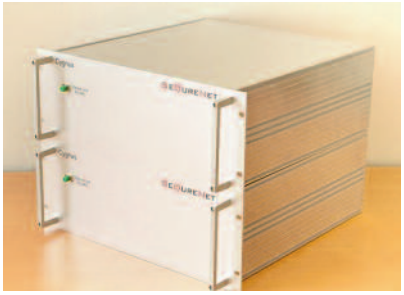
Confidentialité des échanges et physique quantique

Novembre 2013

La physique quantique ouvre la voie à des applications radicalement nouvelles, telles que la cryptographie quantique. C'est à cette discipline que se consacre Romain Alléaume, chercheur à l'Institut Mines-Télécom. Au sein de l'équipe qu'il a créée à Télécom ParisTech, le chercheur utilise les propriétés spécifiquement quantiques de la lumière pour imaginer et concevoir des systèmes permettant de distribuer des secrets à distance. Ses travaux les plus récents portent sur la sécurisation de ces dispositifs quantiques et sur leur compatibilité avec les réseaux de télécommunications « classiques ».

Beaucoup viennent au monde quantique guidés par la curiosité et l'émerveillement. Romain Alléaume aussi fut intrigué par ces lois de la nature en contradiction avec l'intuition. Parmi elles, le principe de superposition : « *Un système quantique peut être dans plusieurs états différents en même temps* » ; le principe de sensibilité à la mesure : « *Ce qui est également surprenant, c'est que le fait de poser la question à un objet quantique, pour savoir dans quel état il est, change l'état de ce dernier* » ; et le principe d'intrication, une autre spécificité quantique : « *Il désigne des corrélations entre particules quantiques qui empêchent de les décrire séparément* ». Tirant parti de ces propriétés déroutantes, c'est à partir des années 1980 que les chercheurs commencent à imaginer une nouvelle façon de traiter l'information. Non sans peine, explique le chercheur : « *Une difficulté fondamentale pour réaliser un ordinateur quantique vient du fait que les supports de l'information quantique, appelés "qubits", doivent pouvoir interagir entre eux et être modifiés très rapidement tout en étant très bien protégés de l'environnement extérieur* ». Tout paradoxal qu'il soit, l'ordinateur quantique n'est cependant pas chimérique puisqu'il existe bel et bien expérimentalement, le plus gros actuel comptant 14 qubits.



Cygnus, le système QKD mis au point et commercialisé par SeQureNet

Bénéficier de l'environnement pluridisciplinaire de l'Institut Mines-Télécom

L'information quantique interroge un grand nombre de champs disciplinaires, mêlant physique, informatique et théorie de l'information. Elle sollicite les technologies physiques les plus avancées, comme celle des atomes froids, de la supraconductivité et de l'optique, et mobilise de nombreuses équipes de pointe. C'est à Télécom ParisTech que Romain Alléaume a débuté sa carrière de chercheur et créé l'équipe « Information quantique », aujourd'hui composée d'une quinzaine de membres. « *L'Institut Mines-Télécom et l'école ont été déterminants dans l'émergence de l'équipe, notamment à travers les soutiens financiers et les mètres carrés alloués.* » Le chercheur reconnaît qu'il tire de précieux avantages à évoluer à l'Institut Mines-Télécom : « *Il y a l'aspect pluridisciplinaire (codage, mathématiques discrètes, physique, optique), un environnement riche et une ouverture sur l'industrie* ». Un environnement d'autant plus propice que lorsque Romain Alléaume a souhaité créer son entreprise, l'école l'a encouragé et conseillé.

Il se lance en 2008 dans l'aventure industrielle et cofonde SeQureNet, une start-up concevant des systèmes de cryptographie quantique. Plus connue sous son acronyme QKD (*Quantum Key Distribution*), la cryptographie quantique ou « distribution quantique de clés » permet de partager des informations confidentielles à travers une liaison de communication, typiquement une fibre optique, avec une sécurité

SeQureNet, une société issue des laboratoires

SeQureNet, fondée en 2008, est une *spin-off* de l'équipe « Information quantique » de l'Institut Mines-Télécom, qui produit et commercialise des solutions technologiques innovantes offrant aux réseaux de communication un niveau de sécurité accru. SeQureNet commercialise depuis 2012 un système de distribution quantique de clés, Cygnus, reposant uniquement sur des composants standard ; avec ce système, elle a participé à la démonstration expérimentale du record de portée pour cette technologie, de 80 kilomètres contre 25 précédemment. Ces travaux ont été publiés le 14 avril 2013 sur le site de la revue *Nature Photonics*, dans un article intitulé *Experimental demonstration of long-distance continuous-variable quantum key distribution*, et signé de P. Jouguet, S. Kunz-Jacques, A. Leverrier, E. Diamanti et P. Grangier.

Le système Cygnus a déjà suscité l'intérêt du NICT (Institut national japonais des technologies de l'information et de la communication), au Japon, qui en a fait l'acquisition. Deux types d'applications sont visées : la R&D académique et industrielle (déploiement, réseaux et sécurité) et la protection des infrastructures (opérateurs télécom, défense), avec comme argument essentiel la capacité de la QKD à offrir une garantie de sécurisation des échanges de données sur le long terme. **www.sequrenet.com**

nettement meilleure que dans le cadre de la cryptographie classique. L'information est codée sur la lumière, par exemple sur la polarisation des photons. SeQureNet utilise une technologie appelée « cryptographie quantique à variables continues » issue de travaux réalisés à l'Institut d'optique Graduate School et à Thales, et développée aujourd'hui à l'Institut Mines-Télécom. Cette technologie présente plusieurs points forts : un système de détection qui la protège très efficacement des bruits parasites et une très bonne compatibilité avec les infrastructures actuelles. Reposant uniquement sur des composants télécoms standard, elle n'exige pas le recours à des fibres dédiées.

Une sécurité à long terme

L'idée qui sous-tend la QKD est de tourner à son profit la sensibilité à la mesure, faisant d'une apparente faiblesse une vertu. Quiconque chercherait à « lire » le photon messager perturberait son état quantique et introduirait des erreurs. Impossible par conséquent pour un espion d'obtenir que les correspondants partagent et utilisent une clé qu'ils croiraient sûre alors qu'elle a été interceptée. Un autre avantage concurrentiel fondamental de la QKD est sa sécurité à long terme, que ne garantit pas la cryptographie classique. Ainsi, la sécurité de RSA, l'algorithme pionnier de la cryptographie à clé publique inventé par Rivest, Shamir et Adleman[1], repose-t-elle sur une conjecture : la difficulté à factoriser des grands nombres. Mais, suggère Romain Alléaume : « *Rien n'interdit de tout enregistrer aujourd'hui en espérant casser le code demain !* » Alors qu'une clé sûre aujourd'hui le sera encore dans vingt ans avec la QKD. La sécurité intrinsèque de la QKD a conduit le chercheur à tenter de l'intégrer dans des réseaux. C'est un défi auquel il s'est attelé depuis 2004 avec le projet européen SECOQC, qui a abouti en 2008 au déploiement du premier réseau QKD européen.

À travers une collaboration entre Télécom ParisTech et SeQureNet, les travaux de l'équipe portent aujourd'hui sur l'amélioration des performances du système QKD, mais aussi sur son intégration dans les infrastructures de réseaux optiques. Ce ne sont néanmoins pas les seuls objectifs poursuivis : la sécurité pratique des systèmes est aussi un enjeu important, notamment pour l'industrialisation. « *Dans le domaine de la cryptographie, il est normal d'être mis au défi, surtout qu'on doit se comparer avec des systèmes existants, pour lesquels les tests de certification sont très poussés* ». Il est apparu que les systèmes matériels QKD peuvent aussi avoir des failles et qu'il fallait donc les tester de façon préventive. Un retournement de situation qui n'échappe pas à Romain Alléaume : « *Cela remet en question ce dont la QKD s'est beaucoup enorgueillie : l'universalité et l'inconditionnalité de sa sécurité. Une partie de mes travaux actuels porte sur ce point : s'intéresser aux attaques possibles et développer des contre-mesures pour pouvoir garantir la sécurité de la QKD.* » C'est peut-être le coût d'entrée dans la maturité que paie cette jeune discipline. Il existe toutefois une nouvelle approche, basée sur la notion d'intrication permettant de garantir la sécurité des systèmes quantiques malgré l'imperfection des matériels utilisés. Disposer de sources de photons intriqués ouvre des perspectives de recherche considérables non seulement en cryptographie, mais aussi pour fabriquer des « répéteurs quantiques ». L'occasion pour le chercheur et son équipe de mener de nouvelles recherches passionnantes !

[1] Le chiffrement RSA (nommé par les initiales de ses trois inventeurs Rivest, Shamir et Adleman), est un algorithme de cryptographie asymétrique décrit en 1977, très utilisé dans le commerce électronique, et plus généralement pour échanger des données confidentielles sur Internet.

Lier recherche, innovation et industrie

Romain Alléaume entre à l'École normale supérieure de la rue d'Ulm en 1998. En dernière année, déjà intéressé par la cryptographie quantique, il commence une thèse à l'ENS Cachan sur les sources de photons uniques. Attiré par une carrière mêlant recherche et industrie, il intègre en 2001 le Corps des Télécom et suit les enseignements de Télécom ParisTech. Il soutient sa thèse en 2004. Depuis, il est enseignant-chercheur à Télécom ParisTech. Ses recherches actuelles au sein de l'Institut Mines-Télécom portent sur la cryptographie quantique, les réseaux quantiques et la théorie de l'information. Il est par ailleurs le conseiller scientifique de SeQureNet, start-up dont il est un des cofondateurs.

Rédaction : Umaps - Mise en pages : *implica* CR&A - Crédit photo : Institut Mines-Télécom

Suivez l'actualité recherche & innovation de l'Institut Mines-Télécom

http://blogrecherche.wp.mines-telecom.fr et www.twitter.com/Mines_Telecom

INSTITUT Mines-Télécom

CONTACT INFORMATION RECHERCHE & INNOVATION
recherche@mines-telecom.fr

Institut Mines-Télécom
46 rue Barrault - 75634 Paris cedex 13
France

www.mines-telecom.fr

À PROPOS DE L'INSTITUT MINES-TÉLÉCOM

L'Institut Mines-Télécom est un établissement public dédié à l'enseignement supérieur, la recherche et l'innovation dans les domaines de l'ingénierie et du numérique. Il est composé des dix grandes écoles Mines et Télécom sous tutelle du ministre du Redressement productif, deux écoles filiales et compte deux partenaires stratégiques et un réseau de onze écoles associées.

L'Institut Mines-Télécom est reconnu au niveau national et international pour l'excellence de ses formations d'ingénieurs, managers et docteurs, ses travaux de recherche et son activité en matière d'innovation. Les écoles de l'Institut Mines-Télécom sont classées parmi les toutes premières grandes écoles en France.

L'Institut Mines-Télécom est membre des alliances nationales de programmation de la recherche Allistene, Aviesan et Athena. Il entretient des relations étroites avec le monde économique et dispose de deux instituts Carnot. Chaque année une centaine de *start-ups* sortent de ses incubateurs.