Les photons, agents secrets quantiques

Jean-Paul Delahaye

Les photons, agents secrets quantiques

La possibilité d'échanger des clefs secrètes à distance à travers une fibre optique en s'envoyant des photons polarisés résout un problème fondamental de cryptographie. Après une phase de conception théorique suivie d'une phase expérimentale, plusieurs entreprises proposent aujourd'hui des solutions quantiques sans équivalents en cryptographie mathématique.

Puisque c'est notre conception même de l'information que la mécanique quantique est en train de changer, pas étonnant qu'elle ait quelque chose à nous dire au sujet de la cryptographie, science de l'information secrète. En réalité, la mécanique quantique n'en est plus à nous suggérer des idées: la cryptographie quantique, née dans l'esprit de Stephen Wiesner en 1970, précisée en 1982 par C. H. Bennett et G. Brassard, et prouvée expérimentalement en 1989 est depuis quelques mois la première application de l'informatique quantique à être entrée dans le domaine industriel et commercial. Alors que de nombreuses années s'écouleront sans doute avant que votre ordinateur de bureau ne devienne quantique - si cela se produit un jour ! -, vous pouvez acheter aujourd'hui un appareillage de distribution de clefs secrètes par méthode quantique.

L'idée principale est que pour que deux personnes puissent échanger secrètement de l'information, il suffit qu'elles partagent un secret que nul autre ne connaît. Cette clef secrète qui chiffre et déchiffre les messages peut être utilisée de plusieurs façons (méthode par masque jetable, méthode classique de cryptographie mathématique à simple clef), mais cela est bien connu et ce n'est pas la nouveauté. Ce que permet la mécanique quantique et qui n'a pas d'équivalent classique, c'est l'échange à distance entre deux personnes d'une clef, la garantie de sécurité provenant des principes même de la mécanique quantique, théorie éprouvée depuis plus d'un demi-siècle.

Notons que les méthodes de cryptographie utilisées couramment aujourd'hui sont fondées sur des conjectures mathématiques dont on a de bonnes raisons de croire qu'elles sont vraies, mais dont il faut avouer qu'on ne réussit pas à démontrer qu'elles sont vraies. Aucune des méthodes mathématiques utilisées pour sécuriser les cartes bancaires ou les échanges sur le réseau Internet n'a été prouvée inviolable. Se tourner vers des méthodes quantiques présente donc un intérêt évident.

C'est d'ailleurs pour cela qu'a été lancé, en avril 2004, un projet (financé par la Communauté Européenne) pour le développement d'un réseau global de communications sécurisées basé sur la cryptographie quantique (SECOQC, <www.secoqc.net>). Ce projet, ainsi que l'explique son initiateur Christian Monyck, est en partie motivé par le désir d'échapper à l'emprise du système de surveillance ECHELON.

Des produits sur le marché

Deux entreprises vendent aujourd'hui des solutions de cryptographie quantique. Il s'agit d'abord de *MagicQ Technologies, Inc* (New York) qui propose sa *Q-Box Workbench* (à but expérimental) et depuis novembre 2003 son système *Navajo (MagiQ QNP 350)*, le premier système de cryptographie quantique commercial. Le partage des clefs peut se faire sur une distance de 120 kilomètres à travers des fibres optiques. Cette limitation de distance - qu'on peut espérer voir évoluer rapidement (en particulier par la mise en place de réseaux quantiques spéciaux) - est la contrepartie de la sécurité absolue assurée par la technique quantique : pour que l'échange de clef puisse se faire, il faut relier les deux points concernés par une fibre optique ininterrompue.

La seconde entreprise est *id Quantique - spin off* de l'Université de Genève - installée à Carouge, qui propose aussi sa technologie de distribution de clefs depuis quelques mois (en plus d'un site Internet produisant des bits quantiques aléatoires et d'autres appareillages quantiques) (fig. 1 à 3).

Transmission de photons polarisés

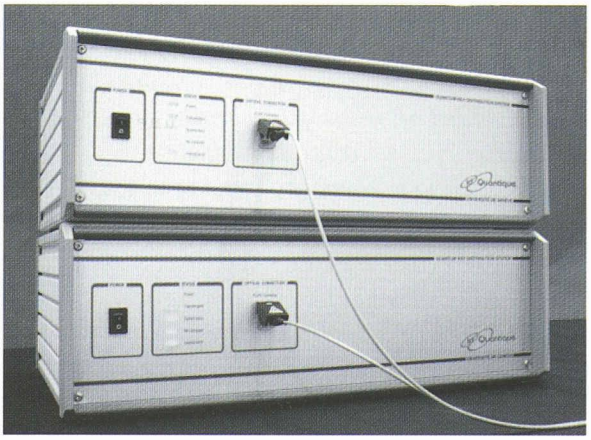
Comment cela fonctionne-t-il ? Plusieurs méthodes quantiques d'échanges de clefs ont été proposées. Certaines sont basées sur la non-localité, d'autres utilisent des photons

Fig. 1 : Système de cryptographie quantique développé par id Quantique *et l'Université de Genève (Photo* id Quantique, *Genève)*

Fig. 2 : Photo satellite illustrant une expérience de transmission de photons à travers une fibre optique, réalisée en février 2002 entre Lausanne et Genève. Plusieurs millions de photons ont été échangés. (Document id Quantique, *Genève)*

polarisés. Ce sont ces dernières qui pour l'instant ont la préférence des expérimentateurs et sont proposées à la vente. Voici la description rapide de la méthode.

Lorsqu'on fait passer un photon à travers un filtre polarisant d'orientation α, le photon est polarisé selon la direction α car le champ électrique associé au photon devient parallèle à l'axe α. Si on le fait passer ensuite dans un filtre polarisant de même orientation, le photon le traverse à coup sûr, ce qu'on peut constater en plaçant un détecteur derrière le deuxième filtre. Lorsqu'on fait passer un photon à travers un filtre d'orientation α, puis à travers un filtre d'orientation $\alpha + 90°$, le photon est absorbé par le second filtre. Si vous savez qu'un photon a été polarisé selon α ou $\alpha + 90°$, en mettant un filtre polarisant orienté selon α et un détecteur derrière le filtre, vous pouvez donc retrouver si le photon qui vous arrive a été polarisé selon α ou selon $\alpha + 90°$: s'il passe c'est qu'il avait l'orientation α, s'il ne passe pas c'est qu'il avait l'orientation $\alpha + 90°$ (voir aussi fig. 2, p. 13).

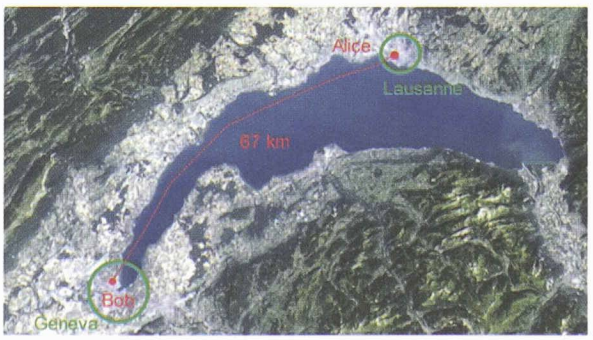


1

Qu'arrive-t-il si vous tentez d'intercepter un photon polarisé d'un angle α avec un filtre orienté d'un angle $\alpha + 45°$? Aléatoirement, une fois sur deux il passe, une fois sur deux il ne passe pas. Donc si vous vous trompez et que vous orientez votre filtre de $\alpha + 45°$, il vous est impossible de retrouver l'information codée, et une fois l'erreur commise il est impossible de revenir en arrière : l'information est perdue car en passant, le photon a été soit absorbé par votre filtre, soit polarisé par votre filtre, ce qui a détruit son ancienne polarisation.

Imaginons qu'on vous envoie un photon polarisé en convenant que « s'il est polarisé d'un angle α ou $\alpha + 45°$ cela signifie OUI, et s'il est polarisé selon un angle $\alpha + 90°$ ou $\alpha + 135°$ cela veut dire NON ». Comment savoir si l'information transmise est OUI ou NON ?

Première hypothèse : vous choisissez de lire la polarisation avec un filtre orienté selon α. Si le message est codé avec α ou $\alpha + 90°$ (polarisations rectilignes), vous réussirez à décoder correctement le message : si le photon passe, c'est que OUI est codé et dans le cas contraire c'est NON. Mais si



2

Fig. 3 : Sources de paires de photons intriqués utilisées pour des expériences de cryptographie quantique (Photo id Quantique, *Genève)*

le message est codé avec $\alpha + 45°$ ou $\alpha + 135°$ (polarisations transversales), vous lirez une réponse aléatoire et vous aurez perdu tout espoir de connaître l'information transmise. Seconde hypothèse : vous choisissez de lire le photon avec un filtre orienté de $\alpha + 45°$. Si le message est codé avec $\alpha + 45°$ ou $\alpha + 135°$, vous allez retrouver l'information, sinon, comme précédemment, vous trouverez quelque chose qui ne signifiera rien.

C'est seulement lorsqu'on vous dira si le message est codé de manière rectiligne (avec α et $\alpha + 90°$) ou transversale (avec $\alpha + 45°$ et $\alpha + 135°$) que vous saurez si ce que vous avez trouvé correspond bien au message. Un photon polarisé peut être vu comme une boîte contenant une information OUI ou NON et comportant deux modes d'ouverture : si vous utilisez le bon, vous tombez sur la bonne information, sinon vous trouvez quelque chose d'aléatoire qui ne signifie rien, sans possibilité de revenir en arrière.

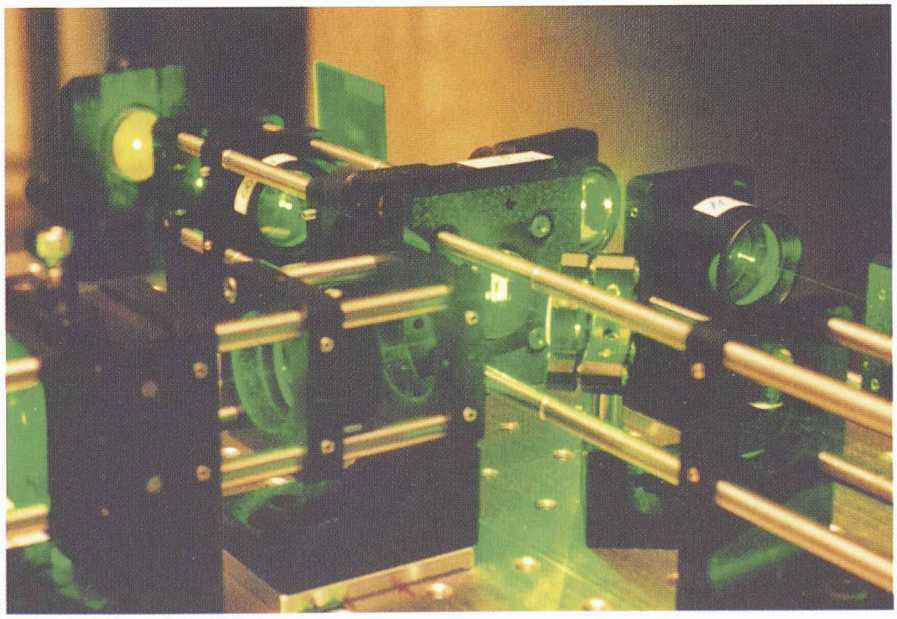
Mode d'emploi

Le protocole de partage des clefs se déduit de cette situation. (a) L'émetteur code une suite aléatoire de OUI et de NON selon le système précédent. (b) L'émetteur choisit au hasard pour chaque photon de coder de manière rectiligne ou transversale, mais garde en mémoire les choix de codage qu'il fait. (c) Le récepteur décode au hasard selon α ou $\alpha + 45°$, et donc, une fois sur deux en moyenne, retrouve ce que l'émetteur a codé, et une fois sur deux trouve quelque chose d'aléatoire. (d) Ensuite l'émetteur (par un autre canal qui n'a pas besoin d'être confidentiel, mais qui doit être infalsifiable, par exemple une onde radio) indique photon par photon si le codage était rectiligne ou transversal. (e) Le récepteur sait maintenant quels sont les bits qu'il a reçu qui sont corrects. (f) Il transmet à l'émetteur la liste des numéros des bits qu'il a correctement décodés. (g) L'émetteur et le récepteur possèdent maintenant une liste de bits communs. Cette liste est la clef partagée.

Le protocole peut être complété pour fournir la garantie qu'aucun espion n'est sur la ligne. Il faut sacrifier quelques-uns des bits communs. L'émetteur indique par exemple que le bit numéro 1 est OUI, que le bit numéro 6 est OUI, le bit numéro 13 est NON etc. Si le récepteur n'a pas précisément cette liste, c'est que leurs photons ont été interceptés. En effet, si un espion a épié la ligne et tenté de lire les photons polarisés puis de les réémettre, il n'a pu dans la première phase que les lire au hasard, comme le récepteur. Donc, une fois sur deux, il n'a pas choisi le bon axe de lecture, et donc, une fois sur deux, il a dû renvoyer un photon polarisé mal imité, et donc, une fois sur quatre, le photon retransmis par l'espion n'est pas celui que l'émetteur et le récepteur connaissent.

L'informatique quantique mûrit rapidement, et l'exemple de la cryptographie nous montre qu'elle pourrait nous concerner tous dans un avenir proche.

Jean-Paul Delahaye
Professeur à l'Université des Sciences et Technologies de Lille
Laboratoire d'Informatique Fondamentale de Lille
UMR CNRS 8022, Bât. M3, F - 59655 Villeneuve d'Ascq Cedex



3