique doit formuler une vision simple et grandiose comme celle qui a mené à la conquête de la lune. Il a été suggéré de formuler cette vision en évitant l'idée de suprématie par rapport à d'autres pays (comme dans le cas de l'alunissage), mais de se concentrer plutôt sur les applications. L'une des possibilités est de parler de toutes les capacités d'un ordinateur quantique et d'ajouter ensuite l'idée d'un réseau quantique. Il ne faut pas oublier que l'objectif présenté au public était celui d'aller sur la lune, mais que le développement de technologies, comme les fusées, constituait le véritable objectif d'importance et probablement aussi l'objectif stratégique des décideurs. Nous devrions recourir à cette même notion.

Dans la formulation de notre grand objectif, il serait préférable de mettre l'accent sur les problèmes que nous souhaitons résoudre, plutôt que de se concentrer sur des notions quantiques qui sont difficiles à comprendre pour les gens. La téléportation d'un océan à l'autre pourrait être un défi grandiose qui interpelle le public et capte son attention. Le développement d'outils pour la cybersécurité pourrait constituer un argument technologique qui convaincrat les décideurs et ceux-ci pourraient y voir une proposition commerciale intéressante. Toutefois, cela pourrait tout de même se révéler trop technologique pour captiver les gens en dehors des communautés scientifiques et technologiques. Nous pourrions aussi nous inspirer d'autres grands défis actuels, comme la médecine génétique, les changements climatiques et l'élucidation des composants fondamentaux de l'Univers (par ex., LIGO et CERN). Comme la cybersécurité sera un souci croissant pour les gens, cette question pourrait

éventuellement les interpellier. Nous pourrions utiliser la phrase transformer la cybersécurité. Le défi pour les chercheurs, dans la formulation de ces visions, sera de faire le pont entre le langage technique et les possibilités éventuelles.

Il est important de présenter ces recherches de façon stratégique en ce qui concerne la création

d'emplois et les possibilités commerciales. De plus, il faudrait souligner que la résolution de certains des défis techniques pourrait favoriser l'essaimage d'entreprise. Nous devons souligner l'importance d'investir sans tarder et aborder la question de la gestion du risque dans un monde futur où les ordinateurs quantiques seront largement accessibles.

## Séances 6 et 7 présidées par Rob Thew et Alexandre Blais avec des présentations de Robert Corriveau, David Danovich, Dan Gale, Rob Thew et Ben Sussman

Le Consortium photonique de l'industrie canadienne (CPIC) offre une perspective à l'industrie sur la façon de collaborer stratégiquement, et de mettre au point et de cerner des possibilités. Le CPIC découle de l'Institut canadien pour les innovations en photonique dont l'objectif était de soutenir le développement de technologies et de favoriser les investissements en la matière. Cela a mené à la création de plusieurs entreprises. Le CPIC a pour vision d'être un moteur stratégique de l'innovation de l'industrie photonique au Canada et cherche maintenant à « soutenir les entreprises canadiennes afin de les aider à optimiser leurs activités et à améliorer leurs profits en facilitant et en accélérant l'application de technologies photoniques qui améliorent la qualité, la productivité et la rentabilité ». Parmi ses membres, notons des représentants de l'industrie, du milieu universitaire et d'organisations gouvernementales. Une bonne partie de son financement provient du CRSNG. L'appel à propositions du gouvernement du Canada sur les « supergrappes » a mené à une proposition sur la détection, c'est-à-dire la collecte, le traitement et la communication de données.

Une étude importante réalisée par le CPIC a été présentée dans le rapport « Les technologies de la lumière — Un atout économique stratégique » qui décrit et analyse le point de vue de différentes industries sur le rôle de la photonique dans leur secteur. Ce rapport se fonde sur des ateliers pancanadiens portant chacun sur un secteur en particulier (par ex., l'énergie à Calgary) auxquels

des parties prenantes de tous les secteurs ont participé. Pour chaque secteur, le rapport dégage des tendances commerciales, des tendances de l'industrie photonique et cerne les possibilités à saisir pour le Canada, le tout résumé dans un tableau illustrant les forces, les faiblesses, les possibilités et les menaces pour la photonique au Canada.

CMC microsystems est une organisation sans but lucratif à l'interface entre le milieu universitaire et l'industrie, et comprend les possibilités que ces deux milieux présentent l'un pour l'autre, ainsi que les obstacles à la création d'une plus grande synergie. CMC est le créateur et le gestionnaire du Réseau national de conception du Canada. Lors de l'établissement d'une collaboration ou d'un projet conjoint, la première étape est de vérifier s'il y a adéquation entre les objectifs et les attentes des universitaires et de l'industrie en matière d'investissement et de résultats. Par exemple, l'industrie est quelque peu insatisfaite de la signature de lettres de soutien qui ne mènent jamais à des résultats tangibles. De plus, l'industrie fonctionne en fonction de feuilles de route, c'est-à-dire un échéancier et un ensemble de cibles, ce qui est moins fréquent en milieu universitaire. Pour éviter les surprises, il est important de vérifier la disponibilité des ressources et s'il y a des conditions à remplir. Les arrangements juridiques nécessaires doivent être en place. Et l'un des aspects les plus importants d'une collaboration efficace est une bonne communication.

En Europe, l'annonce d'un investissement d'un

milliard d'euros par la Commission européenne a considérablement stimulé la recherche sur les technologies quantiques. Cette initiative n'a pas pris forme du jour au lendemain, mais découle plutôt des efforts dévoués et cohérents de longue date de divers chercheurs depuis la fin des années 1990. Parmi les facteurs clés, notons plusieurs rapports d'étape rédigés et soutenus par une grande partie de la communauté de la recherche quantique au sein de l'Union européenne. Plus tard dans le processus, des joueurs de l'industrie se sont joints à cette initiative, menant à une table ronde déterminante réunissant toutes les parties prenantes, y compris des dirigeants de l'industrie et des membres de la Commission européenne. En mai 2016, tout ce travail a culminé en la création de l'initiative phare sur les technologies quantiques (Quantum Technologies Flagship initiative). Un des éléments importants de la création de cette initiative fut un large processus de consultation auprès de la communauté sur le développement de l'initiative. Le programme de recherche stratégique décrit quatre domaines d'application (communication, calcul, simulation et détection-métrologie) qui comptent tous des éléments de génie-contrôle, logiciel-théorie, éducation-formation, ainsi qu'une base en science fondamentale. Dans un horizon de 3, 6 et 10 ans, l'initiative fixe des buts très clairs, énoncés en fonction des objectifs et non pas en fonction d'une technologie spécifique. Pour mener à bien cette initiative, il est essentiel d'avoir une structure de gestion transparente et de garantir la participation de l'industrie.

La question ultime est de savoir si la communauté de la recherche quantique au Canada occupe la position stratégique nécessaire pour tirer profit de l'expérience, par ex., de l'Europe et d'autres industries en vue de réaliser le plein potentiel de la R. et D. en science quantique. L'initiative Quantique Canada traite de cette question.

Actuellement, le Canada dépense davantage par habitant en recherche quantique (non classifiée) que nombre d'autres pays développés et jouit d'une masse substantielle de chercheurs de renommée mondiale dans ses universités. Pour favoriser les investissements en science quantique, il faut souligner les possibilités d'impact possibles.

On capte souvent cet impact par une triple marge bénéficiaire (sociale + environnementale + économique). Parmi les facteurs qui pourraient dissuader de plus amples investissements, notons : concurrence pour des fonds limités, aucune voix communautaire claire, « analyse de rentabilité » imprécise, et absence de soutien public et politique.

Pendant la discussion, un participant a demandé s'il ne manque pas au Canada une source de financement de l'innovation, par exemple, un DARPA canadien? Il a été mentionné que l'écosystème de financement canadien semble désorganisé aux yeux des gens de l'extérieur. Nous devrions pouvoir nous comparer avec d'autres entités de grandes communautés canadiennes, comme Génome Canada et Nucléaire Canada. Nous devrions susciter la participation de l'industrie et la convaincre du besoin d'investir afin qu'une initiative de réseau quantique au Canada puisse jouir de leur soutien. De plus, il est important d'essayer de comprendre les problèmes qui se posent pour l'industrie.

Le fait d'avoir une entité qui servirait d'incubateur et de bailleur de fonds de jeunes entreprises serait une option/exigence. Il est important de se rappeler que de nombreux essaimage d'entreprise se fondent sur des technologies d'avant-garde développées pour des réseaux quantiques, mais que la vraie mine d'or commerciale se situe probablement davantage du côté d'applications non apparentées. De plus, le gouvernement a un rôle important à jouer comme premier adoptant et premier client de l'industrie, en tant que bailleurs de fonds de démonstrateurs et d'infrastructures essentielles, etc. Une supergrappe pourrait constituer une telle entité qui, à l'avenir, serait en mesure de soutenir une initiative sur les réseaux quantiques.

Une façon efficace de convaincre les décideurs et de diffuser les connaissances auprès du public serait de recourir à des bancs d'essai qui peuvent démontrer la viabilité de la technologie. De plus, les bancs d'essai jouent un rôle important pour encourager le développement de systèmes complets en état de fonctionnement.

## Liste des participants (en ordre alphabétique)

Aimee Park - Institut canadien de recherches avancées	Alex Lvovsky - Université de Calgary
Alexandre Blais - Université de Sherbrooke	Amy Cook - Institut canadien de recherches avancées
Andy Sachrajda - CNR Ottawa	Archana Singh - Western Economic Development
Barry Sanders - Université de Calgary	Ben Sussman - CNR Ottawa
Brent Barron - Institut canadien de recherches avancées	Charles Thiel - Université d'état du Montana
Christoph Simon - Université de Calgary	Dan Dalacu - CNR Ottawa
Dan Gale - CMC Microsystems	Daniel Oblak - Université de Calgary
David Danovitch - Université de Sherbrooke	Nikolai Lauk - Université de Calgary
Konrad Lehnert - JILA	Michal Bajcsy - Université de Waterloo
Paul Barclay - Université de Calgary	Robert Thew - Université de Genève
Robert Coriveau - Consortium photonique de l'industrie canadienne	Thomas Jennewein - Université de Waterloo (jour 2)
Wolfgang Tittel - Université de Calgary	Zachary Dutton - BBN Raytheon (jour 1)
<b>Excuses :</b>	
Cheng-Zhi Peng - Université de sciences et technologie de Chine	Matteo Mariantoni - Université de Waterloo
Rebecca Finlay - Institut canadien de recherches avancées	Stephanie Simmons - Université Simon Fraser
Wenzhou Zhang - Université de sciences et technologie de Chine	