Appendix II:

Aspects techniques de la Cryptographie quantique.

1 La cryptographie, introduction.

Les techniques dites de cryptographie visent à envoyer des messages de telle manière que seule une personne autorisée puisse avoir accès à l'information présente dans le message. Pour ce faire, le message original est remplacé par un autre message, réplique du premier sous forme codée. Pour retrouver le message d'origine, il faut inverser la transformation qui l'applique sur sa réplique codée (décoder). En général, cette opération est très difficile, voire impossible à réaliser à moins de posséder des informations sur la technique de codage. Les techniques actuelles de décodage nécessitent l'usage d'une clé qui peut être mise sous la forme d'une série de nombres binaires. La technique de Vernam ([1]), communément appelée *one time pad*, par exemple, a été utilisée avec succès pendant la guerre froide afin d'assurer la confidentialité de la ligne directe entre Moscou et Washington (le fameux téléphone rouge). Elle nécessite une clé dont la longueur est égale à la longueur du message à transmettre. Par exemple, supposons que le message secret consiste en la série (1, 0, 1, 1, 0) et que la clé soit donnée par la série (0, 1, 1, 0, 0). On suppose ici que seuls le récepteur et l'émetteur ont connaissance de la clé. L'émetteur peut alors envoyer, sur un canal public ouvert à tous telles que la radio ou la télévision, la série (1, 1, 0, 1, 0) obtenue en sommant le message et la clé "modulo 2" (1+0 = 1, 0+1 = 1, 1+1 = 0, 1+0 = 1, 0+0 = 0). Il suffit à l'émetteur de sommer cette série avec la clé (1+0 = 1, 1+1 = 0, 0+1 = 1, 1+0 = 1, 0+0 = 0) pour retrouver le message d'origine. Pour quelqu'un qui ne connait pas la clé, le message public est absolument dénué

d'information et pourrait aussi bien signifier chacune des 32 séries formées de cinq nombres binaires[1].

La technique de Vernam présuppose la possibilité pour l'émetteur de transmettre confidentiellement des clés (parfois très longues) à l'émetteur. En pratique, ceci n'est pas toujours simple. Les clés nécessaires au "téléphone rouge", par exemple, étaient transmises sous forme de bandes enregistrées par l'intermédiaire de courriers militaires sous haute surveillance. Ce type de transmission est onéreux, loin d'être pratique et tout bonnement irréalisable dans la plupart des domaines d'application de la cryptographie (transmission d' informations confidentielles entre banques, entre différents états-majors ou ministères...). De là, l'intérêt évident pour toute technique susceptible de transmettre une clé (série de nombres binaires) avec une garantie élevée de confidentialité. Les techniques de cryptographie quantique permettent précisément d'atteindre cet objectif en restant opérationnelles et réalisables concrètement comme nous allons le montrer dans ce chapitre.

2 Principes de base de la cryptographie quantique.

2.1 Aspects non-classiques de la mesure en mécanique quantique.

La description quantique du processus de la mesure se démarque de la description classique par deux éléments essentiels : le caractère fondamentalement probabiliste

[1]Remarque: Shannon ([2]) a montré que de telles techniques présentent une garantie de confidentialité absolue, à la différence de la plupart des techniques actuelles de cryptographie qui font usage de clés plus courtes que le message à transmettre. Les techniques utilisées pendant la seconde guerre mondiale dont elles sont inspirées se basent sur la décomposition d'un nombre sous la forme d'un produit de deux nombres premiers. Cette factorisation nécessite actuellement un temps de calcul fort long mais pas infini. C'est pourquoi ces techniques présentent toutes une garantie de confidentialité limitée. Elles sont tributaires des progrès réalisés en mathématique et en informatique. Un autre exemple de technique à confidentialité limitée nous est fourni par Edgar Allan Poe dans "Le scarabée d'or". Le message est obtenu par simple permutation des lettres de l'alphabet. Le héros compte quelles sont les lettres qui reviennent le plus souvent. En comparant leurs fréquences avec les fréquences moyennes des lettres les plus usitées dans la langue anglaise (dans l'ordre e, a, o, i, d, b...), il retrouve par quelle lettre celles-ci ont été remplacées. Après quelques tâtonnements, il peut alors recomposer l'entièreté du message.

du processus de mesure et la perturbation occasionnée par celui-ci. Pour illustrer ces deux aspects non-classiques de la mesure quantique, considérons le système quantique le plus simple: un système dont l'état est décrit par un espace de Hilbert bidimensionnel. Ce système peut être concrétisé par le spin d'une particule de spin 1/2 (figure 1), par la polarisation d'un photon (figure 2), par l'état d'un électron atomique pour lequel deux niveaux d'énergie seulement sont accessibles, etc.

Tout état du système peut être exprimé comme superposition de deux états de base orthogonaux $|+\rangle$ et $|-\rangle$:

$$|\psi\rangle = \alpha|+\rangle \ + \ \beta|-\rangle. \tag{1}$$

Les amplitudes α et β sont des nombres complexes dont la somme des modules au carré est normalisée à l'unité. Selon les axiomes de la mécanique quantique, on peut associer à toute mesure effectuée sur le système un opérateur auto-adjoint (observable).

Par exemple, l'observable associée à la mesure de l'orientation du spin d'une particule de spin 1/2 réalisée lors de l'expérience de Stern et Gerlach (figure 1) est définie par l'opérateur auto-adjoint $\frac{\hbar}{2}\,\sigma_z$, ou

$$\sigma_z = (|+\rangle\langle+|) \ - \ (|-\rangle\langle-|). \tag{2}$$

Dans cet exemple, $|+\rangle$ et $|-\rangle$ représentent les états dont les spins sont respectivement parallèles et antiparallèles au champ magnétique créé dans l'appareil de mesure de Stern et Gerlach. Toujours selon la mécanique quantique, les résultats possibles de la mesure correspondent aux valeurs propres $+\frac{\hbar}{2}$ et $-\frac{\hbar}{2}$ de l'observable, et sont observés avec les probabilités respectives $|\alpha|^2$ et $|\beta|^2$.

Comme on peut le constater, seuls les états propres de l'observable $|+\rangle$ et $|-\rangle$ ont un spin dont l'orientation selon la direction du champ magnétique est définie sans équivoque (probabilités respectives 1 et 0 d' observer une orientation parallèle au champ). Pour tous les autres états, il est impossible de prédire avec certitude quel sera le résultat de la mesure ; on peut connaître tout au plus les probabilités associées aux différents résultats possibles. Ceci illustre un premier aspect par lequel le formalisme quantique se démarque de l'intuition classique : les prédictions permises par la théorie portent essentiellement sur les probabilités d'observer tel ou tel résultat, sans plus.

En ce qui concerne l'état du système après la mesure, il existe actuellement différentes interprétations contradictoires à propos de ce qui se passe réellement (collapse de la fonction d'onde, décohérence, *empty waves*, *many worlds*, etc. ...). Quoi qu'il en soit, ces interprétations s'accordent sur un point : l'acte de mesure perturbe profondément l'état du système dès lors qu'il n'est pas état propre de l'observable associée à la mesure. Que l'on décrive cette perturbation par une projection comme le font les adeptes de l'interprétation du collapse à la von Neumann ou que l'on considère que l'état du système en tant que tel disparait pour former un état non-produit extrêmement complexe avec l'appareil de mesure comme le suggèrent les partisans de l'approche basée sur la décohérence n'y change rien : après une mesure, l'état du système individuel avant la mesure n'est plus accessible. Ceci illustre un second aspect "étrange" du formalisme quantique : il est impossible de connaître "réellement" l'état d'un système car la mesure même qu'on lui fait subir altère ses propriétés.

2.2 Application à la cryptographie.

Ces deux aspects non-classiques ont été mis à profit dans la cryptographie quantique. Lors de la première réalisation expérimentale d'une technique de cryptographie quantique par Bennet et al. en 1992, la clé était transportée par des photons, et codée par l'intermédiaire de leur polarisation. L'espace de Hilbert associé aux états de polarisation d'un photon est bi-dimensionnel. Soit $|+\rangle$ et $|-\rangle$, deux états dont les polarisations linéaires dans le plan transverse perpendiculaire à la direction de propagation du photon définissent une base orthogonale de ce plan. Tout état de polarisation peut être exprimé comme superposition de ces deux états de base:

$$|\psi\rangle = \alpha|+\rangle \ + \ \beta|-\rangle. \tag{3}$$

Par exemple, un état de polarisation linéaire transversé selon une direction d'angle θ dans la base ainsi définie peut être exprimé comme superposition à coefficients réels des deux états de base $|+\rangle$ et $|-\rangle$:

$$|\psi\rangle = cos\theta|+\rangle \ + \ sin\theta|-\rangle. \tag{4}$$

Si on analyse la polarisation d'un tel état dans un polariseur dont les états propres sont les états $|+\rangle$ et $|-\rangle$, on retrouve la loi de Malus : la probabilité d'obtenir une polarisation + (-) vaut $cos^2\theta$ ($sin^2\theta$). Après une telle mesure, il est impossible de "poser d'autres questions" au photon, celui-ci ayant été irrémédiablement détruit par le détecteur.

Comment est-il possible de mettre à profit ces deux aspects intrinsèquement quantiques de l'acte de mesure, stochasticité et destruction de l'information initiale dans le cadre de la cryptographie ?

L'idée de base est la suivante : supposons que la clé envoyée par l'émetteur soit codée par le biais de la direction de polarisation des photons qu' il émet, et que, de plus, le choix de la base dans laquelle s'effectue la polarisation soit fait au hasard. Dès lors, si un espion tente d'intercepter le signal, il se présentera des cas où sa base de détection (en fait, la direction de son filtre polariseur) ne coïncide pas avec la base de l'émetteur. On se trouve alors dans une situation où le processus de mesure est de nature stochastique et détruit l'information initiale. Cela signifie que, lorsque l'espion retransmet un signal équivalent à celui qu'il a intercepté, il reproduit non pas la série des polarisations initiale, mais une série tronquée. Le signal mesuré par le récepteur est dès lors entaché d'erreur. Mieux, il existe, comme nous allons le montrer, un rapport constant entre la quantité d'information interceptée par l'espion et la perturbation du message qu'il occasionne. L'erreur étant cumulative, on peut dès lors évaluer, sur base du taux d'erreur, la quantité maximale d'informations interceptées par un espion éventuel.

Il est intéressant de noter que les concepts non-classiques qui ont permis l'élaboration de la cryptographie quantique, étaient déjà présents dans la fameuse *gedanken experiment* du microscope dont Heisenberg a déduit son principe d'incertitude ([3]). Là aussi, le processus de mesure présente des aspects indéterministes et perturbe l'état du système observé. Dans la formulation rigoureuse de ces incertitudes (faite ultérieurement par Robertson, [4]), le commutateur (non nul) de deux observables complémentaires joue un role essentiel. Ici aussi, l'utilisation de deux observables non compatibles est un élément essentiel à la faisabilité de la technique.

Dans un contexte classique, par contre, il est, en principe, toujours possible de mesurer un signal sans le perturber. Au cours d'une écoute téléphonique, par exemple, on n'empêche pas la bonne transmission de la conversation. Il est dès lors impossible de corréler le taux d'erreur dans la transmission et l'information dont dispose l'espion.

3 Description d'une technique de cryptographie quantique.

3.1 Codage et transmission de la clé.

Nous présentons dans cette section la toute première technique de cryptographie quantique (le protocole de Bennet et Brassard dont la formulation théorique a été publiée en 1984), telle qu'elle a été réalisée expérimentalement par Bennet, Bessette, Brassard, Salvail et Smolin en 1992 ([5]). Dans cette technique, le signal est codé selon la direction de polarisation des photons envoyés de l'émetteur au récepteur (figure 2). La direction de l'axe du polariseur utilisé pour filtrer la polarisation des photons émis par l'émetteur est choisie au hasard par un générateur de signaux stochastiques parmi les quatre directions 0, 45, 90 et 135 degrés (par rapport à une direction de référence conventionnelle). L'émetteur peut alors se mettre d'accord avec le récepteur pour assigner une valeur binaire à chaque polarisation (par exemple, 0 et 45 degrés signifient 1; 90 et 135 degrés signifient 0). Grâce à cette convention, la série des polarisations mesurées par le récepteur constitue la clé. Le récepteur choisit au hasard (figure 3) la base de détection (la direction de son filtre polariseur) parmi les bases (0, 90) et (45, 135).

Il arrive en moyenne une fois sur deux que la base d'émission et la base de détection coïncident. Dans ce cas, l'état de polarisation du photon incident est état propre de l'observable associée à la détection et l'acte de mesure est essentiellement classique : la valeur codée est correctement mesurée par le récepteur avec probabilité 100 %.

Il arrive en moyenne une fois sur deux que la base d'émission et la base de détection ne coïncident pas. Ceci arrive par exemple lorsque l'émetteur filtre la polarisation du photon selon un angle de 90 degrés et lorsque le détecteur mesure la polarisation dans la base (45, 135). Dans un tel cas, le détecteur mesure les polarisations 45 et 135 avec probabilité 50 %. Cela signifie qu'au lieu d'interpréter correctement la valeur codée (0 dans ce cas), il "voit" tantôt la valeur 0, tantôt la valeur 1, avec la même probabilité dans chaque cas. Il n'est dès lors pas plus avancé que s'il avait simplement joué à pile ou face. De plus, une fois le signal mesuré, le photon est détruit et le détecteur n'a plus accès à l'information initiale. Pour débarrasser la clé de cette information factice, l'émetteur et le récepteur peuvent, après transmission de la clé, communiquer publiquement quels étaient leurs choix de base respectifs pour chacun des signaux détectés et éliminer purement et simplement

les composantes de la série pour lesquelles les bases sont différentes. Il est à noter que cette communication n'informe en rien l'espion sur la nature de la clé, celle-ci étant déterminée par les choix de la direction de polarisation au sein d'une même base et non par le choix de la base.

Supposons maintenant qu'un espion intercepte n photons, et que, tout comme le récepteur, il choisisse au hasard la base de détection (la direction de son filtre polariseur) parmi les bases (0, 90) et (45, 135). Huit cas différents (2 exposant 3) couvrent alors les choix de base possibles faits par l'émetteur, le récepteur, et l'espion. De ces huit cas, quatre seront éliminés lorsque l'émetteur et le récepteur sacrifieront l'information mesurée dans des bases différentes (figure 4). Parmi les quatre cas restant, l'espion détecte et retransmet correctement le signal dans deux cas (base de l'émetteur, du récepteur et de l'espion: (0, 90) ou (45, 135)). Dans les deux cas restant (base de l'émetteur et du récepteur: (0, 90) ou (45, 135), base de l'espion (45, 135) ou (0, 90) respectivement), le signal est détruit par l'espion et le récepteur reçoit l'équivalent d'un signal aléatoire (valeur 1 ou 0 avec la même probabilité).

Après la transmission de la clé, la situation est la suivante: l'espion connait en moyenne $n/2$ composantes de la clé, tandis que la clé envoyée par l'émetteur et celle que possède le récepteur diffèrent en moyenne par $n/4$ composantes. En plus de ces erreurs, d'autres erreurs, liées aux détections de photons thermiques, à la dépolarisation du signal en cours de route ou à tout autre facteur incontrôlable viennent s'ajouter à l'erreur due à la présence de l'espion. Quoi qu' il en soit, l'erreur étant cumulative, l'information maximale dont dispose l'espion est en moyenne inférieure au double du nombre d'erreurs[2].

A ce niveau, la situation est la suivante: le récepteur possède une clé entachée d'un nombre d'erreurs t ; l'espion connait au plus $2t$ composantes de la clé. Deux techniques permettent alors d'éliminer les erreurs de la clé et d'obtenir une nouvelle clé à partir de la précédente avec une garantie de confidentialité proche de l'unité. Ces techniques, appelées respectivement protocole de réconciliation (*reconciliation protocol*) et protocole d'amplification de la confidentialité (*privacy amplification protocol*) par leurs auteurs sont essentiellement classiques. Elles sont réalisées sur un

[2]Il existe en fait des attaques plus dangereuses que celle considérée ici, pour lesquelles la relation entre le taux d'erreur et l'information de l'espion n'est pas linéaire comme dans le cas présent. Ces attaques sont réalisées à l'aide d'une cloneuse quantique optimale. Leur étude sort du cadre du présent article, mais même pour ces cloneuses il existe une relation de complémentarité (figure 6) entre l'information acquise par l'espion et la fidélité de la transmission entre les parties autorisées, Alice et Bob. C'est cette propriété ("un espion ne peut espionner sans perturber") qui fait la spécificité du codage quantique; elle est irréalisable avec des systèmes classiques.

canal public et se basent sur la théorie classique des probabilités. Nous nous contenterons d'en esquisser les principes généraux et renvoyons le lecteur intéressé aux références en fin de chapitre.

3.2 Protocole de réconciliation.

Lorsque l'émetteur et le récepteur ont achevé la transmission de la clé et sacrifié les signaux émis et détectés selon des directions de polarisation différentes, le récepteur possède une version de la clé qui, à cause des erreurs de transmission, diffère de la clé originale envoyée par l'émetteur.

Il est souvent impératif de purger la clé de ses erreurs, par exemple si on veut l'utiliser pour transmettre un numéro de compte bancaire confidentiel. Malheureusement, il est impossible de comparer les deux versions de la clé sur un canal public sans que l'espion en prenne connaissance auquel cas toute l'opération précédente s'avère inutile. Ce problème est surmonté (voir [5], [6]) si, au lieu de comparer les composantes de la clé sur un canal public, émetteur et récepteur comparent les parités de sous-séries extraites de la clé et choisies au hasard. Si un nombre impair d'erreurs est présent dans la sous-série, les parités diffèrent. En reproduisant ce test sur un grand nombre de sous-séries, il est possible de localiser et d'éliminer les erreurs, jusqu'au moment où la probabilité pour qu'une erreur subsiste est arbitrairement faible. Malgré tout, cet échange de données fait en public informe l'espion éventuel sur la nature de la série. Pour l'empêcher d'en profiter, l'émetteur et le récepteur conviennent, à chaque fois qu'ils échangent de l'information sur la parité d'une sous-série, d'une composante prise au hasard dans la sous-série et la sacrifient. Le gain informationnel que l'espion pourrait tirer de sa connaissance de la parité de la série est dès lors réduit à néant.

Comme on le voit, cette technique implique le sacrifice d'une partie importante de la clé. On peut montrer que si le taux d'erreur est trop élevé (plus que 10 % selon [7]), le sacrifice à consentir devient aussi élevé que le contenu de la clé et le protocole de réconciliation est inapplicable. Cette contrainte fondamentale impose, comme nous le montrerons plus tard, de sévères restrictions sur la réalisabilité de la technique.

3.3 Le protocole d'amplification de la confidentialité.

Pendant le protocole de réconciliation, les erreurs ont été reconnues et éliminées. Sur base du nombre d'erreurs, on peut évaluer la quantité maximale d'information dont dispose l'espion. Le protocole d'amplification de la confidentialité consiste à remplacer les composantes de la clé par des composantes obtenues à partir des premières par le biais d'algorithmes choisis au hasard dans un espace fonctionnel bien choisi (voir [5], [6]). Ces algorithmes faisant intervenir la totalité des composantes de la série, l'information dont disposait l'espion se trouve diluée lors de ce processus. À nouveau, une partie de la clé est supprimée à chaque étape. Pratiquement, lorsque l'information sacrifiée dépasse de m unités l'information de l'espion, celui-ci connait au mieux une composante du message remodelé avec une probabilité $\frac{2^{-m}}{ln\,2}$. Ceci permet de réaliser avec succès l'objectif final de la cryptographie quantique: obtenir une garantie de confidentialité quasi absolue sur la transmission de la clé (figure 5).

4 Limitations de la technique.

4.1 Limitations d'ordre technique.

Comme nous l'avons mentionné, le protocole de réconciliation (et donc l'ensemble de la technique dont c'est un maillon essentiel) sont inapplicables dès lors que le taux d'erreur dépasse 10 %. Toute source génératrice d'erreur limite dès lors la technique. Nous allons examiner les principales sources d'erreur et leur effet sur la réalisabilité de la technique.

Au niveau de l'émetteur:

Il n'est pas facile de contrôler avec une grande précision la polarisation des photons, des erreurs pouvant apparaître par exemple au niveau de la direction de polarisation.

Il est surtout difficile de changer rapidement l'axe de polarisation (les fréquences des sources employées sont de l'ordre du mégahertz, voir [8]). Il est possible néanmoins de limiter l'erreur à la source à un facteur de l'ordre de 0,5 % (voir [9]) à condition de réaliser l'expérience avec soin.

Au niveau de la transmission:

Lors de l'expérience de Bennet et al., les photons étaient envoyés dans le vide sur une distance de 30 cm. Actuellement, en vue d'une application pratique de la technique, le signal est envoyé par fibre optique. Ce mode de transmission présente deux désavantages. Premièrement, l'absorption dans la fibre, qui dépend exponentiellement de la distance, influence indirectement le taux d'erreur par le biais du *dark count rate* que nous examinerons tout de suite. Secondement, la dépolarisation du signal qui, pour être évitée, nécessite des fibres de très bonne qualité peu sujettes aux torsions (voir [9]). Cela implique par exemple que les lignes doivent être construites en dur et proscrit l'usage de lignes aériennes sujettes au vent.

Au niveau du récepteur :

Dans un détecteur de photons, on ne peut éviter la détection aléatoire de photons d'origine thermique ou autre (*dark count*). Le taux d'erreur du à ces photons est proportionnel au temps d'ouverture du détecteur. À intensité de signal détecté égale, ce temps est inversement proportionnel à l'intensité du signal transmis et donc directement proportionnel à l'absorption dans la fibre. Cela signifie que l'erreur due à la détection fortuite de photons au niveau du récepteur augmente exponentiellement avec la distance. A cela viennent s'ajouter la perte en intensité occasionnée par l'atténuation du signal à la source (voir paragraphe suivant), et la perte en intensité due à la piètre qualité des détecteurs disponibles à l'heure actuelle (efficacité de l'ordre de 20 % pour les longueurs d'onde employées dans les fibres optiques) . La combinaison de ces effets est telle qu'actuellement la technique est (pour l'instant-car ces limites reculent d'année en année) inapplicable au-delà d'une distance de cent - cent cinquante kilomètres (voir [10]).

4.2 Limitations de principe.

Possibilité d'espionnage par "*beamsplitting*".

La source de photons employée consiste en une source laser[3]. Cela implique que l'on n'a pas exactement un photon par pulse mais que l'on a une distribution plutôt étalée du nombre de photons. Pour un laser cohérent, la distribution est Poissonienne: la probabilité d'observer N photons par pulse est égale à $exp(-\mu) \cdot \mu^N/N!$. Au plus μ, le nombre moyen de photons par pulse, est élevé, au plus le signal

[3]Des sources basées sur le phénomène de *down conversion* ont été employées en cryptographie quantique (voir [8]), mais leur faible intensité ne permet pas de les retenir comme candidats acceptables pour des applications concrètes.

se rapproche d'un signal classique, ce qui augmente la vulnérabilité de la technique. Intuitivement, quand μ est élevé, un espion pourrait intercepter un photon et laisser passer le reste du pulse sans que cela modifie de façon notable la qualité du signal, de telle sorte que son activité reste inaperçue.

La technique d'espionnage dite par *beamsplitting* illustre cette idée (voir [5]) : un espion pourrait par exemple séparer les pulses grâce à un miroir semi-transparent, stocker un photon et analyser sa polarisation dans la base compatible, lorsque celle-ci est annoncée publiquement par l'émetteur après l'émission de la clé. Il pourrait même doper le signal réémis afin de rétablir les populations initiales pour compenser la perte d'intensité due à son activité. Le rapport entre le nombre de pulses contenant un photon et le nombre de pulses contenant plus d'un photon est proportionnel à μ. Afin de minimiser la quantité d'information que l'espion pourrait acquérir par la technique de *beamsplitting*, il faut employer des pulses fortement atténués. Pratiquement, on travaille avec des distributions telles que μ soit de l'ordre de 10 %. Cela veut dire que, grosso modo, neuf signaux sur dix sont vides, un signal sur dix contient un photon, un sur cent en contient deux, un sur mille en contient 3, etc.

Possibilité d'espionnage par "agressive *beamsplitting*".

Cette technique constitue une variante de la technique précédente (voir [5]). Vient s'y ajouter un élément "agressif": non content d'intercepter un photon lorsque le pulse en contient plusieurs, l'espion détruit les pulses ne contenant qu'un photon. Pour compenser la perte d'intensité liée à son activité, l'espion remplace la ligne de transmission utilisée par l'émetteur par une ligne moins opaque (c'est-à-dire une ligne de moindre taux d'absorption). Techniquement, on peut minimiser l'incidence de cette technique d'espionnage en minimisant le quotient μ/T, où μ est le nombre moyen de photons par pulse et T le facteur d'absorption de la fibre sur toute sa longueur.

Il faut noter que ce type d'espionnage, s'il est possible en principe, est irréalisable concrètement: il n'est actuellement possible de stocker un photon que pendant un temps de l'ordre de la milliseconde, après quoi il est absorbé avec une probabilité proche de l'unité.

5 Situation actuelle et perspectives d'avenir.

Comme on le voit, de nombreuses contraintes techniques limitent la faisabilité de la technique. En particulier, la technique de Bennet et al. présentée ici ou des techniques analogues, bien qu'effectivement réalisées sur des distances de plusieurs dizaines de km, sont difficiles à réaliser sur de longues distances. Ceci est du au fait que, dans les fibres actuelles, qui possèdent en général deux modes de polarisation orthogonaux, on ne peut éviter la dépolarisation du signal lorsqu'il est codé selon quatre directions différentes comme l'exige la technique de Bennet et al. [6].

Quoi que l'on fasse, le problème du *dark counts* mentionné précédemment reste insurmontable, et représente la limitation fondamentale sur la distance maximale de transmission de l'information avec les photons uniques. Celui-ci dépend de la longueur de la fibre de manière exponentielle et, même si on gagne un facteur 10 (100) sur l'intensité du signal utile grâce à des raffinements techniques, cela ne constitue qu'un gain en distance de l'ordre de 30 (60) km. Il faut mentionner que le problème de *dark counts* n'existe pas pour les protocoles de la distribution de clé dite "à variables continues" [12], [13] pour lesquels on utilise la mesure *homodine*, une mesure standard en optique quantique qui présente l'avantage de fonctionner en régime continu. Ces protocoles plus récents sont, eux aussi basés sur le principe d'incertitude de Heisenberg, mais les variables qui portent la clé sont continues et non pas discrètes, comme le nome indique. Il serait trop long de les présenter dans le présent exposé, d'autant plus que le principe général ("un espion ne peut espionner sans perturber") et commun aux techniques à variables continues et discrètes [4].

La distance d'application maximale des techniques quantiques de cryptographie peut être évaluée à 100 km (voir [10]). Si on veut développer un réseau de transmissions cryptographiques à l'échelle d'un pays, il sera nécessaire d'implanter régulièrement des postes de retransmission du signal qui présentent des garanties de confidentialité. De tels postes devraient être maintenus sous haute surveillance, ce qui limite bien sur l'applicabilité de la technique.

À courte distance, par contre, par exemple entre différents états-majors, ministères etc. d'une grande capitale telles que Londres ou Paris (à fortiori à Bruxelles), cette technique est réalisable et présente des garanties de sécurité absolue inexistantes pour des techniques classiques.

[4] On peut trouver une introduction très générale et plus technique à la cryptographie quantique dans les références [14], [15].

6 Remerciements.

La majeure partie de ce travail a été effectue par Thomas Durt dans le cadre d'un projet de recherche de l'Instituut van Interuniversitaire Kern Wetenschappen (IIKW), avec le soutien des Fédérale Diensten voor Wet., Techn. en Cult. Aang. dans le contexte du IUAP-III n°9. Il a été diffusé sur le site de Simon Diner (C.N.R.S.) www.omphalos.com maintenant disparu.

References

[1] G. S. Vernam, J. Amer. Inst. Electr. Engrs, **45**, 109-115 (1926).

[2] C. E. Shannon, Bell Syst. Tech. J., **28**, 657 (1949).

[3] W. Heisenberg, Zeitschrift fur Physik, **43**, 172-198 (1927).

[4] H. P. Robertson, Phys. Rev., **34**, 163-164 (1929).

[5] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptol., **5**, 3-28 (1992).

[6] C. H. Bennett, G. Brassard, and J-M. Robert, SIAM J. Comput., **17**, 2, 210-229 (1988).

[7] S. J. D. Phoenix, and P. D. Townsend, Contemporary Physics, **36**, 165-195 (1995).

[8] J. G. Rarity, P. C. M. Owens, and P. R. Tapster, J. Mod. Optics, **41**, 2435-2444 (1994).

[9] J. Breguet, A. Muller, and N. Gisin, J. Mod. Optics, **41**, 2405-2412 (1994).

[10] R. J. Hughes, D. M. Alde, P. Dyer, G. G. Luther, G. L. Morgan, and M. Schauer, Contemporary Physics, **36**, 149-163 (1995).

[11] C. H. Bennett, Phys. Rev. Lett., **68**, 3121-3124 (1992).

[12] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005)

[13] F. Grosshans, G. Van Assche, J. Wenger *et al.* Nature, **421**, 238-241 (2003).

[14] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 - 195 (2002)

[15] G. Van Assche, *Quantum Cryptography and Secret-Key Distillation* (Cambridge University Press, Cambridge, 2006) 262 p.

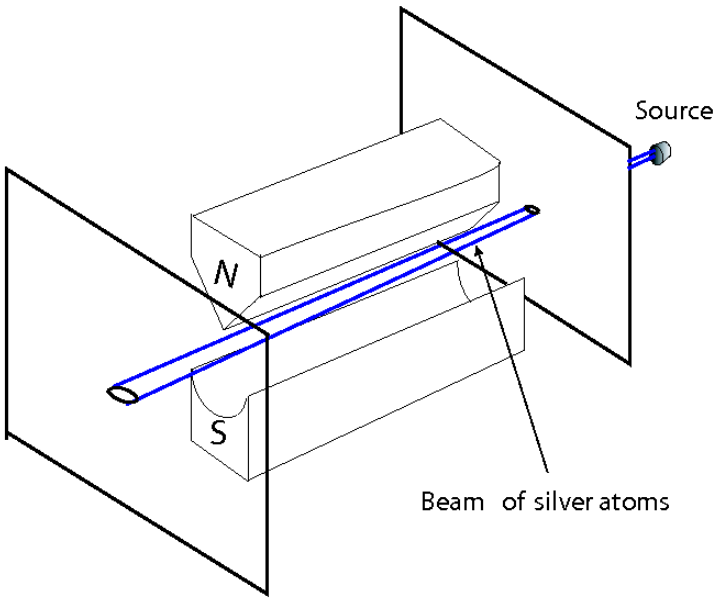

Figure 1: Etats de spin 1/2 lors d' une mesure de type Stern-Gerlach

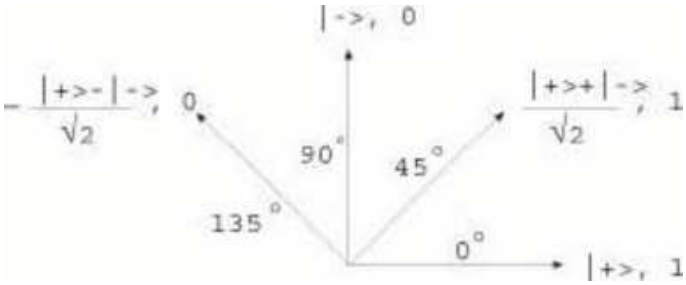

Figure 2: 4 états qubit de polarisation

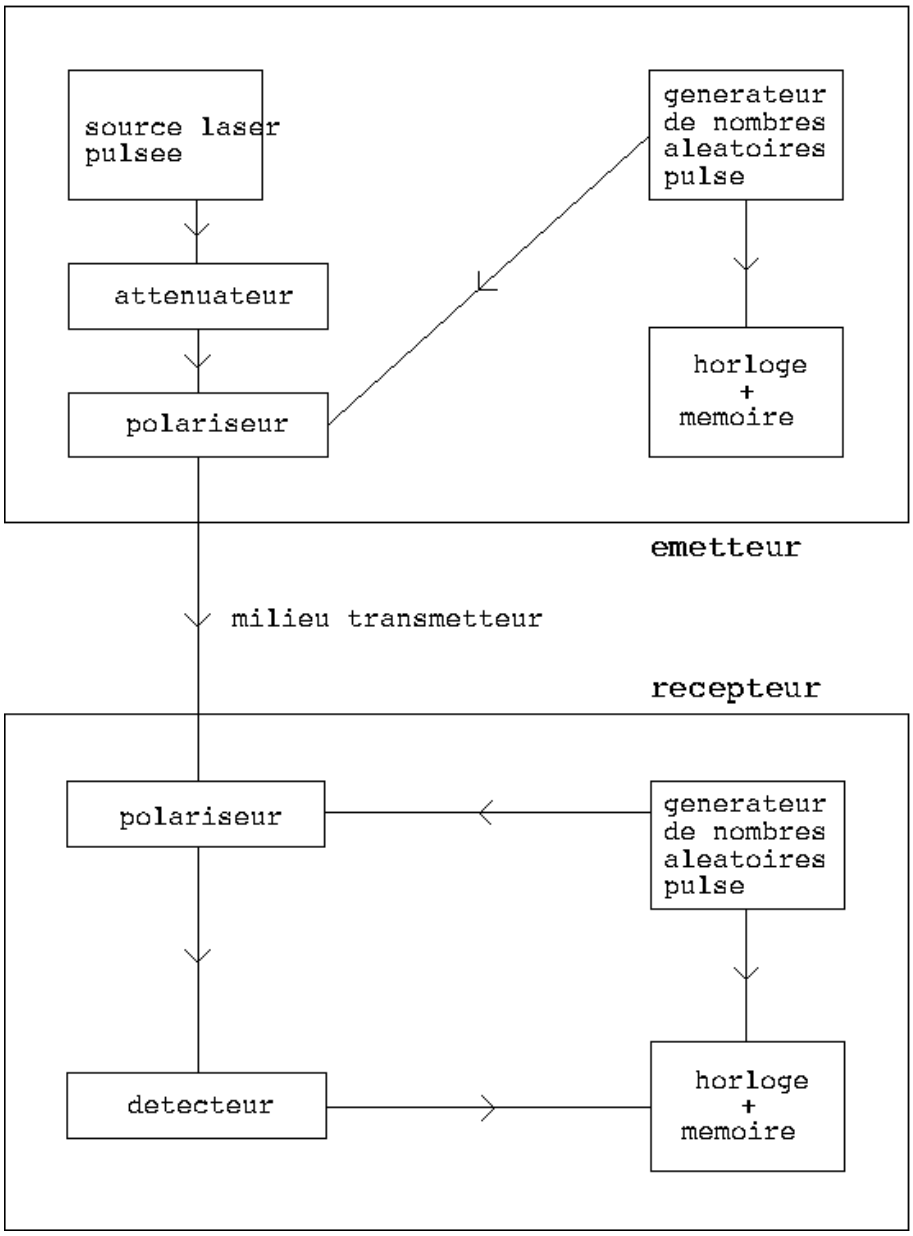

Figure 3: Protocole de Bennett et Brassard 1984 (BB84)

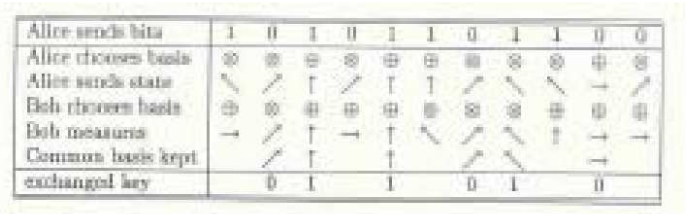

Figure 4: Echange quantique lors de BB84, et clé échangée dans des bases identiques par Alice et Bob

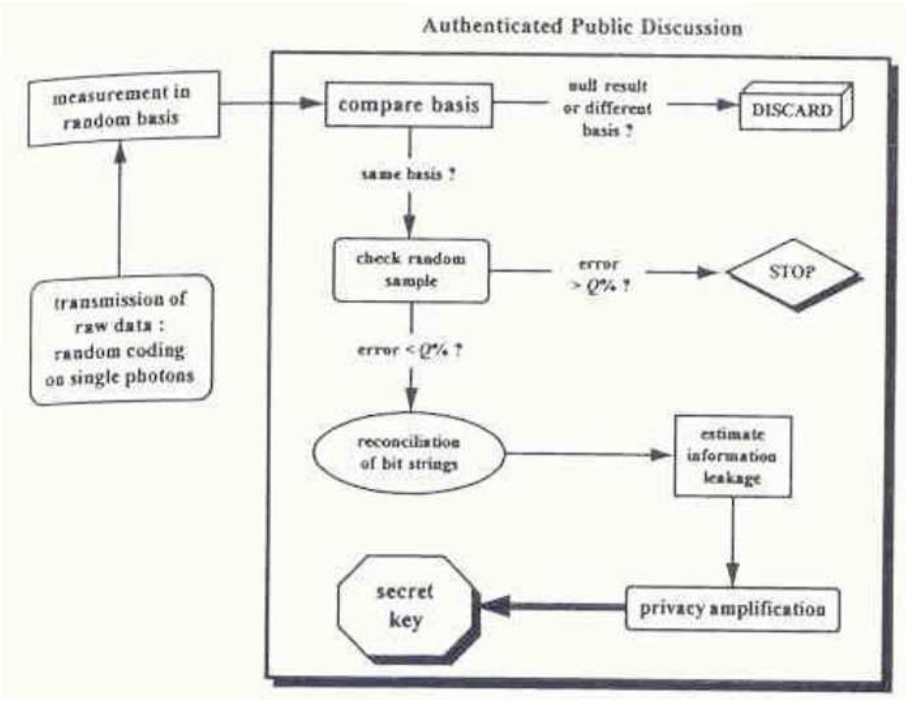

Figure 5: Parties quantique et classique du protocole BB84

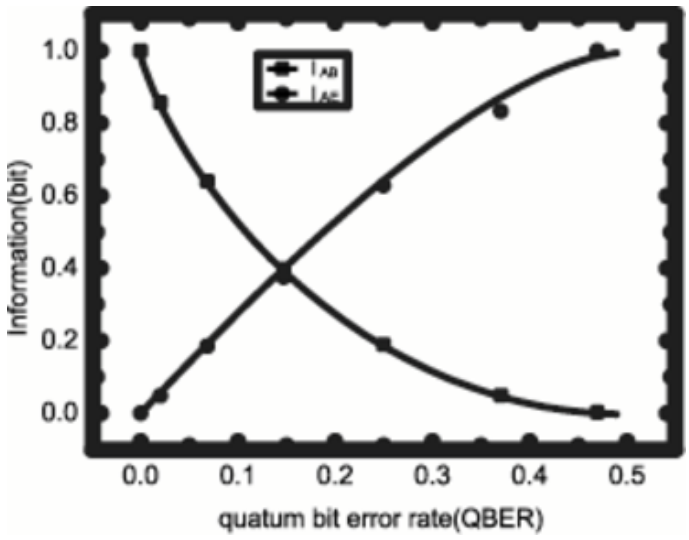

Figure 6: Relation de complémentarite entre l'information de l'espion (courbe montante) et celle des parties autorisées (courbe descendante) en fonction de la perturbation de la transmission due à la présence de l'espion.