Thème Information et Réseaux quantiques

Contributeurs Telecom ParisTech/Infres à cette thématique

Permanents : Romain Alléaume, (Maître de Conférences) ; Gérard Cohen, (Professeur) ; Maurice Gagnaire, (Professeur) ; Hugues Randriam, (Maître de Conférences).

Non-permanents : Anthony Leverrier, doctorant (2006-2009), Rex Medeiros, doctorant en cotutelle avec Université Campina Grande, Brésil (2005-2008), David Elkouss, doctorant en cotutelle avec Université de Madrid (2007-2010), Mehrdad Dianati, post-doctorant (juillet 2006 à juillet 2007), Stefano de Crescenzo, master thesis (janvier 2007 à juillet 2007), Marco Nicoletti, master thesis (novembre 2007 à juillet 2008)

Collaborations privilégiées : groupe de Philippe Grangier (Institut d'Optique),groupe de Nicolas Gisin (GAP Optique Genève), Austrian Research Center Vienne, groupe de Norbert Lütkenhaus (Institute for Quantum Computing,Waterloo, Canada), Institut Mathématique de Bordeaux (Gilles Zémor), Joseph Boutros (Texas A&M Univ, Quatar) Univ. Fed. Campina Grande, Brésil (Francisco Assis, Rex Medeiros), groupe de Nicolas Cerf (Université Libre de Bruxelles).

Réseau de distribution quantique de clés

Romain Alléaume, Maurice Gagnaire, Mehrdad Dianati, Stefano de Crescenzo, Marco Nicoletti.

Protocoles réseaux et architecture pour les réseaux QKD

Nous avons développé une architecture et des protocoles spécifiquement adaptés à la distribution quantique de clé à l'échelle de réseaux de grande taille. Testés et validés au sein du consortium européen SECOQC, une de nos ambitions est de faire de ces protocoles des standards européens. Un processus de standardisation, mené au sein de l'ETSI, a débuté en janvier 2008. Nous travaillons également à l'optimisation des topologies et à la planification des futurs réseaux quantiques, en collaboration avec TSI (François Roueff).

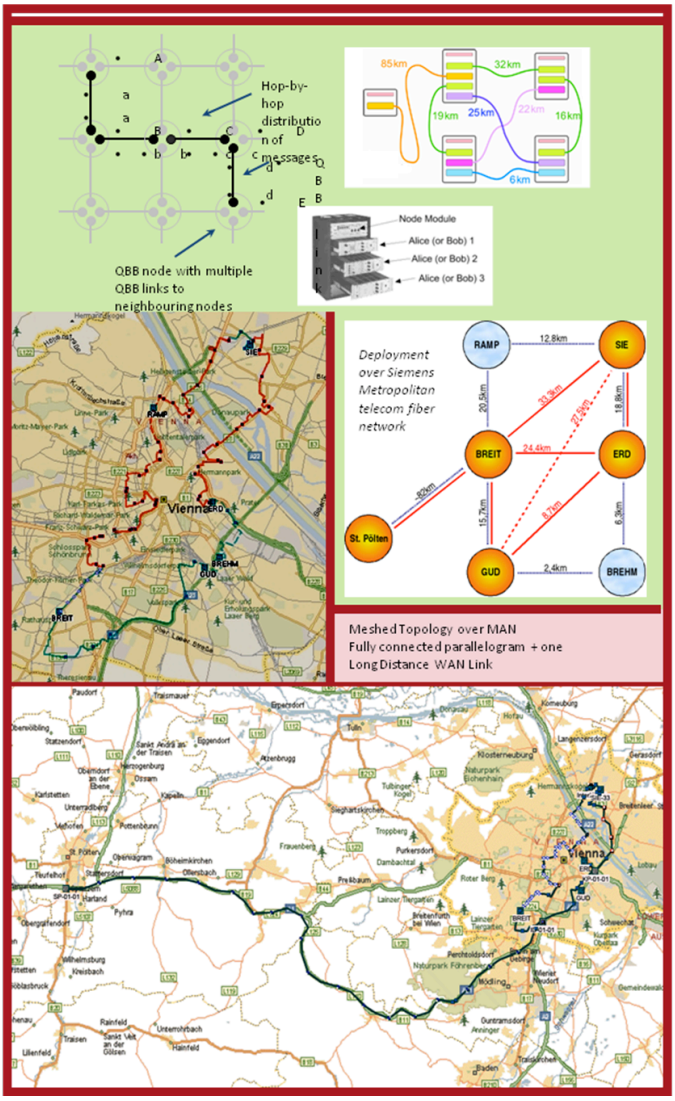
Notre équipe se positionne comme un acteur de premier plan, au niveau européen et mondial, sur cette thématique combinant cryptographie quantique et réseau, comme le témoigne le rôle majeur que nous jouons dans le projet SECOQC. La démonstration et la conférence internationale qui auront lieu à la fin du projet SECOQC devrait permettre d'accroître encore la visibilité et le rayonnement de ces travaux.

Intégration de la cryptographie quantique dans les réseaux numériques, et développement d'applications nouvelles

Dans le cadre des projets SECOQC, SEQURE, et PROSPIQ, nous travaillons à la mise en place de démonstrateurs de distribution quantique de clé (sur réseau fibré et / ou en espace libre).

A l'aide de la subvention ANR du projet SEQURE, nous avons commandé un lien quantique QKD Vectis d'IdQuantique. Nous allons ainsi regrouper un démonstrateur, à TELECOM ParisTech, dont nous maîtriserons toute la chaîne de fonctions : couche physique quantique dont nous testerons la sécurité physique, couche lien avec nos propres codes correcteurs et protocoles (permettant d'accroître débit et distance), couche réseau avec nos protocoles, issus de SECOQC et en voie de standardisation au niveau européen.

Un de nos objectifs de recherche va enfin constituer à développer des applications, tirant au mieux partie des potentialités nouvelles offertes par la cryptographie quantique. Nous sommes l'un des tous premiers groupes explicitement positionnés sur cet axe, positionnement renforcé par la forte cohérence d'ensemble avec les autres activités de l'équipe. Ce travail sera d'ailleurs mené en collaboration avec la spin-off SeQureNet, et impliquera une importante activité de dépôts de brevets et de valorisation.



DEPLOIEMENT DU RESEAU SECOQC SUR UN RESEAU FIBRE METROPOLITAIN, A VIENNE, AUTRICHE
DEMONSTRATION ET CONFERENCE INTERNATIONALE LES 8, 9 ET 10 OCTOBRE 2008

Cryptographie quantique

Contributeurs Telecom ParisTech : Anthony Leverrier, Romain Alléaume, David Elkouss

Collaboration avec Joseph Boutros (Texas A&M at Qatar), Gilles Zémor (Institut de Mathématiques de Bordeaux), Philippe Grangier (Institut d'Optique), Nicolas Cerf (Université Libre de Bruxelles)

Réconciliation de variables gaussiennes corrélées dans le cadre de protocoles de cryptographie quantique

Les protocoles de cryptographie quantique les plus étudiés à ce jour utilisent des variables discrètes et encodent l'information sur la polarisation ou la phase de photons uniques (ou d'impulsions atténuées). S'ils sont relativement bien compris théoriquement, ces protocoles souffrent néanmoins de limitations technologiques importantes, notamment en ce qui concerne la détection. Une approche alternative qui relaxe ces limitations technologiques, consiste à utiliser des variables continues, par exemple les quadratures d'un état cohérent. Dans ce cas, l'obstacle qu'il faut surmonter est celui du traitement classique des variables continues, en particulier l'étape de la réconciliation où deux parties distantes qui possèdent des variables continues corrélées doivent se mettre d'accord sur un message commun, tout en révélant une information minimale à un potentiel espion.

Nous avons développé un protocole de réconciliation utilisant les propriétés algébriques des octonions en dimension 8. Cette méthode a permis de significativement augmenter la portée des protocoles à variables continues : avec le même dispositif expérimental, l'utilisation du nouveau protocole permet d'atteindre 50 km contre environ 30 km auparavant.

Ce résultat fait l'objet d'une publication dans Physical Review A.

Un nouveau protocole de cryptographie quantique à variables continues a également été mis au point. Ce protocole combine les avantages des variables discrètes (grande distance, simplicité de la réconciliation) et des variables continues (rapidité, faible coût), et fait actuellement l'objet d'une demande de dépôt de brevet. Les co-inventeurs sont Anthony Leverrier et Philippe Grangier (CNRS).

Deux axes de recherche sont actuellement en cours d'étude.

D'abord, le nouveau protocole à variables continues pose des problèmes de taille finie dès que l'on essaie d'atteindre des distances de l'ordre de la centaine de kilomètres. Il est nécessaire d'étudier ces effets afin de les quantifier. Notons que les problèmes de taille finie commencent juste à être pris en compte dans le contexte de la cryptographie quantique, y compris pour les protocoles à variables discrètes.

L'autre sujet fait l'objet d'une collaboration avec le professeur Nicolas Cerf de l'Université Libre de Bruxelles et concerne la recherche d'une preuve de sécurité inconditionnelle pour les protocoles de cryptographie quantique à variables continues. Le principal problème ici étant que l'outil utilisé à cette fin pour les protocoles à variables discrètes, une version exponentielle du théorème de De Finetti, n'est pas directement exploitable en dimension infinie.

Codes correcteurs d'erreurs pour la cryptographie quantique à variables discrètes

Aujourd'hui, la plupart des protocoles de cryptographie quantique à variables discrètes comprennent une phase de réconciliation interactive. La réconciliation consiste pour Alice et Bob à corriger, à l'aide de communications classiques, les erreurs introduites par le canal quantique. Une réconciliation interactive signifie qu'Alice et Bob s'échangent des messages tous les deux par opposition à une réconciliation unidirectionnelle où seul un participant peut envoyer des messages au second.

Le protocole le plus utilisé, Cascade, est un protocole interactif qui a été proposé en 1993 avant l'avènement des Turbo-codes et des codes LDPC. Aujourd'hui, ces codes apparaissent comme une alternative sérieuse à Cascade car ils permettent de s'approcher très près de la limite de Shannon tout en évitant la latence importante introduite par les protocoles interactifs.

La comparaison des performances de ces deux types de réconciliation fait l'objet du travail de David Elkouss.

Capacité zéro-erreur quantique

Contributeurs Telecom ParisTech: Rex A. C. Medeiros, Romain Alléaume, Hugues Randriam, Gérard Cohen*.

Collaboration avec Universidade Federal de Campina Grande, Brésil (Institut IQUANTA, Francisco M. de Assis* et Rex A. C Medeiros) [*] : Co-directeurs de thèse

On s'intéresse à la capacité zéro-erreur des canaux quantiques, c'est-à-dire la capacité avec laquelle des canaux quantiques peuvent transmettre de l'information classique avec une probabilité d'erreur strictement égale à zéro. Ce travail est une généralisation aux canaux quantiques de la notion de capacité zéro-erreur introduite par Shannon pour des canaux discrets sans mémoire.

On a exhibé une condition nécessaire et suffisante pour qu'un canal quantique possède une capacité zéro-erreur non nulle et reformulé le problème de la détermination de la capacité zéro-erreur en termes de théorie des graphes. Cette reformulation permet de d'étudier plus facilement certaines propriétés des ensembles d'états quantiques et des mesures associées qui atteignent la capacité.

La question centrale de cette étude est de voir dans quelle mesure la capacité zéro-erreur quantique diffère de sa contrepartie classique. A cet égard, nous avons déjà exhibé des canaux quantiques pour lesquels la famille d'états atteignant la capacité zéro-erreur est non triviale.

Thèses soutenues ou à soutenir

Rex Medeiros, (Juin 2008) : « Capacité zéro-erreur des canaux quantiques ».

Perspectives

Création de SeQureNet en février 2008. L'entreprise SeQureNet est une société « spin-off » vis-à-vis d'activités de recherches menées au sein de Telecom ParisTech dans le cadre du projet européen FP6 SECOQC. Ces recherches ont trait à la mise au point de réseaux de distribution de clés secrètes utilisant la cryptographie quantique. S'appuyant sur les standards européens issus de SECOQC, SeQureNet veut développer des produits et services qui permettront à des utilisateurs / clients de réellement tirer profit des solutions cryptographiques nouvelles rendues possibles par les réseaux de distribution quantique de clés. Créée en février 2008, SeQureNet souhaite être incubée dès avril 2008, afin de pouvoir héberger une équipe de développeurs travaillant sur la mise au point d'une application sur smartphones, en collaboration avec France Telecom, afin ensuite de participer à la démo SECOQC, en septembre 2008, à Vienne.

Création au sein de Telecom ParisTech, en lien avec la fondation de l'institut Telecom, d'un laboratoire de validation, de certification et d'attaques des cryptosystèmes quantique.

Participation à un projet européen de grande ampleur, Space-Quest, coordonnée par l'ESA, visant à déployer des technologies quantiques (et notamment la distribution quantique de clé) dans l'espace (à bord de satellites, en communication avec la terre).

Publications

Journaux

M. Dianati, R. Alléaume, M. Gagnaire, and X. Shen , Architecture and Protocols of the Future European Quantum Key Distribution Network, accepted for publication in the first issue of *Security and Communication Networks*, first semester 2008.
A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, Multidimensional reconciliation for continuous-variable quantum key distribution, Phys. Rev. A (2008)
R. Alléaume, J. Bouda, C. Branciard, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Länger, A. Leverrier, N. Lütkenhaus, P. Painchault, M. Peev, A. Poppe, T. Pornin, J. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A. Shields, H. Weinfurter, A. Zeilinger, Secoqc White Paper on Quantum Key Distribution and Cryptography, *quant-ph/0701168* to be submitted for publication as a highlight paper in the *European Journal of Physics D*, (2008).
R. Alléaume, F. Roueff, E. Diamanti, and N. Lütkenhaus, Long-distance quantum key distribution networks : cost calculations and optimal working points of individual links, en préparation.

Conférences internationales avec comité de lecture et actes

M. Peev, R. Alléaume, T. Länger, N. Lütkenhaus, O. Maurhart, L. Salvail , The SECOQC Quantum Key Distribution Network Prototype: Principles, Design and Implementation, Globecomm, Washington, November 2007.
M. Dianati and R. Alléaume, A Transport Layer Protocol for the SECOQC QKD Quantum Key Distribution Networks, The Third IEEE LCN Workshop on Network Security (WNS 2007), Dublin, Ireland, Oct. 2007.
M.Peev, R. Alléaume, Th.Länger, N.Lütkenhaus, L.Salvail A Quantum Key Distribution Network: Integrated Design and Prototypical Implementation, CLEO Europe, Munich, Jun. 2007.
M. Dianati, R. Alléaume, D. Subacius, *Architecture of the Secoqc Quantum Key Distribution Network*, The First International Workshop on Quantum Security, Guadeloupe, Jan 2007.

Conférences nationales avec comité de lecture et actes

Romain Alléaume, Rex A C Medeiros, Hugues Randriam, Francisco M de Assis, et Gérard Cohen, Zero-error capacity of quantum channels, Journées Codage et Cryptographie, Mars 2008, Carcans.
A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, Réconciliation de variables gaussiennes corrélées dans le cadre de protocoles de cryptographie quantique, Journées Codage et Cryptographie, Mars 2008, Carcans.
R. Medeiros, R. Alléaume, H. Randriam, G. Cohen, F. de Assis, Capacité Zéro-erreur quantique, Journées Codage et Cryptographie, Mars 2008, Carcans.

Autres conférences

R. Alléaume, Capacité Zéro-erreur quantique, Journée Information Quantique, Paris, IHP, 23 Mars 2008.
R. Alléaume, Quantum Communications: from systems to networks, invited talk at the Brazilian National Workshop on Quantum Information, WECIQ 2007, Campina Grande, Brazil Oct 2007.
A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, E. Diamanti, R. Tualle-Brouri et P. Grangier, *An efficient reconciliation protocol for continuous-variable quantum cryptography*, QIPC 2007, Barcelona
R. Alléaume, *Quantum Key Distribution and Networks*, lecturer at the QUROPE winter school, Oberburgl, Austria, Feb 2007.

Brevets à l'étude

Un brevet est en cours de dépôt par Anthony Leverrier et Philippe Grangier, sur un protocole de cryptographie quantique. Un autre brevet est à l'étude, sur la notion de fontaine de secrets et son branchement concret dans des réseaux applicatifs sécurisés.

Autres publications

M. Dianati and Romain Alleaume, "Requirement Specifications of Secoqc QKD Network", SECOQC Project Deliverable, Aug. 2006.
M. Dianati and Romain Alleaume, " SECOQC QKD Network: Design Document", SECOQC Project Deliverable, Oct. 2006.
M. Dianati and Romain Alleaume, "Specifications of the SECOQC QKD Transport Layer Protocols", SECOQC Project Deliverable, Apr. 2007.
S. De Crescenzo, M. Dianati and Romain Alleaume, "A Simulation-based Performance Analysis of the SECOQC QKD network", SECOQC Project Deliverable, Apr. 2007.