Photons uniques et cryptographie quantique

Depuis une vingtaine d'années, de nombreux progrès ont été accomplis dans la maîtrise des propriétés quantiques élémentaires des sources lumineuses. Nous décrivons ici le principe et la réalisation d'une source de lumière émettant des photons un par un et à la demande. Cette source est ensuite mise en œuvre pour réaliser un dispositif complet de distribution quantique de clés de cryptage, fonctionnant entre deux bâtiments de notre laboratoire.

En 1900, Max Planck émet l'hypothèse de la quantification de l'énergie dans les processus d'émission et d'absorption de lumière, pour expliquer l'émission du corps noir. En 1905, Albert Einstein propose une interprétation corpusculaire de l'effet photoélectrique. Ces percées scientifiques fondamentales ont marqué les premiers pas de la mécanique quantique et sont à l'origine du concept de photon. Néanmoins, la notion de photon a très longtemps conservé un statut marginal en optique, car son insertion dans le formalisme ondulatoire « classique » est loin d'aller de soi. Ce formalisme ondulatoire, qui a été introduit par Fresnel vers 1820 et qui a atteint sa forme achevée avec les équations de Maxwell, a rencontré un immense succès. Il est capable de décrire la plupart des phénomènes lumineux d'interférence et de diffraction. Néanmoins, il présente une incompatibilité logique et mathématique avec la notion corpusculaire de « grain d'énergie » associée au concept de photon.

En fait, la nature cache souvent son étrangeté quantique à l'observateur macroscopique en multipliant le nombre des photons – la moindre source macroscopique de lumière émet des millions de milliards de photons par seconde – si bien que l'aspect corpusculaire de la lumière disparaît dans un flux qui semble continu. Cet effet de « moyennage » peut certainement être invoqué pour expliquer tous les succès du formalisme ondulatoire classique. Mais peu après l'apparition du laser – qui représente en un certain sens le champ lumineux le plus proche de l'onde classique idéale – d'intenses recherches ont été menées dans le but de construire des sources de lumière « spécifiquement quantiques », dont le principe de fonctionnement sort complètement du cadre de l'optique ondulatoire classique. C'est ainsi que s'est ouvert un nouveau champ de recherches : l'optique quantique, dont les bases théoriques ont été exposées dans un cours présenté par Roy Glauber à l'école d'été des Houches en 1964. L'un des défis majeurs de cette nouvelle discipline a été le développement de sources capables d'émettre des photons un par un et à la demande, ou « sources de photons uniques ». Ces travaux ont initialement été de nature fondamentale et ont surtout consisté en la mise en évidence d'effets spécifiquement quantiques. Mais, très rapidement, sont aussi apparues des propositions d'utilisations de ces nouvelles sources lumineuses aux propriétés surprenantes. En particulier, Charles Bennett et Gilles Brassard ont proposé en 1984 un protocole de « cryptographie quantique » (protocole BB84), utilisant des photons individuels pour réaliser la distribution de clés de cryptage. L'originalité et la puissance de cette méthode est que sa sécurité est garantie par les lois de la mécanique quantique.

Une source de photons uniques a été développée ces dernières années à l'Institut d'Optique d'Orsay. Ces travaux ont donné lieu, en 2002, à la première mise en œuvre du protocole BB84 utilisant des photons uniques. En 2003, en colla-

Article proposé par :

Gaetan Messin, gaetan.messin@iota.u-psud.fr, Laboratoire Charles Fabry de l'Institut d'Optique (LCFIO), CNRS/Institut d'Optique.
François Treussart, treussar@physique.ens-cachan.fr, Laboratoire de photonique quantique et moléculaire (LPQM), CNRS/ENS Cachan.

Ont également participé à ce travail :

A. Beveratos, R. Tualle-Brouri, J.-P. Poizat, P. Grangier du Laboratoire Charles Fabry de l'Institut d'Optique d'Orsay et R. Alléaume, Y. Dumeige, J.-F. Roch, du Laboratoire de Photonique Quantique et Moléculaire de l'ENS Cachan.

boration avec le LPQM de l'ENS de Cachan, le dispositif expérimental a été amélioré pour réaliser une démonstration de la distribution quantique de clés de cryptage entre deux ailes des bâtiments de l'Institut d'Optique, par transmission de photons uniques à l'air libre et dans des conditions normales d'éclairage nocturne. Ce sont ces travaux que nous présentons ici. Après avoir décrit la source de photons uniques, nous exposerons les grandes lignes du protocole de cryptographie quantique BB84. Nous expliquerons ensuite comment cette source a pu être intégrée dans un dispositif complet de distribution quantique de clés et quelles sont les performances de notre prototype.

Sources de photons uniques

Impulsions à un seul photon

Une source macroscopique de lumière produit un flux de photons lui-même macroscopique, c'est-à-dire composé d'un très grand nombre de photons. Pour décrire cette lumière, il est généralement suffisant de se contenter d'une approche ondulatoire. Ainsi, si l'on envoie sur une lame semi-réfléchissante une impulsion de lumière classique, l'impulsion est divisée en deux impulsions identiques, l'une transmise et l'autre réfléchie, d'intensités égales à 50 % de l'intensité originale. Si l'on place un photodétecteur sur le trajet de la lumière réfléchie et un autre sur le trajet de la lumière transmise, on observera deux signaux de photodétection coïncidant temporellement. Mais que se passe-t-il si l'impulsion envoyée sur la lame semi-réfléchissante contient un seul photon ? Ce photon sera en fait soit réfléchi, soit transmis, au hasard, avec une probabilité de 50 % pour chaque cas et on ne pourra donc *jamais* obtenir un signal sur chacun des photodétecteurs simultanément.

Considérant la lumière comme un flux de photons, on pourrait être tenté de penser que pour obtenir un photon unique, il suffit d'atténuer suffisamment une impulsion de lumière classique. En fait, il n'en est rien. Si l'on atténue une impulsion laser de façon à avoir un photon en moyenne dans chaque impulsion atténuée et que l'on envoie une telle impulsion sur une lame semi-réfléchissante, la probabilité d'obtenir un signal sur chacun des photodétecteurs simultanément (c'est-à-dire d'obtenir deux photons) est égale à la moitié de la probabilité d'en avoir un seul : un photon « en moyenne » est donc clairement très différent d'un photon « unique ». Si l'impulsion est atténuée encore plus fortement, de façon à ce que le nombre moyen de photon devienne très inférieur à un, l'impulsion contiendra rarement un photon et encore plus rarement deux photons. Mais ceci n'est pas non plus une impulsion à un photon, puisque que l'on a le plus souvent zéro photon (au lieu d'un), et que la probabilité d'avoir deux photons n'est jamais nulle (alors qu'elle devrait toujours l'être si l'on n'avait qu'un seul photon !). Il faut remarquer néanmoins que les impulsions laser atténuées (avec typiquement entre 0,01 et 0,1 photon/impulsion) ont été largement utilisées en cryptographie quantique en tant qu'« approximations » de source à un photon. Les défauts cités ci-dessus affectent alors les performances du système : les impulsions « vides » (zéro photon) entrainent une baisse du débit et les impulsions « doubles » (deux photons) affaiblissent la sécurité de la transmission.

Source de photons uniques

Une source de photons uniques n'est pas facile à réaliser car la nature produit en général de la lumière qui suit la statistique de Poisson conduisant aux nombres de photons par impulsion mentionnés au précédent paragraphe. Ceci est essentiellement dû au fait qu'une source macroscopique contient un très grand nombre d'atomes émetteurs. Pour obtenir une source de photons uniques, il faut en fait isoler un émetteur unique, ne pouvant émettre qu'un seul photon à la fois. C'est l'idée qui a guidé le groupe de Léonard Mandel à Rochester, qui, en 1976, a isolé *spatialement* l'émission d'atomes individuels, dans un jet atomique très dilué. Ces travaux sont considérés comme la première mise en évidence indubitable de la nature quantique de la lumière. Une autre expérience, isolant *temporellement* l'émission d'un seul atome, a été réalisée en 1986 à l'Institut d'Optique. Il existe beaucoup d'autres approches (cf. encadré 1), mais dans la suite de cet article nous allons nous concentrer sur une méthode très simple, permettant d'obtenir une source de photons uniques très stable, fonctionnant dans l'air à température ambiante. Cette source utilise en fait des centres colorés du diamant : il s'agit de défauts du diamant constitués de l'association d'un atome d'azote (N) et de la vacance d'un atome de carbone (V) dans la structure cristalline du diamant.

Les centres NV du diamant

Les centres NV sont actifs optiquement, ils absorbent et émettent dans le visible sur des plages de longueur d'onde distinctes (figure 1), ce qui permet de collecter leur lumière de fluorescence en la séparant de la lumière d'excitation. Ils se comportent pratiquement comme des systèmes à deux niveaux incohérents (voir figure 1 de l'encadré 1), sont fixes dans la maille cristalline du diamant, photostables à température ambiante et relativement peu concentrés, ce qui les rend facilement manipulables.

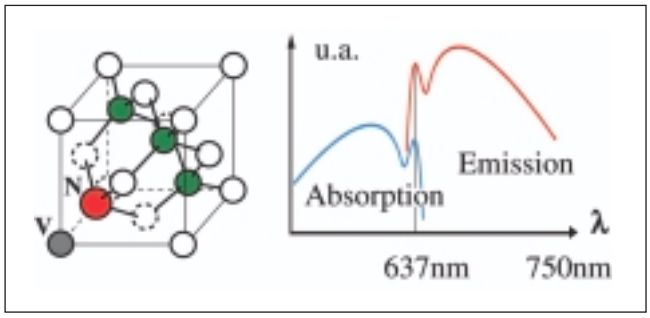

Figure 1 - *Centre NV dans la maille cristalline du diamant. Spectres d'absorption et d'émission.*

Encadré 1

Comment produire les photons un par un ?

Différents schémas pour produire les photons « à la demande » ont été imaginés au cours des dernières années. La plupart sont des variantes de l'idée de base qu'un émetteur quantique fluorescent individuel (une molécule, un atome, un « îlot quantique » semi-conducteur...) porté dans son état excité par une impulsion laser va émettre un photon et un seul. Dans le cas du centre coloré NV du diamant, une impulsion laser suffisamment énergétique porte l'émetteur individuel dans un état vibrationnel excité. Du fait du couplage avec la matrice cristalline, il se désexcite ensuite de façon non radiative (flèche en pointillé sur la figure 1) à l'intérieur du niveau électronique excité, puis de ce niveau électronique excité vers le niveau vibrationnel de plus basse énergie. Il émet ainsi un seul photon de fluorescence avant de revenir vers le niveau électronique fondamental.

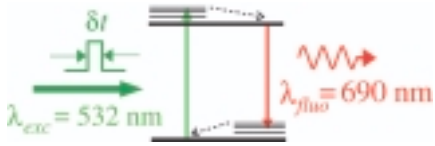

Figure 1 - *Excitation d'un émetteur unique.*

Si la durée t de l'impulsion de pompe est très petite devant la durée de vie radiative, mais grande devant la durée de relaxation non-radiative, le centre est excité une seule fois par impulsion et un unique photon est émis durant le cycle absorption–émission. Les photons peuvent être produits périodiquement à l'aide d'un laser impulsionnel dont la période de répétition est très grande devant la durée de vie radiative. La mise en œuvre de cette idée nécessite de détecter efficacement la lumière émise par le centre individuel. En principe, la méthode la plus efficace est de coupler l'émetteur à une microcavité optique, qui va « stimuler » l'émission par des effets d'électrodynamique en cavité. Cette approche a été mise en œuvre très récemment avec des émetteurs semi-conducteurs ou avec des atomes refroidis par laser. Une approche plus simple, qui est utilisée ici, est de concevoir un système optique de grande ouverture numérique, afin de recueillir la fraction la plus grande possible de l'émission spontanée du centre émetteur. Il faut alors aussi éliminer la lumière parasite, créée par exemple par la fluorescence de la matrice cristalline. On utilise pour cela un dispositif de microscopie confocale (figure 2 du corps du texte). Pour s'assurer qu'il n'y a qu'un seul émetteur au foyer de l'objectif, on enregistre les corrélations temporelles entre les photons de fluorescence (points noirs dans le « peigne » des impulsions d'excitation, figure 2). Le faisceau de fluorescence est séparé en deux parties de même intensité à l'aide d'une lame semi-réfléchissante, de part et d'autre de laquelle sont disposées deux photodiodes à avalanche au silicium fonctionnant en régime de comptage de photons. Un « convertisseur temps-amplitude » transforme le retard entre un photon détecté sur l'une des photodiodes (« Start ») et le suivant sur l'autre photodiode (« Stop »), en une tension proportionnelle à ce retard. Cette dernière alimente un « analyseur multicanal » dont la fonction est de construire en temps réel l'histogramme des retards entre photons consécutivement détectés.

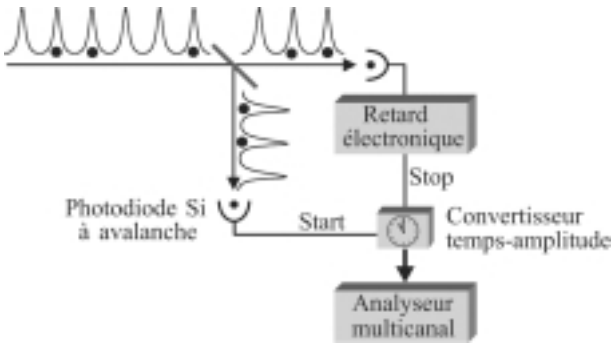

Figure 2 - *Mesure de corrélations de photons.*

Le diagramme obtenu (figure 3) présente une série de pics régulièrement espacés de la période de répétition du laser de pompe (ici 188 ns). Ces pics, qui correspondent aux coïncidences entre photons provenant d'impulsions décalées dans le temps, ont une largeur directement reliée à la durée de vie radiative du centre coloré, qui est ici proche de 20 ns. Les retards négatifs sont réalisés en faisant passer le signal provenant de l'une des deux photodiodes dans une ligne à retard (figure 2).

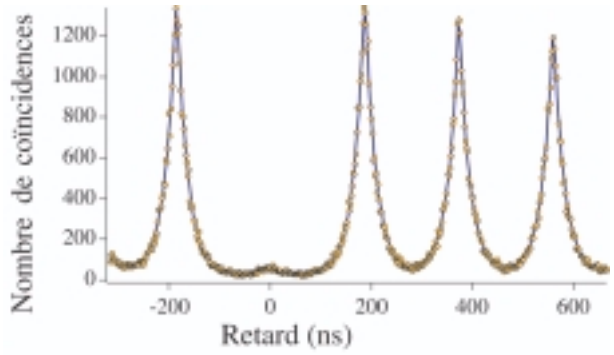

Figure 3 - *Diagramme de corrélation de photons.*

On observe au milieu de la fenêtre temporelle d'analyse le pic correspondant au retard nul, c'est-à-dire à une détection en coïncidence de part et d'autre de la lame séparatrice. Ce pic possède une aire beaucoup plus petite que celle de ses voisins et il disparaîtrait totalement pour une source de photons uniques idéale, car la détection simultanée de deux photons (ou plus), un sur chaque détecteur, est alors impossible. La persistance d'un pic résiduel révèle que la source comporte encore quelques événements mutiphotoniques, liés à la lumière parasite. Remarquons que l'existence d'un deuxième centre coloré dans le même nanocristal conduirait à une hauteur du pic central environ moitié de celle des pics adjacents. L'expérience démontre clairement l'unicité du centre émetteur, ainsi que du photon émis.

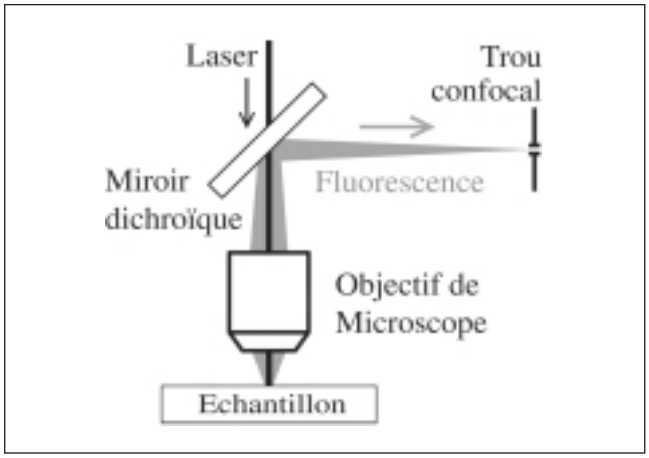

Figure 2 - *Principe de la microscopie confocale pour accroître le rapport signal sur fond en collectant la fluorescence d'un volume de l'ordre de 1 μm^3.*

L'excitation et la détection de centres NV uniques est faite au moyen d'un dispositif de microscopie confocale (figure 2). Un objectif de microscope de grande ouverture numérique focalise un laser d'excitation sur l'échantillon. La lumière de fluorescence est collectée par le même objectif suivi d'un filtre (miroir dichroïque) coupant le laser, puis elle passe par un trou de filtrage qui sélectionne les rayons provenant d'un petit volume autour de l'objet. Pour des raisons pratiques, on utilise des nanocristaux de diamant, d'un diamètre d'environ 90 nm, plutôt qu'un échantillon massif. Ils sont mélangés à un polymère en très faible concentration et dispersés sur une lamelle de microscope ou sur un miroir, ce qui permet d'accroître la quantité de fluorescence collectée. Les études menées sur ces nanocristaux en régime d'excitation laser continue ont permis d'observer l'émission, par un centre NV unique, de photons séparés temporellement.

Il est alors relativement facile d'obtenir une source émettant des photons un par un à la demande : il suffit de remplacer le laser d'excitation continu par un laser impulsionnel. Une impulsion d'une durée inférieure à la durée de vie radiative et d'intensité suffisante porte le centre NV dans son état excité avec une probabilité proche de 100 %. Au bout d'un temps de l'ordre de la durée de vie radiative du niveau électronique excité, un unique photon est émis et le centre coloré est prêt pour une nouvelle excitation (encadré 1). Dans notre cas, un laser impulsionnel émettant dans le vert (à 532 nm) a été développé et produit des impulsions d'une durée d'environ 1 ns, séparées de 188 ns ; l'intensité d'excitation moyenne est de quelques milliwatts. Avec ces paramètres, il est possible d'obtenir jusqu'à 150 000 photons uniques par seconde, émis dans le rouge autour de 690 nm, dans une bande spectrale d'une centaine de nanomètres de large.

Cryptographie quantique

Depuis les années 1980, le développement des télécommunications numériques a été accompagné par celui de la cryptographie à des fins autres que militaires (transactions financières, secret industriel). Le problème essentiel de la cryptographie est celui de la distribution des clés de cryptage ; en effet, les systèmes de cryptage mathématiquement les plus sûrs présentent une difficulté commune : ils sont à clé privée. Cela signifie qu'ils nécessitent une communication préalable des deux interlocuteurs, conventionnellement nommés Alice et Bob, pour se mettre d'accord sur le choix de la clé qu'ils devront utiliser pour coder et, symétriquement, pour décoder. Cette communication préalable devra être sûre, car si un espion, appelé Eve (jeu de mot avec l'anglais to *eavesdrop*, écouter clandestinement), entre en possession de cette clé, il pourra décoder tous les messages qu'il verra passer. D'où l'idée d'utiliser des systèmes de codage ne nécessitant pas de clé privée commune.

Le protocole « RSA »

La solution retenue et largement utilisée jusqu'à maintenant, en particulier sur Internet, a été mise au point en 1977 par Rivest, Shamir et Adleman : c'est le protocole « RSA ». Il s'agit d'un protocole de cryptographie asymétrique reposant sur l'usage de deux clés : une clé publique et une clé privée. La clé publique sert au codage et utilise un algorithme difficilement inversible qui ne permet le décodage qu'au moyen de la clé privée. Pratiquement, Alice choisit une clé privée et génère la clé publique correspondante, qu'elle diffuse alors publiquement. Bob utilise la clé publique d'Alice pour coder un message, l'envoie publiquement à Alice qui est la seule à pouvoir le décoder au moyen de sa clé privée. La sécurité de ce protocole est garantie par la complexité algorithmique, c'est-à-dire par l'impossibilité pratique de déduire la clé de décryptage privée de la clé de cryptage publique avec les moyens informatiques connus dans un délai raisonnable. Rien ne prouve cependant que cette sécurité ne soit pas mise à mal dans un futur proche par l'évolution rapide des algorithmes et des matériels.

Le protocole BB84

Le protocole de cryptographie quantique proposé par Bennett et Brassard en 1984 (BB84) est une autre solution au problème de distribution de clés privées : il permet à deux personnes séparées spatialement de construire ensemble une clé secrète qu'ils seront les seuls à connaître, par l'envoi de l'une vers l'autre de photons uniques. Son avantage essentiel est que la sécurité est garantie, cette fois, par les lois de la physique quantique.

Le principe central de BB84, comme celui d'autres protocoles de cryptographie quantique qui ont été proposés par la suite, est qu'Alice va coder les bits qu'elle veut transmettre à Bob sur des grandeurs quantiques incompatibles, c'est-à-dire qui ne peuvent pas être connues simultanément (au sens du principe de Heisenberg). C'est par exemple le cas pour deux polarisations non orthogonales d'un photon unique (voir encadré 2). L'information envoyée par Alice

sera donc essentiellement ambiguë et toute personne essayant de l'extraire va commettre des erreurs. Ceci n'est pas gênant pour Bob, car les bits erronnés pourront être éliminés ultérieurement par une discussion publique, qui ne révèlera pas les bits corrects (voir encadré 2).

Sécurité du protocole

Que se passe-t-il par contre si un espion, Eve, tente d'intercepter les communications entre Alice et Bob ? On suppose généralement que l'objectif d'Eve est d'intercepter le plus d'information possible sans être détectée et qu'elle dispose pour cela de tous les moyens que ne lui interdit pas la mécanique quantique. Mais au moment où elle peut agir sur un photon transmis d'Alice vers Bob, elle ne sait pas sur quelle polarisation l'information a été codée. Si elle tente malgré tout d'extraire cette information, elle va non seulement faire des erreurs, mais elle va aussi en faire apparaître chez Bob. Afin de déceler la présence d'Eve, le « taux d'erreur » (fraction de la clé entachée d'erreur) est évalué par Alice et Bob. Pour cela Bob révèle publiquement à Alice une petite partie de la clé brute. A partir de cette évaluation du taux d'erreur, Alice et Bob estiment la quantité maximale d'information qu'Eve a pu intercepter. Une fois cette estimation réalisée, un traitement classique de l'information permet finalement de réduire à néant l'information acquise par Eve, au prix, il est vrai, d'une réduction de la taille de la clé. Notons que la probabilité d'avoir des photons émis deux par deux rentre dans l'évaluation de la quantité d'information qu'Eve peut extraire : plus cette probabilité est élevée, plus Eve peut obtenir d'information et plus la clé s'en trouvera raccourcie.

Le protocole BB84, qui est maintenant très bien compris théoriquement, a aussi été très vite mis en œuvre en laboratoire, d'abord par ses auteurs en 1987. Cependant, les physiciens ne disposaient pas à l'époque de source de photons uniques et ils ont dû utiliser pour les simuler des sources d'impulsions classiques suffisamment atténuées pour que le taux de photons émis deux par deux soit assez bas. Quelques sociétés spécialisées proposent même, aujourd'hui, des dispositifs commerciaux fonctionnant sur ce principe. Afin de rendre la sécurité du protocole optimale, il reste nécessaire d'utiliser une véritable source de photons uniques (voir encadré 2 et figure 4).

Cryptographie quantique avec des photons uniques

Disposant à l'Institut d'Optique d'une source de photons uniques compacte, stable et fonctionnant à température ambiante, c'est tout naturellement qu'a été entreprise la construction d'un dispositif de cryptographie quantique reposant sur le protocole BB84.

Le dispositif, schématisé figure 3, est composé de deux montages indépendants, l'un correspondant à Alice, l'autre correspondant à Bob. Chacun est contrôlé par un ordinateur. Le canal de communication quantique consiste en la transmission de photons polarisés d'Alice vers Bob à l'air libre ; le canal de communication classique utilise le réseau Internet. Les phases de réconciliation et de purification (cf. encadré 2) sont effectuées automatiquement *via* Internet au moyen du programme « QuCrypt », développé par L. Salvail à l'Université de Aarhus (Danemark), installé sur chaque ordinateur.

Alice et Bob

Chez Alice se trouve la source de photons uniques décrite plus haut. Un polariseur intégré à la source assure que tous les photons émis ont la même polarisation. Afin de vérifier que l'on a bien des photons uniques, un miroir amovible permet d'envoyer le flux produit sur un montage de mesure de corrélations de photons, identique à celui décrit dans l'encadré 1. Lorsque le miroir amovible est enlevé, les dis-

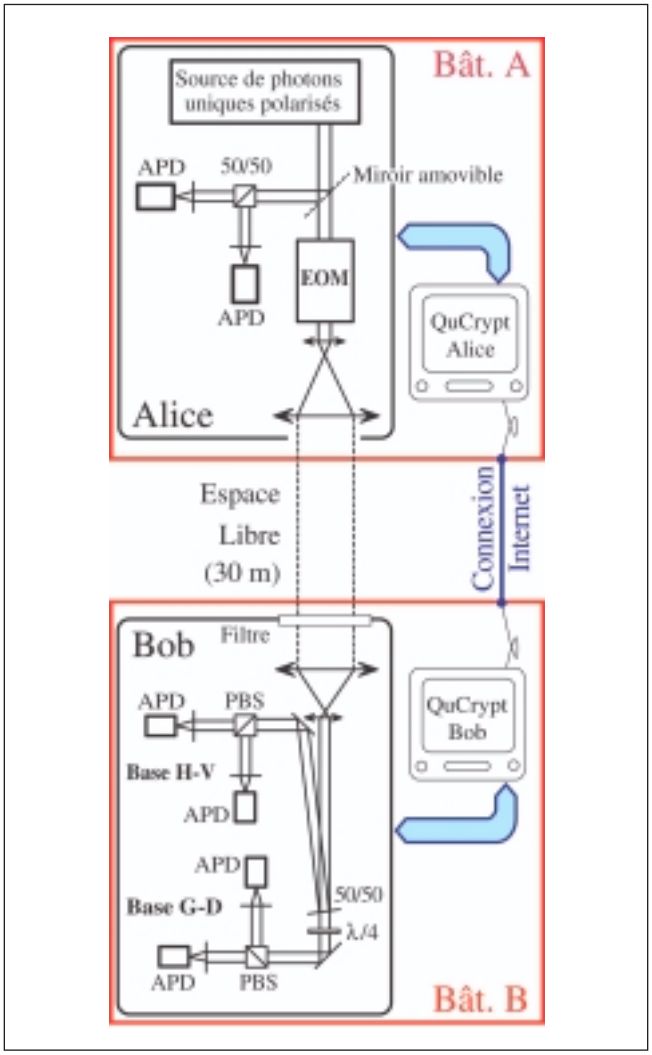

Figure 3 - *Montage pour l'expérience de cryptographie quantique avec une source de photons uniques. APD : photodiodes à avalanche en régime de comptage de photons ; PBS : cube séparateur de polarisation ; EOM : modulateur électro-optique ; 50/50 : lame semi-réfléchissante ; λ/4 : lame quart d'onde.*

Encadré 2

Protocole de cryptographie quantique BB84

Le protocole BB84 permet à deux protagonistes (Alice et Bob) de construire ensemble une clé de cryptage connue d'eux seuls. Il repose sur le codage par Alice et le décodage par Bob de la polarisation d'une séquence de photons uniques sur quatre états choisis dans deux « bases de polarisation » de la lumière, perpendiculaires au faisceau : dans notre expérience, nous utilisons une base linéaire, correspondant aux polarisations orthogonales Horizontale (H) et Verticale (V), et une base circulaire correspondant aux polarisations orthogonales Droite (D) et Gauche (G). Le protocole se déroule en trois étapes, illustrées par la figure 2. Premièrement, Alice choisit aléatoirement un bit (0 ou 1) pour chaque photon unique de la séquence et elle le code sur la polarisation de ce photon. Il faut pour cela qu'elle choisisse au hasard une base de codage en polarisation (linéaire ou circulaire), puis qu'elle utilise, par exemple, la convention H=1, V=0 si elle choisit la base linéaire et D=1, G=0 si elle choisit la base circulaire, comme représenté figure 1.

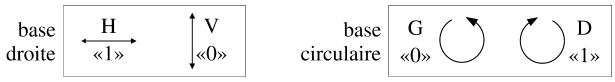

Figure 1 - *Bases linéaire et circulaire et bit codés.*

Le photon ainsi polarisé est envoyé à Bob par un canal de transmission « quantique », qui peut être simplement une fibre optique ou l'air libre. Pour chaque photon susceptible d'être reçu (idéalement tous, s'il n'y pas de perte) Bob effectue une mesure de polarisation en choisissant aléatoirement la base linéaire ou la base circulaire. Il obtient ainsi, en utilisant toujours la convention de la figure 1, une séquence de bits appelée clé brute*, qui diffère de celle envoyée par Alice, parce que sa base de mesure n'est pas toujours celle choisie par Alice, mais aussi simplement à cause d'une erreur de transmission.*

Lors de la seconde étape, appelée réconciliation*, Alice et Bob se communiquent publiquement leurs choix de base et excluent tous les bits de la séquence pour lesquels les polarisations des photons n'ont pas été codées et mesurées dans les mêmes bases. Il ne reste donc dans cette* clé filtrée *que les erreurs de mesure (ou de codage) : ici un « 0 » dans la figure 2.*

Dans la troisième étape, dite de purification*, Alice et Bob estiment le taux d'erreur dans leur clé en comparant publiquement une faible fraction de leurs séquences respectives, qui est donc sacrifiée. Cette évaluation des erreurs est fondamentale, car elle renseigne Alice et Bob sur l'information dont a pu s'emparer un espion éventuel, Eve. Par prudence, toutes les erreurs sont attribuées à Eve, dont les moyens techniques ne sont limités en principe que par les lois de la physique. La purification effectuée ensuite est une opération purement algorithmique. Tout d'abord, Alice et Bob corrigent les erreurs encore présentes : lorsque le taux d'erreur est assez bas, des algorithmes de correction d'erreur permettent de produire efficacement des clés parfaitement identiques chez Bob et Alice. Ensuite, ils réalisent une* amplification de confidentialité*, qui réduit la taille de la clé, mais qui « brouille » toute connaissance résiduelle qu'Eve pourrait avoir de la clé finale. Pour que cet algorithme fonctionne, il faut qu'ils aient une évaluation de la quantité d'information connue d'Eve. C'est précisément ce qui a été obtenu lors de l'étape précédente : il existe un lien quantitatif entre l'information acquise par Eve et le taux d'erreur mesuré par Bob.*

À la fin de toutes ces opérations, Alice et Bob partagent donc une clé totalement secrète, qui sera de taille non nulle à condition que le taux d'erreur initial évalué par Alice et Bob ne soit pas trop élevé (en pratique inférieur à 10 %).

Si les photons utilisés dans le protocole ne sont pas uniques, comme c'est le cas avec des impulsions atténuées, Eve peut, en théorie, prélever les photons surnuméraires pour gagner de l'information sans être repérée. L'étape de purification tient compte de cette possibilité et inclut dans l'évaluation de la quantité d'information maximale dont peut disposer Eve la probabilité d'avoir plus d'un photon. Plus cette probabilité est grande et plus il faudra réduire la taille de la clé pour garantir la sécurité. On voit donc là tout l'intérêt d'avoir des sources de photons uniques : à grande distance, lorsque les pertes deviennent importantes, une source de photons uniques permet encore d'extraire une clé de taille non nulle là où des impulsions atténuées ne le permettent plus (cf. figure 4 du corps du texte).

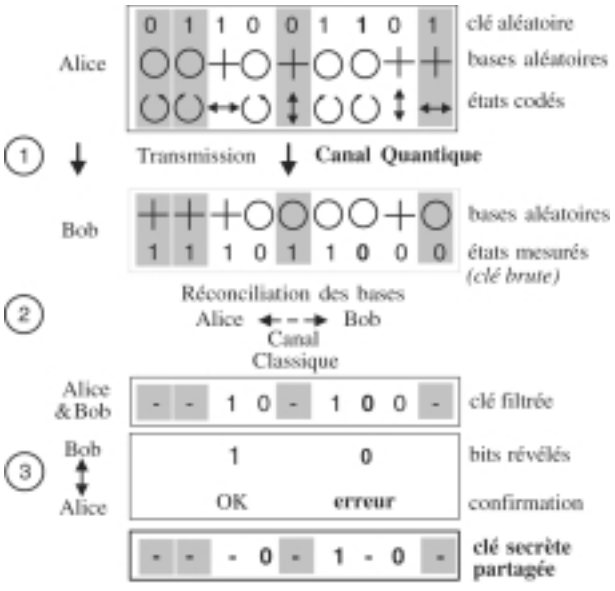

Figure 2 - *Partage d'une clé secrète.*

positifs d'Alice et de Bob permettent de réaliser le protocole BB84 décrit dans l'encadré 2. Chaque photon unique polarisé traverse un modulateur électro-optique qui permet, par l'application d'une tension choisie par Alice, de transformer sa polarisation en l'une quelquonque des quatre polarisations du protocole BB84. Le photon est ensuite transmis à Bob au moyen d'un système afocal grossissant qui permet de réduire la divergence du faisceau.

L'électronique de contrôle d'Alice permet d'envoyer des séquences durant 0,2 s, correspondant à un million d'impulsions d'excitation et, pour chacune de ces impulsions, à un état aléatoire du modulateur électro-optique, mémorisé dans l'ordinateur d'Alice. Seul un petit nombre de ces impulsions correspond effectivement à l'émission d'un photon unique polarisé vers Bob : une partie est perdue dans la source elle-même au niveau de la collection par l'objectif de microscope, une autre partie est perdue lors de la polarisation des photons uniques et quelques photons sont perdus ensuite à cause des facteurs de transmission de divers éléments optiques. Finalement, environ 25 000 photons sont réellement envoyés vers Bob.

Chez Bob, situé à 30 mètres d'Alice et dans un autre bâtiment, un filtre optique passe-bande centré sur la longueur d'onde des photons uniques permet d'éliminer une grande partie de la lumière ambiante. Cela est suffisant pour faire fonctionner le disposif en extérieur de nuit, en présence d'éclairage public. Un dispositif afocal identique à celui d'Alice collecte les photons uniques et les dirige vers une lame semi-réfléchissante. Cette lame envoie chaque photon vers l'un ou l'autre des deux systèmes de lecture de l'information correspondant soit à la base linéaire, soit à la base circulaire. C'est ainsi que Bob choisit aléatoirement une base de décodage pour chaque photon. Pour chacune des deux bases, un séparateur de polarisation et deux photodiodes à avalanche identiques à celles se trouvant chez Alice permettent de mesurer l'état de polarisation du photon reçu. Un système d'acquisition électronique permet de stocker les résultats de ces mesures dans l'ordinateur de Bob. A cause des pertes optiques et de l'efficacité quantique des détecteurs (environ 60 %), seulement 30 % des photons envoyés sont ainsi mesurés par Bob. Ces opérations constituent la première étape du protocole BB84 tel qu'il est décrit dans l'encadré 2. Elles donnent lieu à une clé brute d'environ 7500 bits pour une séquence d'une durée de 0,2 s.

Performances

La réconciliation conduit à une clé filtrée d'environ 3700 bits. En pratique, plusieurs séquences sont échangées. Certaines sont utilisées pour calibrer le taux d'erreur dont la valeur était inférieure à 2 % lors de nos expériences. On peut alors procéder à la phase mathématique de purification (correction des erreurs et amplification de confidentialité). A la fin de cette phase, la clé secrète purifiée contient environ 3000 bits par séquence, soit un taux de transmission de clé partagée de l'ordre de 15 kbits/s sur le canal quantique.

Finalement, l'intérêt de l'utilisation d'une source à photons uniques est illustré par la figure 4. Elle représente le taux de bits secrets en fonction de pertes par atténuation introduites sur la ligne de transmission afin de simuler une propagation à grande distance. On constate qu'une source d'impulsions atténuées ne permet plus de transmettre une clé en présence d'une atténuation de 12 dB, qui correspond à une perte de 93.7 % simulant la propagation sur une longue distance, alors que ceci est encore possible avec notre source de photons uniques.

Notons que dans le cas de la source d'impulsions atténuées le nombre de photons moyen par impulsion $\langle n \rangle$ est facilement contrôlé expérimentalement. Ce nombre peut ainsi être optimisé pour chaque valeur de l'atténuation afin de produire le taux de bit secrets le plus élevé compatible avec les contraintes de sécurité que nous nous fixons (courbe en tirets noirs sur la figure 4). Malgré cette optimisation, la source de photon unique présente toujours un avantage sur la source d'impulsions atténuées lorsque l'atténuation ajoutée sur la ligne est suffisamment grande.

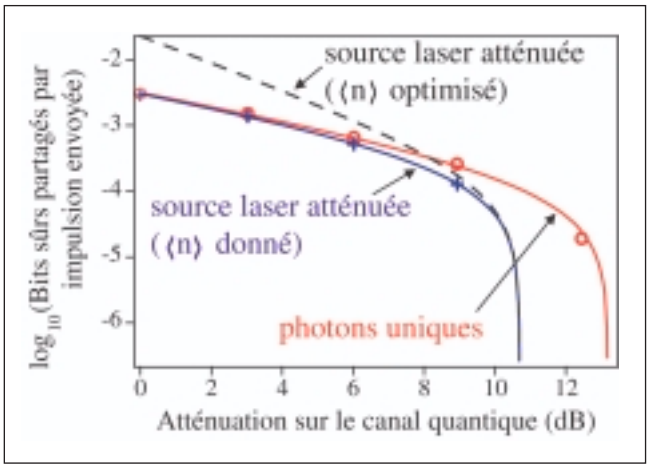

Figure 4 – *Comparaison des performances d'un système de distribution de clé utilisant soit des photons uniques, soit des impulsions atténuées.*

Perspectives

Notre dispositif a clairement permis de démontrer, pour la première fois, la faisablilité d'un dispositif de cryptographie quantique utilisant des photons uniques et reposant sur le protocole BB84. Depuis, une autre expérience a été réalisée à l'université de Stanford, en utilisant une source cryogénique basée sur l'émission d'îlots quantiques semiconducteurs. Notre prototype a été capable de fonctionner de nuit et à l'air libre. La distance sur laquelle il peut fonctionner n'est pas limitée à 30 mètres : nous avons simulé, par des atténuations sur le canal quantique, un fonctionnement sur des distances pouvant atteindre plus de 300 km verticalement, en vue d'une transmission vers un satellite. L'augmentation de cette distance limite passe par l'amélioration des qualités de la source de photons uniques : efficacité de

collection des photons uniques, directivité, affinement du spectre d'émission (qui nous permettra de mieux isoler spectralement la source de la lumière ambiante), taux de photons émis deux par deux réduit. Des études continuent d'être menées dans ce sens à l'ENS de Cachan.

L'utilisation de sources de lumière quantique n'en est qu'à ses débuts. A l'Institut d'Optique, des systèmes de cryptographie quantique par variables continues sont en développement : au lieu d'utiliser des photons uniques et des bases de polarisation, ces systèmes utilisent des impulsions à faible nombre de photons et l'information est codée dans l'amplitude et la phase du champ lumineux. Ces dispositifs semblent très prometteurs et intéressent déjà certains acteurs du monde industriel.

Pour en savoir plus

Beveratos (A.), Brouri (R.), Gacoin (T.), Villing (A.), Poizat (J.-P.) et Grangier (P.), « Phys. Rev. Lett. », 89, 2002, p. 187901.
Alléaume (R.), Treussart (F.), Messin (G.), Roch (J.-F.), Dumeige (Y.), Beveratos (A.), Brouri (R.), Poizat (J.-P.) et Grangier (P.), « New Journal of Physics », 6, 2004, p. 92.
Gisin (N.), Ribordy (G.), Tittel (W.) et Zbinden (H.), « Rev. Mod. Phys. », 74, 2002, p. 145.