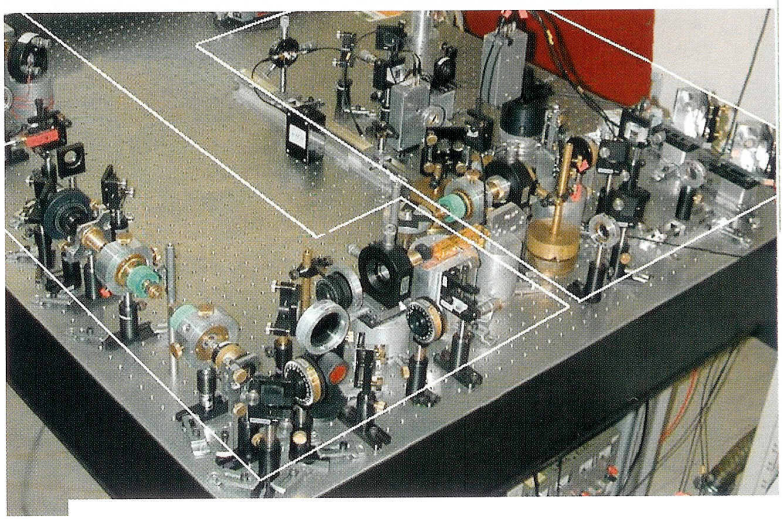
à l'université 13

Les secrets de la cryptographie quantique

La cryptographie nous cache des choses... C'est en tout cas son objectif: permettre une sécurité absolue dans l'échange de messages qui doivent rester secrets. Que ce soit de l'écrit, du son ou de l'image, tout est cryptable grâce aux techniques actuelles. Mais celles-ci ne garantiront sans doute pas la confidentialité à long terme: chaque jour les « casseurs de codes » gagnent des points grâce à l'évolution des mathématiques et des ordinateurs... La solution pourrait venir de la physique quantique, comme nous l'explique Nicolas Cerf, à la tête du Service de Théorie de l'informationde la Faculté des Sciences appliquéesde l'ULB. Il y a quelques mois, il cosignait un article dans le magazine Nature, qui fait progresser la question du cryptage quantique.

Esprit libre : En tant qu'ingénieur et physicien, vous vous intéressez à la transmission d'information au niveau microscopique. En quelques mots, cela consiste en quoi?

Nicolas Cerf : Je m'intéresse à ce qui se passe lorsque de l'information est portée par des particules élémentaires, étape ultime prévisible de la miniaturisation des composants électroniques du futur. Depuis un siècle, on sait par exemple que la lumière est constituée de grains élémentaires, les photons. Récemment, on s'est demandé quelles seraient les possibilités nouvelles de traitement de l'information si l'on arrivait à encoder chaque bit, 0 ou 1, dans un photon unique. Pourrait-on exploiter les spécificités de la physique fondamentale à l'échelle microscopique (la physique quantique) pour en arriver à une application telle que la cryptographie?



L'équipe de Nicolas Cerf travaille en étroite collaboration avec celle de Philippe Grangier, de l'Institut d'optique d'Orsay en Fronce. Photo : Institut d'optique, CNRS

Esprit libre : Qu'est-ce que la cryptographie quantique?

Nicolas Cerf : C'est une technique permettant l'échange d'une clé secrète entre deux parties, un émetteur et un récepteur. Ceux-ci peuvent alors chiffrer un message confidentiel qu'ils désirent se communiquer en utilisant un code comme celui de Vernam. Ce code, connu depuis longtemps, est sûr car il est impossible à un espion qui n'aurait pas la clé de décoder le message. En contrepartie, les deux parties doivent posséder une clé (soit une longue séquence de bits aléatoires) qu'ils ne peuvent utiliser qu'une seule fois. Si elle est réutilisée, même partiellement, les messages chiffrés deviennent vulnérables. C'est cette faiblesse qui a été exploitée par les alliés pour casser le code Enigma utilisé par les Allemands durant la seconde guerre mondiale. Conséquence: il faut chaque fois utiliser de nouvelles clés et, finalement, la distribution de clés s'avère être un défi majeur. C'est là qu'intervient la physique quantique: elle permet de garantir la confidentialité de cette distribution de clés.

Esprit libre : Qu'avez-vous apporté comme éléments nouveaux à ces recherches?

Nicolas Cerf : Nous avons proposé un schéma de cryptographiebasé sur des impulsions cohérentes de la lumière comprenant plusieurs photons. Du point de vue expérimental, la différence est de taille puisque ces impulsions cohérentes peuvent être produites très simplement par un laser. La technique de détection utilisée par le récepteur, plus standard, ne nécessite pas le comptage des photons individuels. Tout cela permet d'accroître nettement les taux de distribution de clés secrètes et, par là, de remédier à l'un des points faibles de la cryptographie quantique. L'expérience qui a démontré la validité de ce concept a été réalisée par l'équipe de Philippe Grangier à l'Institut d'optique d'Orsay en France, et le traitement des données, par Gilles Van Assche, doctorant dans mon service.

Esprit libre :

défi majeur. C'est là qu'intervient la physique quantique: elle permet de garantir la confidentialité de cette distribution de clés.

Esprit libre : La recherche sur cette technique a été entamée voici vingt ans. Quelle est sa particularité?

Nicolas Cerf : La naissance de cette discipline date de 1984 : un chercheur d'IBM et un expert en cryptographie de l'université de Montréal ont proposé un protocole théorique permettant le partage de clés secrètes entre deux parties via l'échange de photons uniques. Il a fallu attendre une dizaine d'années pour que les premières expériences soient réalisées, même si elles se limitaient alors à l'échange d'une clé entre deux points situés sur une même table d'optique. Ensuite, dès les années 90, de nouvelles expériences ont permis d'étendre la portée en reliant les deux parties par une fibre optique. Actuellement on parvient à distribuer une clé via une fibre optique sur une distance d'une centaine de kilomètres!

Quelles pourraient être les applications commerciales de votre recherche?

Nicolas Cerf : Il y a actuellement deux start-up dans le monde (ID Quantique et MagiQ) qui proposent un système de cryptographie quantique. De notre côté , une demande de brevet a été déposée pour ce nouveau procédé de cryptographiequantique . Quelques dizaines de brevets existent déjà dans ce domaine, mais notre schéma est le premier qui utilise les impulsions cohérentes de la lumière. La société française Thales projette d'ailleurs la réalisation d'un prototypede notre système . Il est clair que ce type de procédé sera utile avant tout pour des liaisons spécialisées dont la sécurité est critique et justifie l'investissement dans un changement radical de technologie. On peut imaginer que cela puisse par exemple intéresser le monde bancaire ou militaire. Pour l'Internet par contre, le passage à la cryptographie quantiquereste encore du domaine de la fiction.

> Alain Dauchot

ESPRIT LIBRE > DÉCEMBRE 2003 / JANVIER 2004 [N° 18]