

# Description du projet

## 1-Contexte et objectifs

Ce projet a pour but d’accompagner par une recherche théorique le développement des réseaux quantiques et de leurs usages. Notre ambition est de fournir tous les résultats motivant l’intégration des réseaux quantiques dans les infrastructures existantes. Nous pensons que ce travail permettra à terme d’établir le cahier des charges des futurs réseaux “tout optique”.

Les membres de ce projet contribuent activement par leurs publications et leurs collaborations internationales aux domaines qui constituent ce projet (traitement quantique de l’information, cryptographie, ...). Le LRI et l’INRIA ont par ailleurs une longue tradition d’innovation qui justifie naturellement notre engagement commun dans ce projet.

**Contexte** — Depuis une dizaine d’années, le calcul quantique est un domaine de recherche très actif. Historiquement, c’est en cryptographie que le premier résultat d’informatique quantique est apparu. Il s’agit du protocole de distribution de clés secrètes de Bennett et Brassard [BB84] qui a été prouvé inconditionnellement sûr. Ce premier résultat était à la fois surprenant et motivant. Rappelons qu’en cryptographie classique, la sécurité des schémas de distribution de clés secrètes est fondée sur des tâches supposées difficiles (comme la factorisation de grands nombres ou l’inversion de permutations). Pour le protocole de distribution quantique de clés par contre, la preuve de sécurité s’appuie uniquement sur les principes de la mécanique quantique (comme le principe de non-clonage des états quantiques).

Toutefois c’est l’algorithme de factorisation de Shor [Sho94] qui a sans aucun doute attiré le plus d’attentions et d’efforts de recherche dans cette discipline. Il a montré comment factoriser en temps polynomial de grands entiers à l’aide d’un ordinateur quantique. Naturellement la révolution déclenchée par ces nouvelles perspectives s’est traduite par une recherche internationale de grande qualité et des résultats à sa hauteur : de nouveaux algorithmes ont été découverts ainsi que des protocoles cryptographiques sans équivalent classique (partage de secrets quantiques, chiffrement impossible à copier, téléportation, ...).

Stimulés par ces résultats théoriques, de nombreux groupes expérimentaux se sont orientés vers la réalisation de processeurs quantiques. Une grande variété de systèmes physiques a été retenue pour la construction de prototypes (spins nucléaires, ions piégés, cavités optiques, grilles optiques, électrons dans les semi-conducteurs, ...). Même si beaucoup d’entre eux semblent prometteurs et ont parfois abouti à des ordinateurs quantiques de taille modeste, les difficultés pour obtenir des registres de grande taille sont hors d’atteinte des techniques actuelles. En revanche, en ce qui concerne la cryptographie quantique, l’étape des démonstrations de principe est largement dépassée. En effet, depuis 2 ans la distribution quantique de clés par fibre optique est opérationnelle sur des distances de l’ordre de 100 km [SGG<sup>+</sup>02]. Plusieurs start-up (ID-Quantique, MagiQ) commercialisent déjà des produits basés sur la cryptographie quantique. La phase pré-industrielle a commencé.

Le caractère novateur de la recherche dans ce domaine a conduit à une organisation assez inédite : l’ensemble des laboratoires constituant la tête de pont des technologies quantiques pour l’information ont une composition essentiellement pluridisciplinaire. Ils font collaborer des équipes théoriques aussi bien qu’expérimentales, et savent bénéficier du savoir acquis depuis de longues années sur les algorithmes et protocoles classiques pour les adapter au domaine quantique. Dans la mesure de cette ACI et au regard de l’organisation de ces groupes leader, nous participerons à des collaborations d’envergure avec d’autres équipes à l’étranger (Berkeley, MIT, Los Alamos National Laboratory, Institute for Quantum Computing), tout en tirant parti au mieux du soutien et des connaissances de nos laboratoires respectifs pour ce qui concerne la cryptographie et les algorithmes classiques et quantiques.

Par ailleurs, nous mènerons à bien ce travail en parallèle avec d’autres activités connexes démontrant notre forte implication dans ce domaine. En particulier le LRI est membre du projet RESQ du 5<sup>ème</sup> programme cadre européen. Ce projet rassemble toutes les équipes européennes travaillant sur le traitement quantique de l’information (aspects physiques et informatiques). Par ailleurs, certains d’entre nous sont bénéficiaires de l’ACI cryptologie “Cryptanalyse Quantique” dont le but est de prévoir

quelles seront les conséquences à long terme sur la cryptographie de la construction d'un ordinateur quantique. Ces différents projets participent à une logique commune que nous exploiterons pour favoriser les échanges scientifiques.

Enfin, la diversité des formations (J. Kempe et H. Ollivier ont une formation initiale en physique théorique) et des environnements de travail (INRIA - LRI) permettront à l'ensemble des personnes impliquées de suivre de façon détaillée les développements techniques et conceptuels de la discipline.

**Objectifs** — Au regard du contexte scientifique et des avancés technologiques probables, on peut prédire que, dans un futur proche, nous aurons à disposition des canaux de communication reliés à des processeurs de faible puissance tous deux capables de traiter l'information quantique et par ailleurs connectés aux infrastructures classiques existantes. C'est ce qui constituera les réseaux quantiques de demain.

A l'heure actuelle, nous avons, entre autres, à faire face aux problématiques suivantes :

- la détermination des spécifications requises pour un traitement efficace (sûr et fiable) de l'information quantique au sein de ces réseaux ;
- l'optimisation de l'utilisation de ces structures en terme d'usages ;
- l'interfaçage avec les structures existantes de traitement de données.

Dans ce contexte les membres du projet se proposent d'apporter des éléments nouveaux pour les points suivants :

- La fiabilisation des communications et notamment l'étude de codes correcteurs d'erreurs plus adaptés aux communications à longue distance. Nous envisageons de généraliser les notions de codes convolutifs et de décodage itératif à la protection de l'information quantique.
- Le routage de l'information quantique ainsi que sa robustesse dans ces réseaux, en particulier par une modélisation en terme de marche aléatoire quantique.
- L'amélioration ou l'adaptation au cas quantique d'algorithmes distribués utilisant ces réseaux comme le problème des agendas ou encore le calcul distribué sécurisé dont certaines données doivent être gardées confidentielles (vote électronique, ...).

## 2-Description du projet

Depuis sa découverte au début du XX<sup>ème</sup> siècle, la mécanique quantique n'a cessé de susciter paradoxes et interrogations. Ce n'est que relativement récemment que l'on s'est aperçu que certaines de ses propriétés étranges — enchevêtrement et superposition — pouvaient être astucieusement combinées pour améliorer la complexité d'algorithmes informatiques et de protocoles de communication. Parallèlement, ces propriétés ont été mises en œuvre dans les protocoles cryptographiques quantiques de distribution de clés et en garantissent la sécurité inconditionnelle [BB84]. Ces avancées importantes ont initié une lente mais néanmoins certaine révolution de l'algorithmique et de la communication. La recherche sur les aspects quantiques de ces domaines gagne en importance et la communauté scientifique témoigne d'une intense activité.

Le résultat qui a sans doute le plus marqué et donné son essor à cette discipline est celui de Shor [Sho94], montrant comment factoriser de grands entiers en temps polynomial avec un ordinateur quantique. Ce problème, réputé difficile en informatique classique, est la clef de voûte de nombreux protocoles cryptographiques. Il va sans dire que la construction effective d'un ordinateur quantique aurait entre autres de sérieuses répercussions en cryptographie. Cette supériorité du calcul quantique a été confirmée par une suite d'articles [DJ92, BV97, Sim94, IMS03, FIM<sup>+</sup>03] exhibant des problèmes à oracles pour lesquels les machines de Turing quantiques sont superpolynomialement plus puissantes que leurs analogues probabilistes.

Mis à part le développement d'algorithmes proprement dits, la génération, la distribution et le stockage de l'enchevêtrement sont des tâches cruciales pour l'essor des techniques associées à la communication quantique. Il ne fait plus aucun doute qu'elles seront maîtrisées dans un avenir proche et ce contrairement au développement de l'ordinateur quantique qui requiert des efforts bien plus considérables. Ainsi on a vu dans les dernières années plusieurs démonstrations expérimentales des

protocoles de distribution quantique de clés. Certains groupes, dont le plus représentatif est celui N. Gisin à Genève, ont même atteint une maturité suffisante pour proposer des systèmes commerciaux de cryptographie inconditionnellement sûre basée sur la mécanique quantique. Toutes les recherches expérimentales ont maintenant dépassé le stade de démonstration de principe et travaillent à adapter leurs techniques pour pouvoir fonctionner soit à l'air libre, soit sur les fibres télécom classiques (1550 nm).

On peut donc pronostiquer sans risque que des réseaux de communications quantiques seront disponibles sous peu. Dans un premier temps ils seront certainement dévolus à des applications spécifiques pour lesquelles une confidentialité maximale doit être garantie. Dans un second temps, ils auront la capacité de distribuer de l'enchevêtrement entre leurs différents nœuds, ce qui permettra de les utiliser pour accomplir des tâches de plus en plus complexes.

De nombreux groupes de recherches se sont constitués autour d'une approche multi-thématique regroupant à la fois l'algorithmique, la communication mais aussi la physique quantique. En effet, il est important de rester au contact des physiciens expérimentateurs afin d'être à même de comprendre et de répondre à leurs problèmes par des solutions théoriques nouvelles. Par exemple, le théorème de non-clonage quantique [WZ82] a longtemps semblé rendre impossible tout mécanisme de correction d'erreur pour les états quantiques. Il n'en n'est rien et depuis quelques années un formalisme adapté est à notre disposition [Got97]. Entre autres, il a permis d'établir un seuil d'imprécision en dessous duquel le calcul quantique pourra être stabilisé [Zal96, Aha01]. Cette information est d'importance cruciale car elle permet de juger des efforts à fournir pour parvenir à la construction d'un ordinateur quantique de grande taille. Les algorithmes de correction d'erreurs sont également un élément essentiel dans le développement des réseaux quantiques. En effet, à l'heure actuelle la totalité des expériences se heurte à une barrière fondamentale : le taux d'absorption des photons lors de la communication. Dans le protocole de distribution quantique de clés ceci se traduit par une limitation du débit et de la distance des transmissions. Une étude des codes correcteurs adaptés aux transmissions quantiques à longue distance doit donc être envisagée.

D'autre part ces réseaux posent la question du routage efficace de l'information. Plusieurs options ont déjà été proposées, mais elles sont fondées sur des protocoles classiques de routage (type TCP/IP) et ne profitent pas de l'efficacité quantique. Cependant, l'un d'entre nous a montré que les marches aléatoires quantiques permettraient d'atteindre l'objectif d'un routage entièrement quantique. Un protocole fondé sur ce concept serait intrinsèquement plus efficace que ses analogues classiques. On pourrait alors envisager le transfert d'une information chiffrée par des méthodes quantiques dans un réseau sans avoir à envoyer des informations classiques concernant le routage du paquet, ce qui pourrait éventuellement affecter la sécurité des transmissions.

Par ailleurs, l'interaction entre algorithmique et communication permet de prévoir les nouveaux usages de ces réseaux quantiques. En effet, nous assistons à une intensification de la recherche dans le domaine de la communication quantique et ce principalement grâce à la motivation produite par le déploiement futur de ces réseaux. De nouvelles primitives cryptographiques n'ayant pas de contrepartie classique commencent à être introduites et réclament des études globales en terme de sécurité. Le domaine de l'algorithmique distribuée sur ces réseaux pour calculer des fonctions avec des données confidentielles est également en plein essor.

## Fiabilisation de l'information

L'intérêt de la mécanique quantique pour le traitement de l'information provient principalement de sa linéarité. En effet un bit quantique (qubit) peut non seulement être dans les états  $|0\rangle$  et  $|1\rangle$  mais également dans toute surposition linéaire de ces deux états. Il est donc crucial de conserver ce caractère lors d'un calcul ou d'une transmission de données afin de bénéficier de toutes les capacités du traitement quantique de l'information.

**La décohérence, problème central du traitement quantique de l'information** — Malheureusement dans les systèmes quantiques ouverts, c'est à dire en interaction avec un environnement, les superpositions quantiques sont extrêmement instables [Zur91]. En général, l'interaction avec un

environnement conduit à l'apparition d'une base privilégiée dans laquelle toute superposition quantique est réduite à un banal mélange statistique. Cette réduction s'apparente à la perte de toutes les propriétés qui donnent au traitement quantique de l'information une puissance qui ne peut être égale par son équivalent classique. Ce phénomène est appelé décohérence.

Dans le contexte des réseaux quantiques, les solutions retenues jusqu'à présent consistent à coder l'information dans la polarisation ou encore dans la phase de photons envoyés ensuite sur une fibre optique. Dans bien des protocoles, il faut en outre que les photons soient envoyés individuellement. Ainsi même si les fibres optiques ont de très bonnes propriétés en terme de pertes, les photons ainsi envoyés interagissent fréquemment avec le milieu de propagation ce qui se traduit par des modifications aléatoires de leur polarisation, ou pire par une absorption pure et simple. L'information se trouve donc souvent altérée au cours de la transmission.

Les solutions pratiques visant à contourner cette difficulté sont pour l'heure extrêmement limitées. En effet on ne peut augmenter la puissance d'émission puisqu'il faut toujours envoyer des photons uniques. Par ailleurs, une amélioration des qualités optiques des fibres ne semble pas raisonnable dans le contexte actuel puisque les expérimentateurs ont pris le parti de réaliser leurs prototypes avec des matériels optiques intégrés permettant d'utiliser les réseaux de fibres optiques télécom existants.

Il est donc nécessaire d'apporter à ce problème des éléments théoriques nouveaux, adaptés aux transmissions à longue distance.

**La correction d'erreurs quantiques, une solution pour combattre la décohérence** — La décohérence des états quantiques a tout d'abord été appréhendée d'un point de vue uniquement physique. Ensuite, grâce au développement du traitement quantique de l'information, elle a été formalisée en termes d'erreurs sur un canal de transmission. Ce traitement appelait naturellement à l'utilisation de codes correcteurs. Cependant, la tâche est immédiatement apparue plus complexe qu'à première vue. En effet, dès son apparition, le traitement quantique de l'information a été marqué par un résultat d'importance, le théorème de non-clonage quantique [WZ82]. Il signifie en substance que l'information contenue dans un bit quantique, si elle n'est pas connue à l'avance, ne peut être copiée parfaitement. Ce résultat a longtemps dissuadé les chercheurs d'entreprendre des études sur les codes correcteurs d'erreurs. En effet, il semblait compromettre définitivement toute tentative d'introduire une quelconque redondance dans les messages quantiques afin de les protéger de la décohérence.

Heureusement, il n'en est rien. Depuis 1995 [Sho95], on sait qu'il existe des schémas de correction d'erreurs quantiques. De tels codes correcteurs d'erreurs doivent bien sûr prendre en compte les spécificités de la mécanique quantique. Ainsi leur structure est souvent plus complexe que leurs analogues classiques. Entre autres, le traitement visant à la correction d'erreur doit pouvoir être implémenté de façon linéaire, sans pour autant révéler aucune information sur le message transmis. Le non respect de ce dernier point conduirait à la destruction de l'information quantique initialement codée. Un formalisme permettant d'obtenir de nombreux codes correcteurs d'erreurs quantiques a été développé au cours des dernières années. Il s'agit des codes stabilisateurs [Got97].

Cependant, l'utilisation de tels codes correcteurs d'erreurs est principalement tournée vers la stabilisation du calcul quantique. En effet, ces schémas ont été développés afin de combattre la décohérence au cœur même des processeurs quantiques. Plus précisément, ils permettent de manipuler l'information qu'ils contiennent sans pour autant nécessiter un décodage de cette même information. Par conséquent les propositions actuelles pour construire des ordinateurs quantiques reposent sur la concaténation de nombreux niveaux de codes stabilisateurs. L'information pourrait alors être manipulée par des appareils imprécis sans pour autant mettre en péril les propriétés quantiques assurant la puissance de telles machines. C'est ce qui apparaît dans la littérature sous le nom de calcul quantique tolérant les erreurs (fault-tolerant quantum computing) [Sho96, Ste98].

Du fait de leur champ d'application ces codes correcteurs ne sont pas particulièrement bien adaptés aux transmissions à longue distance. Or, comme nous l'avons déjà dit, les réseaux quantiques nécessitent que de tels schémas soient mis en œuvre rapidement. C'est ce que nous nous proposons de faire. Pour cela nous envisageons d'adapter au formalisme stabilisateur la notion de codes convolutifs.

## Les codes convolutifs quantiques, une solution adaptée aux transferts à longue distance —

Dans le domaine classique, les codes convolutifs sont, et de très loin, les codes les plus utilisés en pratique pour protéger l'information [JZ99, Lee97]. Leur intérêt provient essentiellement de la conjonction des faits suivants :

- un simple registre à décalage permet de réaliser le codage,
- ils peuvent être décodés au maximum de vraisemblance pour tous les modèles de canaux sans mémoire avec un algorithme de faible complexité : l'algorithme de Viterbi.

Ces codes ont pour vocation de réduire le nombre d'erreurs par bit après décodage. Ainsi ils ne cherchent pas à supprimer toutes les erreurs, mais simplement à en diminuer le nombre. L'élimination des erreurs restantes se fait ensuite éventuellement par l'utilisation d'un code en blocs. L'avantage d'utiliser ces codes convolutifs est de garantir un taux d'erreur par bit après décodage qui permette au code en bloc de prendre le relais et de finir la correction d'erreurs. Cette combinaison d'un code en blocs et d'un code convolutif permet de décoder en pratique avec une complexité de calcul raisonnable, tout en garantissant des probabilités d'erreur après décodage très faibles (de l'ordre de  $10^{-6}$  –  $10^{-10}$ ).

Dans le domaine quantique, on peut recenser une seule tentative visant à décrire les codes convolutifs. Nous pensons que cette dernière n'a pas eu l'écho qu'elle méritait en raison, entre autres, du caractère très obscur de l'article [Cha98]. Cependant, notre approche se démarquera assez nettement de celle suivie dans cet article. En effet, nous voulons construire ces codes dans le formalisme stabilisateur principalement en raison de sa grande souplesse d'emploi. Plus particulièrement, ce formalisme permet de prendre en compte facilement les opérations de concaténation, ce qui sera sans doute essentiel dans l'emploi futur de tels codes. Par ailleurs, le fait que leur manipulation puisse être réalisée de façon insensible aux imprécisions est cruciale compte tenu de l'état actuel des techniques à disposition des expérimentateurs.

D'autre part, nous avons généralisé au cadre des codes convolutifs quantiques l'algorithme de Viterbi pour tous les modèles de canaux où l'erreur est discrète. Dans le cas classique, l'algorithme de Viterbi se généralise aisément à des modèles d'erreur continus, comme le canal gaussien par exemple. Les modèles d'erreur les plus proches de la réalité physique ne sont pas toujours discrets néanmoins, et nous comptons étudier la généralisation de notre version de l'algorithme de Viterbi quantique à des modèles d'erreur plus complexes.

L'équipe du projet est déjà très impliquée dans cette activité. Elle accueille notamment deux stagiaires (DEA et Polytechnique) sur des sujets relatifs aux codes convolutifs quantiques.

**Décodage itératif, exploiter au mieux les ressources** — La solution classique évoquée précédemment, c'est à dire l'utilisation de codes convolutifs concaténés éventuellement avec un code en blocs a été la solution retenue en pratique pour la plupart des applications. Cependant, depuis l'apparition des turbo-codes qui combinent deux (voire plus) codes convolutifs et leur décodage de manière itérative, il est apparu que l'on pouvait dépasser très nettement les performances des schémas de concaténation code en blocs/code convolutif tout en ayant une complexité de décodage faible. Les turbo-codes établissent désormais les nouveaux standards en la matière.

Nous comptons étudier dans ce projet la possibilité de combiner plusieurs codes convolutifs quantiques et leur décodage, de manière à obtenir des turbo-codes quantiques. Par ailleurs, il apparaît actuellement dans la théorie des codes correcteurs classiques que la combinaison de plusieurs codes convolutifs ne constitue pas la seule famille de codes qui peuvent être décodés itérativement. Parmi celles-ci, on peut compter les codes de Gallager, les codes à matrice de parité creuse irréguliers, les codes de Tanner, etc., plusieurs d'entre elles rivalisent avec les performances des turbo-codes tout en ayant une complexité de décodage similaire.

Nous nous proposons également d'étudier la généralisation de ces familles au cadre quantique, et notamment la possibilité de créer des codes stabilisateurs avec des générateurs creux. La difficulté technique n'est pas tant d'adapter l'algorithme de décodage itératif classique au cadre quantique, que de construire les codes eux-mêmes. En effet, depuis notre travail sur les codes convolutifs quantiques, nous savons non seulement qu'une des versions les plus simples du décodage itératif (l'algorithme de Viterbi) se généralise au cas quantique, mais aussi que des autres versions plus sophistiquées de

décodage itératif se généralisent sans peine au cas quantique.

**Conclusion** — L'équipe du projet possède une avance certaine dans l'appréhension des problèmes évoqués plus haut et souhaiterait pouvoir la concrétiser dans le cadre de cette ACI. Le domaine étant assez vaste nous souhaiterions accueillir un doctorant pour travailler sur le sujet.

## Routage de l'information quantique

Nous l'avons vu précédemment, la fiabilité de la transmission d'information par des liens quantiques sera un des défis à relever avant le déploiement de réseaux quantiques dignes de ce nom. Ce n'est cependant pas la seule problématique. Il faudra en outre doter ces réseaux d'algorithmes de routage adaptés afin de permettre l'échange d'information entre deux nœuds bien définis.

Un tel point de vue est cependant un peu réducteur car l'échange d'information quantique ne procède pas nécessairement des mêmes ressorts que son analogue classique. En effet, dans bien des cas, il n'est besoin que de partager une grande quantité d'enchevêtrement entre différents points avant le début d'un protocole pour en améliorer de façon sensible la performance. Par exemple, un canal quantique parfait peut être simulé grâce à un bit d'enchevêtrement et deux bits classiques. C'est la fameuse téléportation quantique décrite de façon théorique par Bennett, Brassard, Crépeau, Josza, Peres et Wootters [BBC<sup>+</sup>93], puis mise en pratique par Bouwmeester, Pan, Mattle, Eibl, Weinfurter, et Zeilinger [BPM<sup>+</sup>97].

Par conséquent nous envisagerons le routage dans ces réseaux non seulement sous l'approche traditionnelle consistant à envoyer une information d'un nœud à un autre mais également dans le but de distribuer massivement de l'enchevêtrement entre tous les nœuds.

**Un contexte particulier** — L'avancement actuel et l'évolution probable des techniques liées au traitement quantique de l'information laisse prédire que les premiers réseaux développés auront pour vocation de relier des processeurs quantiques de taille et de puissance très limitées. Il est par conséquent impératif de tenir compte de cette spécificité afin de pouvoir adapter au mieux les algorithmes de routage dans ces réseaux. En effet, cela signifie à la fois que la plupart des usages de ces réseaux seront centrés sur des schémas faisant intervenir des algorithmes distribués et que par ailleurs la capacité de stockage de l'information dans les nœuds du réseau sera faible.

En ce qui concerne la communication proprement dite, l'information quantique sera codée dans les propriétés physiques de photons. Il n'est pas nécessaire de préciser qu'il n'y a aucune alternative crédible à ce choix. Cependant, sachant qu'il est pour l'instant difficile de transférer l'information quantique d'un système à un autre, il semble même opportun de se pencher plus particulièrement sur les approches "tout optique".

Dans le cas classique, on rencontre parfois des contraintes similaires et une solution dite "de la patate chaude" est une réponse adaptée à ce type de conditions. Plus précisément, l'information n'est jamais stockée dans les nœuds, mais toujours renvoyée au hasard jusqu'à ce qu'elle atteigne son destinataire final. Dans certains cas, l'information s'éloigne de son destinataire, mais elle finira par l'atteindre car elle ne cesse de progresser sur le réseau. Cette technique à l'avantage d'augmenter de façon sensible la quantité d'information pouvant transiter dans le réseau car elle évite les problèmes de collision qui ne pourraient être résolus sans stockage temporaire d'information dans un nœud.

Ce type de protocole de routage, déjà bien connu dans les réseaux classiques, doit donc être adapté aux spécificités quantiques.

**Marches aléatoires quantiques** — Il est courant de modéliser un réseau de communication par un graphe (orienté ou non) dont les sommets correspondent aux unités de traitement de l'information, et les arêtes aux canaux de communication (fibres optiques par exemple). Le principe de routage que nous avons évoqué plus haut s'apparente alors à une marche aléatoire du paquet d'information sur ce graphe.

Récemment, nous avons introduit la notion quantique correspondante — la marche aléatoire quantique [AAKV01]. Bien que la motivation ayant conduit à cette recherche soit essentiellement algorithmique, il n'en reste pas moins qu'il s'agira sans doute d'un élément clef des protocoles de routage pour la communication quantique. Les évolutions quantiques étant toujours unitaires (et donc réversibles) les marches aléatoires quantiques sont sensiblement différentes de leurs analogues classiques. Néanmoins, certaines notions ont immédiatement été adaptées avec succès (temps de mélange, mélange rapide, . . .), ce qui a permis l'émergence d'une théorie cohérente pour les chaînes de Markov quantiques. Parmi les résultats obtenus, nombre d'entre eux indiquent une différence de comportement notable des marches quantiques par rapport à leurs analogues classiques : elles se mélangent plus rapidement [AAKV01].

Dans la continuité de ces efforts, nous avons défini la notion de temps d'accès (hitting time) pour le domaine quantique. Il mesure le temps moyen nécessaire à une marche aléatoire partant d'un sommet du graphe pour accéder à un autre sommet. Cette quantité semble d'importance si l'on a en tête de possibles applications au routage dans les réseaux. Or là encore les résultats sont surprenants : pour une topologie d'hypercube et pour des sommets opposés, la différence en faveur du cas quantique est exponentielle [Kem02].

Les protocoles de routage que nous nous proposons de construire semblent donc prometteurs. Ils paraissent pouvoir contourner le principal problème de leurs analogues classiques (la relative inefficacité en terme de vitesse de transmission) sans en perdre les avantages. Nous travaillerons à vérifier ces présomptions et à étudier très en détail comment ces propriétés observées dans des cas particuliers se généralisent à des topologies différentes. Nous pensons également soumettre à l'analyse la robustesse et la sécurité de nos protocoles. En particulier, nous considérerons le cas où la topologie du réseau change de manière imprévue ou lorsqu'un nœud n'est pas pleinement fonctionnel.

**Conclusion** — Les marches aléatoires quantiques sont un outil puissant et largement sous-exploité à l'aune de ses conséquences potentielles dans le domaine du routage. Par ailleurs, il n'est pas à exclure que les études d'ordre général qui seront menées établiront de nouveaux résultats utiles pour inventer des algorithmes quantiques originaux comme cela a déjà été fait en partie [SKW02].

## Algorithmes distribués sécurisés et autres protocoles cryptographiques

Bien qu'historiquement la distribution quantique de clefs soit la première des applications de communication quantique, il n'est pas certain que ce soit dans ce domaine qu'il faille attendre les innovations les plus surprenantes. En effet, la distribution quantique de clefs bien qu'inconditionnellement sûre ne fait que palier une déficience du monde classique. Elle apporte une sécurité accrue sans véritablement changer nos schémas habituels de protection des données. En revanche, certaines des avancées de la communication quantique ont un potentiel bien plus grand. La téléportation quantique [BBC<sup>+</sup>93], le masquage quantique de données [DLT02] ou encore le cryptage impossible à copier [Got02] offrent des primitives nouvelles à l'usage des cryptologues.

La recherche que nous comptons mener sur les algorithmes et nouveaux protocoles comporte des éléments parmi les plus novateurs, mais en contrepartie les résultats y sont moins certains. Notre volonté est de toujours faire coexister deux approches complémentaires. D'une part, nous investissons dans des collaborations avec des groupes experts en algorithmes cryptographiques sur réseaux, afin d'améliorer ces algorithmes par une utilisation systématique d'enchevêtrement multipartenaires. D'autre part nous proposerons des approches totalement quantiques pour résoudre des problèmes connus ou éventuellement afin de constituer de nouvelles primitives cryptographiques.

Plusieurs tâches ont déjà attiré notre attention. Il s'agit entre autres du partage de secret ou de la dissimulation d'information. Les avantages d'une résolution quantique de ces problèmes sont bien souvent liés au théorème de non-clonage et à la destruction de l'information quantique lors d'une mesure. Les différents protocoles qui sont envisagés restent néanmoins simplistes et pourraient très certainement être améliorés si une étude systématique y était consacrée. Les autres applications potentielles de ces réseaux concernent les algorithmes distribués avec des données confidentielles. Le vote électronique est l'archétype de ces algorithmes. En effet, tout en garantissant l'anonymat des suffrages, il faut néanmoins pouvoir contrôler qui a voté et en fin de compte fournir le décompte des

voix. Là encore, il semble qu'un traitement quantique puisse fournir des résultats surprenants, mais ce sujet reste encore une préoccupation marginale de beaucoup de chercheurs.

Nos actions pour mener à bien cette tâche seront centrées sur la collaboration avec d'autres chercheurs déjà sensibilisés à cette problématique. Par ailleurs, nous souhaitons former un étudiant post-doctorant à cette problématique spécifique, tout en lui permettant d'aborder les autres domaines relatifs aux réseaux quantiques.

### 3-Résultats attendus

La constitution de réseaux quantiques et leur étude est un sujet novateur dans la communauté du traitement quantique de l'information. Nous comptons donc participer à la pose des premiers jalons de ce qui, à terme, constituera les réseaux du futur.

**Codes convolutifs et décodage itératif** — En ce qui concerne la fiabilisation du transfert de l'information, nos études préliminaires nous ont montré qu'il sera possible de généraliser la notion de code convolutif au domaine quantique. Dès la mise en place des bases théoriques — ce qui fera l'objet de publications dans des journaux à comité de lecture et de dissémination des résultats lors de conférences internationales —, nous envisageons une exploration plus systématique des codes en terme de performance et de ressources requises. Ce travail sera confié en grande partie à un étudiant en thèse.

Par ailleurs nous comptons étudier s'il est possible de combiner plusieurs codes convolutifs quantiques et les décoder de manière itérative de manière à avoir une version quantique des turbo-codes. Nous avons à notre disposition un exemple qui montre que cela est théoriquement possible. Nous pensons explorer cette voie de manière plus systématique dans le futur.

Parallèlement, nous pensons étudier d'autres architectures de codes prometteuses, notamment en généralisant les codes à matrice de parité creuse qui sont connu pour avoir d'excellentes performances pour le décodage itératif classique. Les résultats que nous comptons établir sont de première importance non seulement pour les réseaux quantiques, mais également pour le traitement quantique de l'information en général. En effet, la construction de répéteurs quantiques fonctionnant à l'aide de codes correcteurs d'erreurs entraînera la mise au point de processeurs quantiques dédiés de très petite taille, ce qui aura pour effet d'accroître encore une fois l'intensité de la recherche tant du point de vue expérimental que théorique.

**Routage** — La seconde problématique de notre projet est relative à l'étude du routage par des protocoles "tout optique". On peut décomposer le travail à effectuer en deux grandes étapes. La première consiste à approfondir l'étude des propriétés des marches aléatoires quantiques sur des réseaux de topologie variée. Dans un second temps, nous tenterons d'établir des protocoles utilisant les propriétés de ces marches aléatoires pour assurer le bon transfert de l'information. Ceci s'accompagnera d'une étude de l'efficacité et de la sécurité du protocole ainsi que de sa robustesse face à des changements imprévus de la configuration du réseau (perte d'un ou de plusieurs nœuds, nœud altérant l'information, introduction d'erreurs sur les liens, ...). Ces résultats seront sanctionnés par des publications dans des journaux scientifiques et des participations à des conférences internationales. Une part importante de ces études pourrait être menée par un étudiant en thèse.

**Algorithmes distribués et protocoles cryptographiques** — La dernière approche que nous avons souhaité inclure dans ce projet concerne le développement d'algorithmes distribués sécurisés et de protocoles cryptographiques où chaque participant a une puissance de calcul quantique limitée. Notre action s'apparentera à un défrichage, visant à recenser les nouvelles applications liées au déploiement de ces réseaux. Pour cela nous entreprendrons des collaborations avec les groupes leader dans le domaine classique pour ces problématiques et commencerons des programmes d'échanges réciproques. D'autre part, inspirés par les solutions éprouvées nous tenterons d'améliorer l'efficacité des protocoles existants par un recours systématique à l'enchevêtrement (vote électronique, calcul distribué

sûr, ...), sans pour autant négliger des approches originales pour doter ces réseaux d'applications sans équivalents classiques. A cet effet un étudiant post-doctorant avec une formation pluridisciplinaire (protocoles classiques et théorie de l'information quantique) serait recruté.

**Dissémination et représentation** — Nous pensons par ailleurs qu'il est important de former en France un groupe multidisciplinaire dans le domaine des réseaux quantiques et de leurs applications afin de consolider notre place dans une recherche internationale de haut niveau. Cette tâche sera menée à bien par la formation de trois étudiants dans le domaine (deux doctorants, un post-doctorant). Nous souhaitons les encourager fortement à collaborer avec des groupes étrangers pour des séjours de l'ordre de 2 mois tous les ans, afin qu'ils développent leurs capacités tout en attirant en France les meilleurs étudiants.

### Echéancier

<b>Année 1</b>	Mise en place des résultats théoriques pour les codes convolutifs. Début de l'étude systématique des codes convolutifs et de leurs performances. Etude des marches aléatoires quantiques pour des topologies variées. Recensement des protocoles et algorithmes cryptographiques classiques et quantiques se prêtant à une mise en réseau.
<b>Année 2</b>	Codes quantiques à matrice de parité creuse. Décodage itératif de codes quantiques. Approfondissement de l'étude des propriétés intrinsèques des marches aléatoires quantiques. Début de l'étude des protocoles de routage, de leur robustesse et de leur sécurité. Proposition de protocoles originaux pour les réseaux quantiques ou amélioration de protocoles cryptographiques existants.
<b>Année 3</b>	Poursuite des tâches engagées l'année précédente et exploitation des résultats. Amélioration du seuil de calcul tolérant les imprécisions Spécifications pour des répéteurs quantiques Spécifications pour des routeurs quantiques robustes et sûrs Propositions expérimentales pour réaliser de nouvelles fonctions cryptographiques à l'aide de ces réseaux.

## 4-Summary

This project places itself at the interface of cryptography, communication and algorithm design for *quantum networks*.

In recent years, quantum computation, quantum cryptography and quantum information has turned into an extremely active and fruitful area of research. Historically, the first seminal result was the celebrated protocol for unconditional quantum key distribution by Bennett and Brassard [BB84]. This first result was equally surprising and motivating, since all classical cryptographic schemes are based on computational hardness assumptions which have not been proved (like factoring of integers or inversion of permutations). The laws of quantum mechanics guaranty the security of the quantum protocol without any further pre-supposition. The next milestone was Shor's famous quantum algorithm to factor numbers in polynomial time [Sho94]. Stimulated by these initial results the last ten years have witnessed a multitude of research activities which have led to new algorithms and cryptographic protocols without classical equivalent (e.g. quantum secret sharing, quantum coin flipping, uncloneable encryption, ...).

As a consequence, experimentalists and theorists conjugated their efforts to examine a variety of physical systems as possible candidates for a large scale quantum computer. In particular it has been proposed to use nuclear spins of atoms in molecules (NMR), trapped ions, atoms and photons

in optical cavities, Bose-Einstein condensates in optical lattices or electron degrees of freedom in semiconductors. Even though many of them seem promising and have already resulted in small size quantum information processors, the technological challenges to be overcome to build large quantum registers are humongous. It seems unlikely that we will meet the requirements for a scalable quantum computer in a near future. In contrast, quantum cryptography and the associated quantum communication channels are already at work. Here, we passed the stage of proof of principle and in the last few years numerous quantum key distribution schemes have been implemented, in particular using free-space photon propagation or optical fibers (extending over 100 km).

Taking into account the technological progress, it is likely that in a very near future, we will dispose of high quality quantum communication channels connected to small or medium size quantum information processors coupled to the usual classical resources. This constitutes the quantum networks we wish to explore. It is our ambition to furnish all the results necessary to motivate the integration of quantum networks into the existing infrastructures. It is imperative to perform this study now because the infrastructure of the all-optical networks are still being defined and are not yet fully deployed.

At this point we have to face the following tasks :

- Determine the necessary specifications for an efficient, secure and reliable processing of quantum information in these networks ;
- Find the optimal applications to maximally profit from the advantages quantum mechanics adds to these networks ;
- Interface these nets with existing data infrastructures and assure their security.

In this context the members of this project propose to supply solutions to the following open questions :

- The protection of the communicated quantum information and in particular the applicability of error correcting codes for long distance on-line communication. We envisage to generalize the notion of convolutional codes and their iterative and maximum likelihood decoding to the quantum setting.
- The efficient, secure and robust routing of quantum information in these networks. In particular we want to model quantum information transmission in terms of quantum random walks.
- The improvement or adaptation to the quantum setting of secure distributed algorithms using these networks. Among these, we will focus on scheduling problems, secure multi-party computation, electronic voting, . . . , as well as other applications using multipartite entanglement.

The members of this project have the required expertise to perform this kind of research. Our involvement in the core areas of the proposed research (quantum computing, quantum and classical cryptography, quantum random walks, multipartite entanglement) has been testified through publications and invited talks in conferences and workshops [Kem]. The fields covered by both institutions, LRI (quantum and classical algorithms) and INRIA (cryptography and coding) naturally predispose us to successfully conduct this joint project. In addition, both LRI and INRIA have a long tradition of innovation which justifies this engagement.

## Références

- [AAKV01] D. Aharonov, A. Ambainis, J. Kempe, and U. Vazirani. Quantum walks on graphs. In *Proc. 33th STOC*, pages 50–59, New York, NY, 2001. ACM.
- [Aha01] D. Aharonov. Accuracy thresholds : Can we beat  $10^{-4}$ ? *Talk at ITP Conference on Quantum Information*, 2001.
- [BB84] Charles H. Bennett and Gilles Brassard. Quantum cryptography : Public key distribution and coin tossing. *Proceedings of IEEE international Conference on Computers, Systems and Signal Processing*, page 175, 1984.
- [BBC<sup>+</sup>93] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70 :1895–1899, 1993.

- [BPM<sup>+</sup>97] D. Bouwmeester, J. W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger. Experimental quantum teleportation. *Nature*, 390 :575–579, 1997.
- [BV97] Ethan Bernstein and Umesh Vazirani. Quantum complexity theory. *SIAM J. Comp.*, 26 :1411–1478, 1997.
- [Cha98] H.F. Chau. Quantum convolutional correcting codes. *Phys. Rev. A*, 58 :905–909, 1998.
- [DJ92] D. Deutsch and R. Jozsa. Rapid solution of problems by quantum computation. *Proc. R. Soc. London A*, 439 :553–558, 1992.
- [DLT02] David P. DiVincenzo, Debbie W. Leung, and Barbara M. Terhal. Quantum data hiding. *IEEE Trans. Inf. Theo.*, 48 :580, 2002.
- [FIM<sup>+</sup>03] K. Friedl, G. Ivanyos, F. Magniez, M. Santha, and P. Sen. Hidden translation and orbit coset in quantum computing. In *Proc. of the 35th ACM STOC*, 2003.
- [Got97] Daniel Gottesman. *Stabilizer codes and quantum error correction*. PhD thesis, California Institute of Technology, Pasadena, CA, 1997. Also arXiv, quant-ph 9705052.
- [Got02] D. Gottesman. Uncloneable encryption. *arXiv*, quant-ph :0210062, 2002.
- [IMS03] G. Ivanyos, F. Magniez, and M. Santha. Efficient quantum algorithms for some instances of the non-abelian hidden subgroup problem. *I. J. Found. Comput. Sci.*, 2003.
- [JZ99] R. Johannesson and K. Zigangirov. *Fundamentals of Convolutional Coding*. Digital and Mobile Communication. IEEE press, 1999.
- [Kem] J. Kempe. List of invited talks. <http://www.lri.fr/~kempe/talksvisits.html>.
- [Kem02] J. Kempe. Quantum random walks hit exponentially faster. *arXiv*, quant-ph :0205083, 2002.
- [Lee97] L. H. Charles Lee. *Convolutional coding : fundamentals and applications*. Artech House Publishers, 1997.
- [SGG<sup>+</sup>02] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and Zbinden. *New J. Phys.*, 4 :41, 2002.
- [Sho94] P. W. Shor. Algorithms for quantum computation : Discrete logarithms and factoring. In S. Goldwasser, editor, *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, pages 124–134, Los Alamitos, CA, 1994. IEEE Computer Society.
- [Sho95] Peter W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev A*, 52 :2493, 1995.
- [Sho96] P. W. Shor. Fault-tolerant quantum computation. In *Proceedings of the 37th Symposium on the Foundations of Computer Science*, pages 56–65, Los Alamitos, California, 1996. IEEE press. Also arXiv, quant-ph 9605011.
- [Sim94] Daniel R. Simon. On the power of quantum computation. *35th Annual Symposium on Foundations of Computer Science*, page 116, 1994.
- [SKW02] N. Shenvi, J. Kempe, and K. B. Whaley. A quantum random walk search algorithm. *Phys. Rev. A*, 2002. to appear.
- [Ste98] A. M. Steane. Efficient fault-tolerant quantum computing, 1998. Also arXiv, quant-ph 9809054.
- [WZ82] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299 :802, 1982.
- [Zal96] C. Zalka. Threshold estimate for fault tolerant quantum computation. *arXiv*, quant-ph :9612028, 1996.
- [Zur91] W. H. Zurek. Decoherence and the transition from quantum to classical. *Physics Today*, 44 :36–44, 1991.