Cryptographie quantique - solution au problème de distribution de clefs secrètes

Mélanie Langlois
Université d'Ottawa

Décembre 1999

Résumé

Après un bref historique sur la cryptographie quantique, il est montré comment les photons peuvent être utilisés pour transmettre de l'information. Le protocole de distribution de clefs secrètes, BB84, dont la sécurité inconditionnelle est due au principe d'incertitude de Heisenberg, est ensuite exposé. Puis deux problèmes d'ordre pratique sont pris en considération pour montrer qu'il est possible, après quelques ajustements, de mettre en pratique ce protocole. Finalement, les résultats des premières expériences réalisées sont donnés.

1 Introduction

Deux personnes voulant communiquer par le biais de messages chiffrés en utilisant un média, tel qu'un journal, recherchent l'intimité alors que deux personnes désirant prendre conjointement des décisions basées sur de l'information confidentielle et voulant communiquer de manière à se protéger non seulement d'espions potentiels, mais aussi l'une de l'autre, recherchent la discrétion. L'intimité et la discrétion sont deux objectifs de la cryptographie.

Il y a deux mille ans, la sécurité d'un message chiffré dépendait entièrement des processus de chiffrement et de déchiffrement que l'on se devait de garder dans le plus grand des secrets. De nos jours, le sécurité d'un message chiffré réside plus particulièrement dans la clef car les processus de chiffrement et de déchiffrement connaissent en général une grande diffusion médiatique. Ainsi, deux personnes qui auront éventuellement besoin de communiquer dans l'intimité ou la discrétion doivent prévoir une clef et la garder secrète. Par ailleurs, Shannon a démontré que la sécurité d'un message chiffré ne peut être absolue que si chaque message échangé entre deux personnes est chiffré avec une clef aussi longue que celui-ci et que cette clef doit être différente pour chaque message devant être chiffré. En

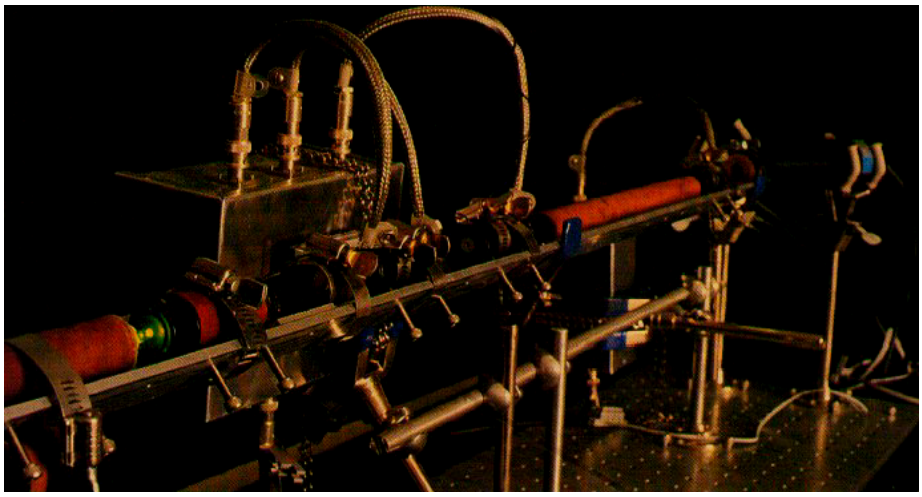
fait, le code de Vernam est le seul qui soit mathématiquement reconnu comme inviolable, mais le fait de devoir utiliser une clef différente pour chaque chiffrement est à l'origine d'un problème d'ordre pratique considérable connu sous le nom de *problème de distribution des clefs secrètes*. Bien sûr il est possible pour deux personnes d'établir pour chaque nouveau message à chiffrer une nouvelle clef, mais le problème auquel elles doivent faire face est la transmission de cette clef de l'une à l'autre, car cette clef ne doit demeurer connue que d'elles et ne peut donc pas être envoyée par un canal publique vulnérable à toutes sortes d'interceptions passives. Les mathématiques offrent toutefois des solutions, bien qu'imparfaites, à ce problème, par exemple sous la forme du système de clefs publiques introduit en 1976. Par ailleurs, la physique s'est aussi penchée sur ce problème car, après tout, l'information échangée lors de la distribution d'une clef est souvent transmise par un moyen physique: la lumière, le son, les ondes radio ou encore les électrons. L'espionnage peut alors être vu comme étant l'acquisition de mesures faites sur le moyen physique utilisé pour la transmission. En théorie, l'acquisition de telles mesures perturbe l'état de ce moyen physique permettant ainsi aux utilisateurs d'effectuer leurs propres mesures afin de déterminer s'ils sont espionnés ou non. En pratique toutefois, tous ces canaux classiques peuvent être espionnés de façon passive sans que les utilisateurs légitimes ne soient en mesure de le déterminer. L'avantage appartient ici a celui qui possède la technologie la plus avancée. Ce que la physique, ou plus particulièrement, la mécanique quantique propose pour tenter de résoudre le problème est de concevoir des canaux de communication, les canaux quantiques, ayant la propriété d'être inviolable, c'est-à-dire que s'il y a espionnage sur un tel canal, alors il ne peut avoir lieu sans être détecté.

C'est cette perspective offerte par la cryptographie quantique que j'ai voulu étudier. La cryptographie quantique suggère cependant plusieurs autres applications toutes aussi intéressantes et j'ai donc décidé de les présenter dans le bref historique qui suit cet introduction. J'expliquerai ensuite comment un protocole de distribution de clefs secrètes peut être basé sur les propriétés des photons polarisés et je montrerai comment un tel protocole, BB84, peut être mis en pratique.

2 Historique

Au début des années 1970, Stephen Wiesner, alors à l'université de Columbia, écrit un rapport présentant des idées tout à fait nouvelles. Wiesner propose d'utiliser la mécanique quantique pour coder des billets de banques dont l'infalsifiabilité serait garantie par le principe d'incertitude d'Heisenberg. De plus, il propose aussi d'utiliser la mécanique quantique pour construire un canal multiplexeur permettant d'entremêler deux messages d'une façon qu'on ne puisse en lire qu'un seul et qu'en le lisant, on rende l'autre illisible. Bien que les idées de Wiesner ne furent finalement publiées qu'en 1983 dans la revue Sigact News, elles inspirèrent Charles H. Bennett du laboratoire de recherche IBM T.J. Watson et Gilles Brassard de l'université de Montréal, qui, au courant de ces idées bien avant 1983 à la suite de

FIG. 1 – *Prototype de Bennett et Brassard construit en 1989 au laboratoire de recherche de IBM T.J.Watson.*



discussions avec Wiesner, proposent en 1984 un protocole de distribution de clefs secrètes. Bennett et Brassard savaient que leur système tel que présenté en 1984 était totalement impraticable et telle était aussi l'opinion des gens du domaine. Toutefois, les raffinements apportés durant les années subséquentes ont permis la construction du premier prototype complètement opérationnel (Figure 1). Les expériences conduites à partir de ce prototype fait au laboratoire de recherche IBM T.J. Watson ont permis de montrer qu'il était possible grâce au canal quantique de transmettre des clefs secrètes de plusieurs centaines de bits à une vitesse de 10 bit/s [8], entre deux points distants de 32 cm [2], et ce même si ce canal est espionné tout au long de la transmission!

Il s'agissait vraiment d'un très grand événement et les partisans de la cryptographie quantique avaient raison de se réjouir car cette réussite amena un engouement de plus en plus grand pour la cryptographie quantique. Maintenant, les applications suggérées depuis les idées de Wiesner deviennent le centre d'intérêt de beaucoup de chercheurs. Pour illustrer cet essor, voici deux lignes du temps: la première montre les idées introduites en cryptographie quantique depuis le rapport de Wiesner en 1970 jusqu'au moment où, en 1989, Bennett et Brassard réalisent leur prototype (Figure 2), alors que la deuxième montre les apports les plus importants apportés à la cryptographie de 1990 à 1997 (Figure 3).

En comparant ces deux lignes du temps, on remarque que depuis que Bennett et Brassard ont permis à la cryptographie quantique de passer de la fiction à la réalité, les chercheurs ont déployé des efforts non seulement pour l'avancement des protocoles de distribution des clefs secrètes, mais aussi pour donner naissance

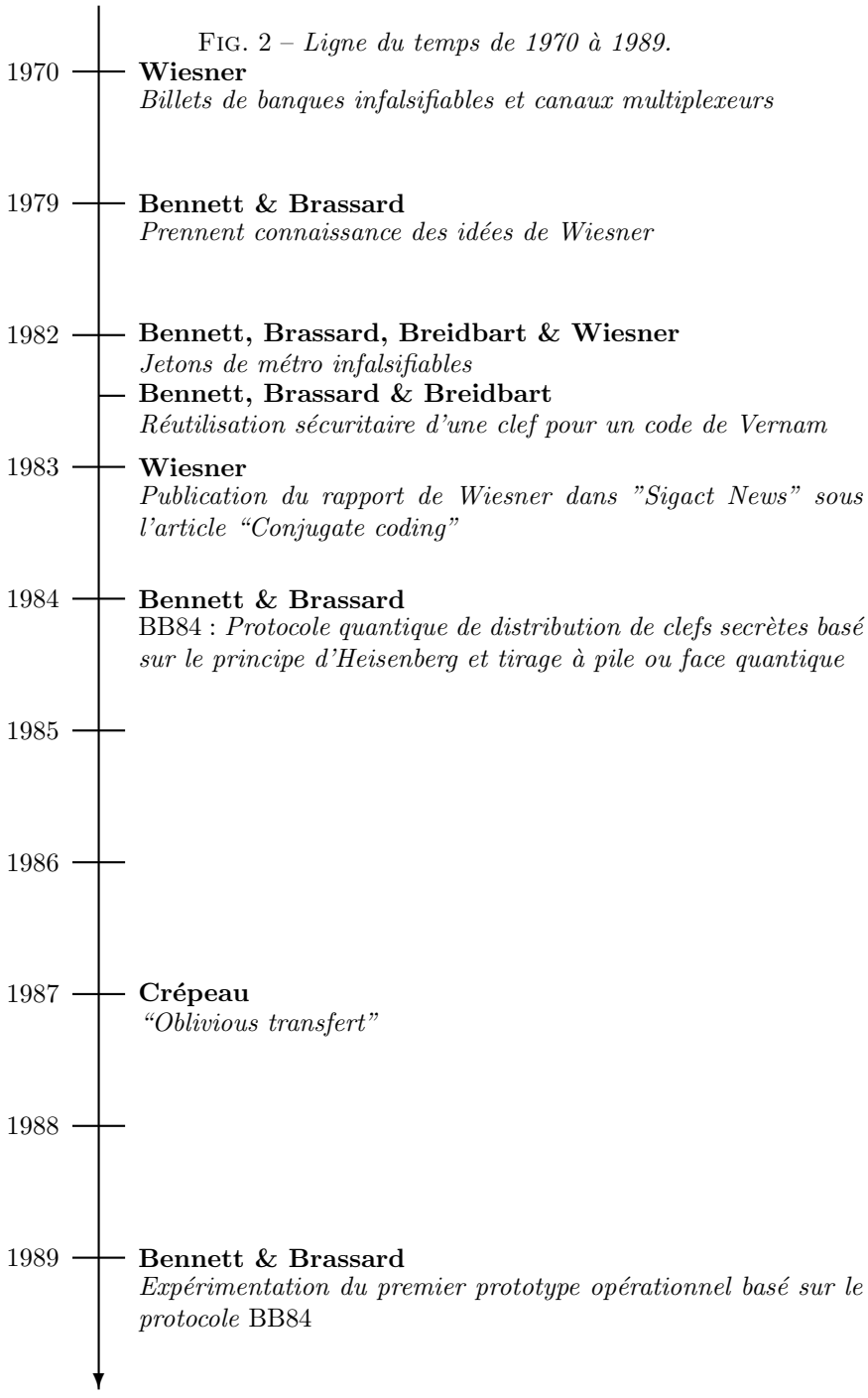
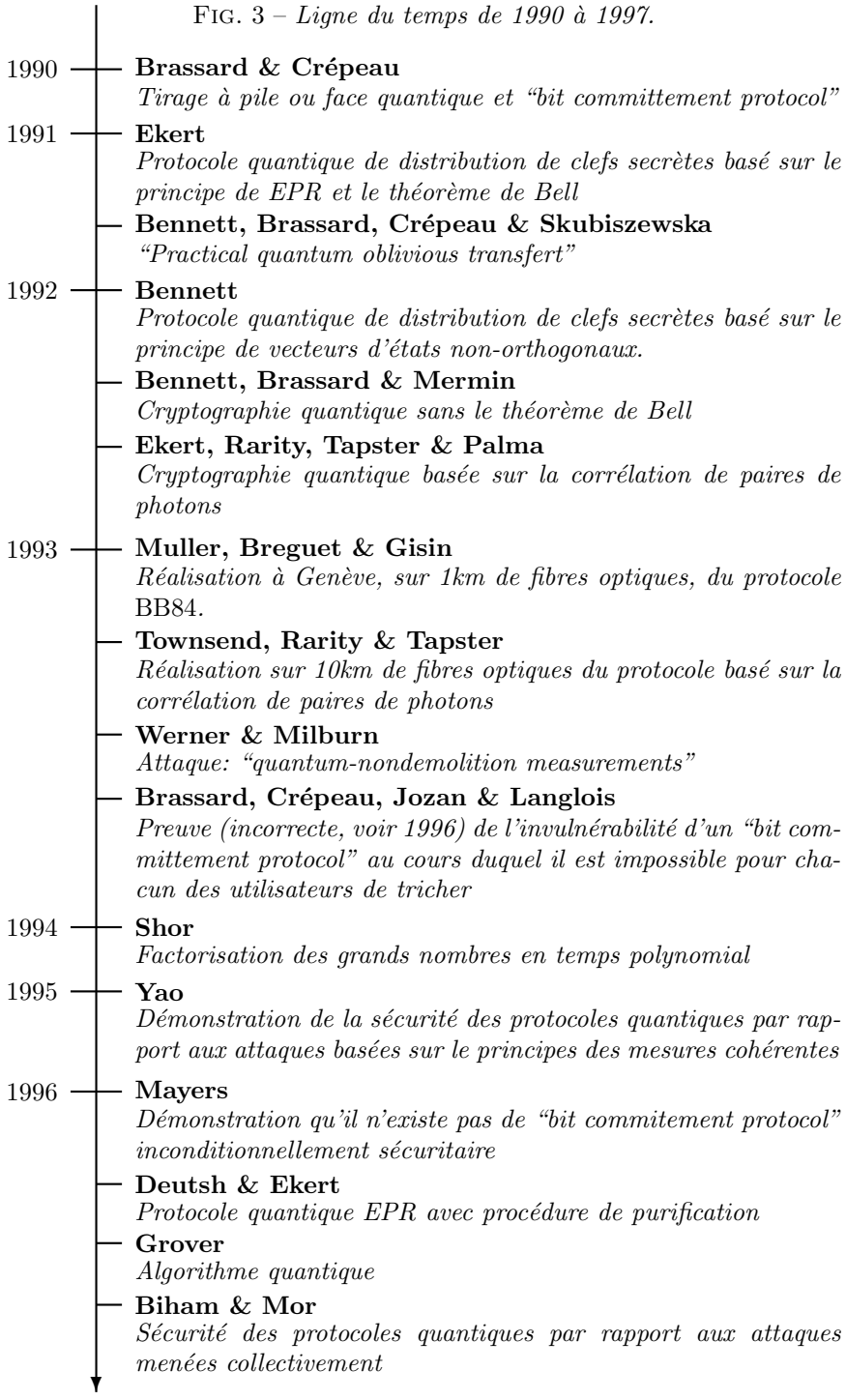


FIG. 2 – *Ligne du temps de 1970 à 1989.*

FIG. 3 – *Ligne du temps de 1990 à 1997.*



à plusieurs autres applications. Parmi celles-ci, notons l'algorithme quantique de recherche proposé en 1996 par K. Grover. Bien que cette application demeure encore impraticable, elle n'en est pas moins stupéfiante. En fait, l'algorithme de Grover [6] appliqué à la recherche exhaustive d'une clef utilisée pour chiffrer un message avec un algorithme symétrique permettrait, théoriquement, d'augmenter significativement la vitesse de recherche de la clef pour une paire (message, chiffre) donnée. Par exemple, pour DES et une paire (message, chiffre), on obtiendrait la solution unique après en moyenne 185 millions de chiffrements au lieu des $2^{55} \approx 3{,}6 \times 10^{16}$ chiffrements requis pour mener une attaque exhaustive "classique"!

Que dire de plus? Le cryptographie quantique semble promettre beaucoup. Voyons donc dans les sections qui suivent ce qu'il y a de prometteur dans les protocoles quantiques de distribution de clefs secrètes.

3 Protocoles quantiques de distribution de clefs secrètes

La physique classique dont l'objet est l'étude des corps et des phénomènes macroscopiques, établit qu'il est possible de mesurer n'importe quelle propriété d'un certain objet sans qu'elle en soit affectée. La physique quantique propose quant à elle une théorie gouvernant tous les objets, autant au niveau macroscopique que microscopique, bien que ses conséquences soient beaucoup plus évidentes pour les systèmes microscopiques, comme dans le cas des particules subatomiques. En fait, en physique quantique, l'action de mesurer une certaine propriété d'un système microscopique n'est pas un processus passif et extérieur au système, mais fait partie intégrante de la mécanique quantique de ce système. Ainsi, en construisant un canal quantique basé sur un phénomène quantique particulier, on pourrait espérer supprimer la possibilité d'un espionnage actif ou passif, ou, plus précisément, qu'il soit impossible de mener une attaque sans être détecté avec une très grande probabilité.

J'exposerai dans les sections suivantes comment le principe d'incertitude de Heisenberg appliqué aux photons, la plus petite partie ou quantum de la lumière, permet d'obtenir la base d'un protocole de distribution des clefs secrètes (BB84) inconditionnellement sécuritaire, et comment l'ajout de quelques étapes au protocole permet de le rendre praticable.

3.1 Propriétés des photons polarisés

Un photon peut être considéré comme étant un minuscule champs électrique oscillatoire. La direction de l'oscillation définit alors la polarisation du photon. Lorsque l'on fait passer la lumière à travers un filtre polarisant, les photons seront

absorbés ou transmis selon de leur polarisation:

- Si le photon est polarisé parallèlement à l'angle d'orientation du filtre, alors ce photon sera transmis sans changement de polarisation.
- Si le photon est polarisé perpendiculairement à l'angle d'orientation du filtre, alors ce photon sera absorbé.
- Si le photon est polarisé selon une direction intermédiaire, alors ce photon sera transmis avec probabilité $\cos^2(\alpha)$, où α est l'angle de polarisation du photon mesuré par rapport à l'angle d'orientation du filtre. C'est-à-dire que si le photon est polarisé selon un angle de γ et que le filtre est orienté selon un angle de β, alors $\alpha = \gamma - \beta$. Si le photon est transmis, alors sa nouvelle polarisation correspondra à l'angle d'orientation du filtre.

La polarisation de la lumière transmise par le filtre polarisant est donc égale à l'angle d'orientation du filtre. Ainsi, les photons initialement polarisés selon un angle de γ ont maintenant tous une polarisation correspondante à l'angle du filtre, soit un angle de β, ce qui implique que leur polarisation initiale est complètement perdue. Il est ainsi impossible d'essayer d'obtenir de l'information sur la polarisation initiale d'un photon en le faisant passer par un deuxième filtre d'orientation $\tilde{\beta} \neq \beta$. De plus, il est impossible de cloner un photon afin d'effectuer plusieurs mesures de polarisation avec des filtres d'orientations différentes puisque ceci va à l'encontre des fondements de la mécanique quantique.

Les points suivants, qui se rapportent au $3^{\text{ième}}$ cas donné plus haut, sont à remarquer:

1. Plus la polarisation du photon incident au filtre est près de l'angle d'orientation du filtre, i.e plus $\gamma - \beta$ est près de 0, plus la probabilité que le photon soit transmis est grande.
2. Si $\alpha = 0°$, alors la probabilité que le photon soit transmis est: $\cos^2(0°) = 1$.
3. Si $\alpha = 90°$, alors la probabilité que le photon soit transmis est: $\cos^2(90°) = 0$, où de façon complémentaire, la probabilité que le photon soit absorbé est: $1 - \cos^2(\alpha) = \sin^2(\alpha)$, et $\sin^2(90°) = 1$.
4. Le comportement est complètement aléatoire , i.e. le photon est transmis (ou absorbé) avec probabilité $\frac{1}{2}$, lorsque $\cos^2(\alpha) = \frac{1}{2}$, soit lorsque $\alpha = 45°$ ou $\alpha = 135°$.

Ces propriétés permettent d'utiliser un photon polarisé pour réaliser le concept de bit quantique ou **qubit**. Un qubit pour un système quantique quelconque est défini par $q = \alpha\langle 0| + \beta\langle 1|$, où α,$\beta \in \mathbb{C}$, $\|\alpha\|^2 + \|\beta\|^2 = 1$ et $\langle 0|$ et $\langle 1|$ représentent respectivement un bit de valeur 0 et un bit de valeur 1. Pour un système de photons polarisés, on peut par exemple associer le symbole $\langle 0|$ à une polarisation horizontale et $\langle 1|$ à une polarisation verticale. Ainsi, le qubit associé à un photon polarisé avec un angle de γ sera donné par $q = \cos(\gamma)\langle 0| + \sin(\gamma)\langle 1|$.

Par ailleurs, on peut représenter les qubits sous forme vectorielle en utilisant un vecteur de deux composantes, $q = (\alpha,\beta)$. Ces vecteurs sont tous de norme 1 et forment un espace de Hilbert de dimension 2. Ainsi, pour l'exemple précédent, $q = (\cos(\gamma), \sin(\gamma)) = \cos(\gamma)r_1 + \sin(\gamma)r_2$ où $r_1 = (1,0)$ et $r_2 = (0,1)$ sont les vecteurs de base de l'espace de Hilbert et représentent respectivement les polarisations horizontale et verticale. Lorsque l'on fait passer le photon à travers un filtre polarisant avec une orientation horizontale ou vertical on dit que l'on mesure la polarisation du photon. Effectuer cette mesure sur les vecteurs de l'espace de Hilbert correspond à la décomposition de l'espace de Hilbert en ses sous-espaces orthogonaux. Pour un système de photons polarisés, le nombre de sous-espaces orthogonaux est 2 et ces sous-espaces peuvent être décrit selon les vecteurs d'une des trois bases suivantes:

- Base rectilinéaire: $r_1 = (1,0), r_2 = (0,1)$
- Base diagonale: $d_1 = (\delta,\delta), d_2 = (\delta, -\delta)$ où $\delta = \frac{\sqrt{2}}{2}$
- Base circulaire: $c_1 = (\delta,\delta i), c_2 = (\delta i,\delta)$

Weisner donne une définition mathématique pour le concept de bases conjuguées: deux bases sont conjuguées si un système représenté dans une des bases se comportera de façon aléatoire lorsqu'il est soumis à une mesure faite selon l'autre base, et si l'information codée par le système est alors détruite irréversiblement. En fait nous avons déjà montré que tout photon polarisé avec un angle de 45° ou 135° sera transmis par un filtre polarisant d'orientation horizontale avec probabilité 1/2 et que ce photon s'il est transmis sera polarisé selon le même angle que l'angle d'orientation du filtre et n'aura donc plus aucune mémoire de sa polarisation initiale. Ainsi les bases rectilinéaire et diagonale, rectilinéaire et circulaire, et aussi diagonale et circulaire sont conjuguées. Par ailleurs, le principe d'incertitude d'Heisenberg repose sur le fait qu'en mécanique quantique il est impossible de mesurer une de deux propriétés d'une paire de propriétés complémentaires sans perturber l'autre. Il est donc possible d'appliquer le principe d'incertitude de Heisenberg aux photons polarisés puisque qu'on a montré l'existence de telles paires de propriétés complémentaires. Ainsi, pour établir un protocole quantique de distribution des clefs secrètes, il faut choisir une paire de bases conjuguées et utiliser les photons non pas pour garder de l'information mais bien pour transmettre de l'information.

3.2 Le protocole BB84

Le but du protocole est de permettre à deux utilisateurs, Alice et Bob, d'échanger une clef aléatoire et secrète pouvant être utilisée ensuite pour chiffrer un message selon le code de Vernam. Le protocole nécessite que les deux utilisateurs aient accès à un canal quantique et à un canal classique. Voici les étapes du protocole:

1. Alice génère et envoie à Bob par le canal quantique une suite de photons

polarisés dont la polarisation est choisie aléatoirement parmi les éléments des bases rectilinéaire et circulaire.

2. Bob reçoit les photons et pour chacun décide au hasard de mesurer la polarisation selon la base rectilinéaire ou circulaire.
3. Bob annonce à Alice par le canal classique la base choisie pour mesurer la polarisation de chacun des photons.
4. Alice et Bob comparent leurs résultats en communiquant par la canal classique et rejettent tous les cas où Bob n'a pas fait le bon choix pour la base.
5. Alice et Bob déterminent s'ils ont été espionnés, par exemple en comparant publiquement quelques données d'un sous-ensemble choisi aléatoirement parmi l'ensemble de leurs données restantes après l'étape 4.
6. Si le test montre de manière évidente qu'il y a eu espionnage, alors Alice et Bob rejettent les données échangées et recommencent à l'étape 1. Autrement Alice et Bob conservent les données restantes de l'étape 5 et interprètent alors la polarisation horizontale et circulaire-droite comme un bit de valeur 0 et la polarisation verticale et circulaire-gauche comme un bit de valeur 1. Ces bits forment la clef sécrète connue d'Alice et Bob seulement.

La figure 4 présente un exemple du protocole tel que simulé par un didactitiel [1] pour 64 photons envoyés par Alice et reçus par Bob avec une probabilité de 0,20 (les détecteurs ne sont pas efficace à 100%). De plus, pour cet exemple, Alice et Bob vont comparer à l'étape 5 la moitié de leurs données pour déterminer s'il y a eu espionnage.

FIG. 4 – *Exemple d'exécution du protocole* BB84

```
We will use these symbols
+   rectilinear
O   circular
for representing the types of photon measurements and these
<   left-circular
>   right-circular
|   vertical
-   horizontal
for representing the measurements themselves.

To review:

Alice  sends: ><><>|-<|-|--|><><><><||<<>>|-<|><|-||>--<|><||<><>-|>>>>->-><<<|
Bob measures: +++++O+O+O+O+O+O+++++++O+OOOO+O++++OO+O+++OO++OOO++O++O+++O+O+OO
Bob    reads: ||--| -<| |>-<|<-||-  |<->>< -> || <>   - > ||<> - <- >- | -<-<>
Bob    tells: +++++ +O+ +O+O+O++++  +O+OOO +O ++ OO   + O ++OO + O+ O+ + +O+OO
Alice  tells:       -<. | .  <      .< ..      |        . |..>      >     . <
Bob    tells:       -<. | .  <      .< ..      |        . |..>      >     . <
```

Les deux dernières lignes de cet exemple montre qu'Alice et Bob n'ont pas été espionnés puisque les données comparées concordent parfaitement. Les données

1. Voir notes à la suite des références pour les détails

restantes, soient celles illustrées par le symbole ".", sont celle qu'Alice et Bob utiliserons pour former leur clef secrète. Si Alice et Bob ont déterminé qu'un bit de valeur 0 serait donné par les polarisations horizontale et circulaire droite et qu'un bit de valeur 1 serait donné par les polarisations vertical et circulaire gauche, alors leur clef secrète dans cet exemple serait: **101000111**.

La section qui suit explique comment l'espionnage peut avoir lieu sur le canal quantique et comment Alice et Bob, grâce au principe d'incertitude de Heisenberg, peuvent le détecter.

3.3 Espionnage

Supposons qu'Ève cherche à découvrir la clef secrète qu'Alice et Bob vont essayer de s'échanger en utilisant le protocole BB84. Dans cette section, nous allons supposer qu'Ève ne peut mener qu'une attaque passive sur le canal classique et donc ne peut pas modifier les messages qu'Alice et Bob doivent s'échanger pour compléter le protocole.

Pour obtenir de l'information sur la clef secrète qu'Alice et Bob tentent d'échanger, Ève doit intercepter les photons envoyés par Alice, puis, pour chacun des photons interceptés, mesurer sa polarisation selon l'une des deux bases, rectilinéaire ou circulaire, et finalement envoyer un nouveau photon polarisé à Bob pour chaque photon intercepté. Cette attaque, qui porte le nom de "intercept/resend attack", est pratiquement impossible à réaliser avec succès, et ce peu importe la puissance de calcul dont dispose Ève. En fait, tout comme Bob, Ève doit décider pour chaque photon intercepté de mesurer sa polarisation selon une des deux bases, et tout comme Bob, Ève ignore la base choisie par Alice. Ainsi, à cause du principe d'incertitude d'Heisenberg et du fait que les deux bases forment une paire de propriétés complémentaires, tout espion menant cette attaque cours le risque d'introduire des incohérences dans les données d'Alice et Bob. En fait, Ève en interceptant et mesurant la polarisation des photons envoyés par Alice, fera en moyenne 1 fois sur 2 le mauvais choix pour la base. La polarisation se comporte alors de façon aléatoire et même si Ève envoie à Bob un photon de polarisation en accord avec le résultat de sa mesure, elle enverra 1 fois sur 2 un "mauvais" photon. Ainsi, Ève introduit une erreur dans les données de Bob 1 fois sur 4 car Bob mesurera ce "mauvais" photon dans la "bonne" base (celle choisie par Alice) 1 fois sur 2. Si Ève intercepte tous les photons envoyés par Alice, il y aura donc incohérence entre les données d'Alice et Bob dans 25% des données échangées. En comparant un sous-ensemble de leurs données, Alice et Bob sont donc en mesure de déterminer avec quasi-certitude s'il y a eu espionnage sur le canal quantique.

S'il y a eu espionnage, Alice et Bob doivent alors recommencer le protocole du début. Un espion pourrait certainement empêcher tout échange de clef entre Alice et Bob en menant cette attaque à chaque nouvelle tentative d'Alice et Bob, mais Ève ne peut en aucun cas tromper Alice et Bob en leur faisant croire que

l'échange a réussi de façon sécuritaire si en fait ce n'est pas le cas. Le protocole, considéré sous ce point de vue théorique est donc inconditionnellement sécuritaire. Certaines considérations d'ordre pratique compliquent cependant le déroulement du protocole, comme le montre la section qui suit.

3.4 Considérations d'ordre pratique

Lors de la création d'un prototype permettant la réalisation du protocole, il faut considérer les deux problèmes suivants:

1. Les photo-détecteurs ne sont pas efficaces à 100% et peuvent être perturbés par du bruit.
2. Les impulsions lumineuses contenant exactement un photon sont techniquement difficiles à produire.

Ces deux problèmes peuvent cependant être résolus. D'abord, puisque les photo-détecteurs ne sont pas efficace à 100% et qu'il est probable qu'ils ne détectent pas un photon, certains photons envoyés par Alice seront perdus. De plus, le bruit à l'intérieur du photo-détecteur peut causer une fausse détection, c'est-à-dire que le photo-détecteur détecte un photon alors qu'aucun photon n'a été envoyés par Alice. Il s'agit alors d'un "dark count". Ces imprécisions entraînent nécessairement des incohérences dans les données d'Alice et de Bob, et ce même s'il n'y a pas eu espionnage sur le canal quantique. Ainsi, si Alice et Bob rejettent leurs données dès qu'ils identifient une erreur, ils ne réussiront alors probablement jamais à échanger une clef secrète en suivant ce protocole. Pour remédier à ce problème, il faut ajouter une étape supplémentaire au protocole, soit une étape afin de permettre à Alice et à Bob de corriger les erreurs dans leurs données. Pour ce faire, Alice et Bob doivent exécuter via le canal classique un protocole de correction des erreurs. La section qui suit détaille le protocole tel que choisie par Bennett et Brassard [2] pour leurs expériences de 1989.

Ensuite, pour résoudre le deuxième problème, plutôt que de produire des impulsions lumineuses contenant exactement un photon, on produit des impulsions lumineuses de très faible intensité μ, où μ est le nombre de photons par impulsion. Ces impulsions lumineuses sont très faciles à obtenir en utilisant un laser [5] et le nombre moyen de photons par impulsion pour ces impulsions suit une distribution de Poisson. Toutefois, en procédant ainsi, Ève aura la chance, chaque fois qu'une impulsion lumineuse contient plus d'un photon, de dévier vers son appareil un des photons de cette impulsion et de mesurer la polarisation selon l'une des deux bases. Ce type d'attaque connue sous le nom de "beam splitting attack" est tout à fait indétectable tant et aussi longtemps qu'Ève prend soin de toujours laisser les photons non-déviés de l'impulsion atteindre l'appareil de Bob sans être perturbés, et que l'intensité de l'impulsion lumineuse est assez intense. Il est important de noter qu'en fait, plus l'intensité d'une impulsion lumineuse est grande

plus elle aura un comportement semblable aux signaux classiques. Par ailleurs, la probabilité qu'Ève réussisse à dévier un ou plusieurs photons d'un impulsion donnée sans causer de perturbation aux autres photons est égale à $\frac{\mu^2}{2}$ lorsque μ est suffisamment petit [2]. Ainsi, afin d'empêcher le plus souvent possible Ève de mener son attaque, on doit choisir $\mu << 1$, c'est-à-dire qu'Alice doit envoyer à Bob des impulsions lumineuses de très faible intensité. Ceci diminue certainement les chances que Bob détecte un photon, mais les chances qu'Ève et Bob détectent tous deux un photon sont encore plus faibles. Toutefois, même si la valeur de μ est très petite, Ève gagnera toujours de l'information en menant cette attaque. Par exemple, si $\mu = 10^{-3}$ alors Ève connaîtra toujours 0,025% [2] des données d'Alice et Bob. Il devient donc impossible pour Alice et Bob d'interpréter leurs données pour obtenir directement une clef secrète. En ajoutant au protocole une procédure de purification ("amplification privacy protocol"), Alice et Bob pourrons alors obtenir une clef secrète dont Ève ne connaîtra au maximum qu'une fraction de 1 bit d'information.

La section qui suit reprend le protocole de la section 3.2 en y détaillant les nouvelles étapes.

3.5 Le protocole BB84 mis en pratique

Il faut tout d'abord revoir l'étape 5 du protocole de la section 3.2. En fait, puisque les imprécisions dues aux photo-détecteurs et celles dues à l'espionnage fait sur le canal quantique sont indissociables, Alice et Bob n'ont d'autre choix que de tenter de corriger les incohérences présentes dans leurs données. La procédure de correction des erreurs présentée dans [2] requiert qu'Alice et Bob suivent les étapes suivantes:

1. Choisir une permutation aléatoire (et la transmettre via le canal classique [3].)
2. Appliquer cette permutation à leurs données.
3. Diviser les données après permutation en bloc de taille κ où κ est déterminé à partir du taux d'erreur estimé et de sorte que la probabilité qu'un bloc contienne plus d'une erreur soit faible.
4. Comparer la parité des bloc:
   - les blocs de même parité sont acceptés temporairement comme étant sans erreur,
   - l'erreur dans les blocs de parité différente est localisée à l'aide d'une recherche dichotomique et est corrigée.
5. Rejeter toutes les dernières données [4] de chacun des blocs.

2. Car 99,95% des impulsions contenant au moins un photon n'en contiennent qu'un seul.
3. On suppose que le canal classique ne peut pas subir d'attaque actives.
4. Une donnée correspond à 1 bit.

Cette dernière étape est nécessaire afin d'empêcher Ève, qui a la possibilité d'écouter les message sur le canal classique, de gagner de l'information lors de cette procédure. Par ailleurs, cette procédure ne permet pas de corriger toute les erreurs, comme dans le cas de blocs contenant un nombre pair d'erreurs. Alice et Bob doivent donc répéter la procédure jusqu'à ce qu'il ne reste plus que très peu d'erreurs dans l'ensemble de leurs données. Puis, pour corriger ces quelques erreurs, ils doivent compléter les étapes précédentes en comparant, l'un après l'autre, des sous-ensembles de données, pas nécessairement de même taille, pris aléatoirement parmi l'ensemble de toutes leurs données et répéter la procédure jusqu'à ce qu'environ 20 sous-ensembles considérés successivement soient tous de même parité. À ce point les données d'Alice et Bob concordent, mais ils leur est impossible de déterminer si les erreurs corrigés étaient dues aux photo-détecteurs ou à l'espionnage. Ils ne peuvent donc pas déterminer s'il y a eu espionnage ou non. Ce qui est une grande perte selon mon opinion car dans tous les cas, Alice et Bob ne peuvent pas utiliser toutes leurs données pour produire leur clef et devront en sacrifier un bonne partie pour obtenir une clef secrète. Ils doivent donc supposer en tout temps que leurs données ne sont que partiellement secrètes (clef impure) et essayer de déterminer quelle est la quantité d'information qu'Ève possède de ces données. Bennett et Brassard dans [2] donnent une borne supérieure pour cette valeur:

$$k = N\left(\frac{\mu}{2} + 2p\right) \text{ bits},$$

où N est le nombre de photons reçus et mesurés dans la bonne base par Bob, μ est l'intensité des impulsions lumineuses, et p est le taux estimé d'erreurs dans les données. Ainsi, si la longueur de la clef impure x est n, k est le nombre de bits d'information que possède Ève et $s > 0$ est un paramètre de sécurité, alors comme démontré dans [4], il suffit qu'Alice et Bob choisissent aléatoirement une fonction de condensation $h : \{0,1\}^n \to \{0,1\}^{n-k-s}$, telle que l'information qu'Ève aura de $h(x)$ sera seulement de $\frac{2^{-s}}{\ln 2}$ bits. Le choix et l'application de cette fonction de condensation constitue maintenant la dernière étape du protocole et est la procédure de purification.

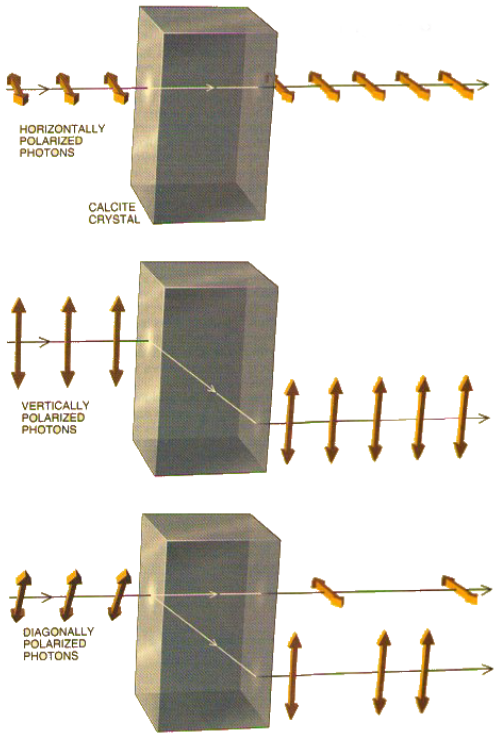
Voyons maintenant quels sont les résultats obtenus des expériences faites à partir du premier prototype opérationnel basé sur cette version du protocole.

3.6 Premières expériences

Pour mettre en pratique le protocole, il faut construire un canal quantique et les appareils nécessaires aux deux utilisateurs pour exécuter le protocole en se servant de ce canal:

1. Un filtre polarisant ou tout autre dispositif permettant à Alice de préparer des photons selon les polarisation choisies.
2. Un deuxième filtre polarisant ou tout autre dispositif permettant à Bob de mesurer la polarisation des photons selon une base choisie aléatoirement. En

FIG. 5 – *Cristal de calcite*



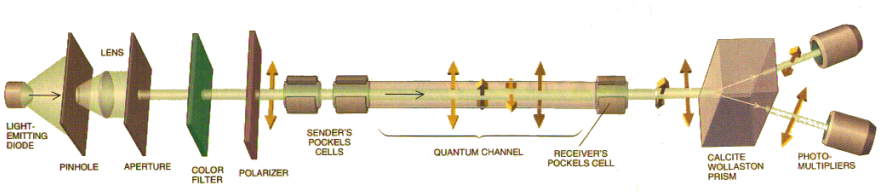
général, il est avantageux d'utiliser un cristal de calcite (Figure 5) puisque ce cristal envoie selon leur polarisation, les photons incidents dans une de deux directions sans en absorber aucun.

3. Deux photo-détecteurs pour détecter et enregistrer les photons.
4. Un canal quantique composé de fibres optiques ou un canal de transmission rectiligne sous vide, pour la transmission des photons d'Alice à Bob.

À la Figure 6, l'ensemble des composantes optiques et électroniques à la gauche du canal quantique est tout ce dont Alice a besoin pour créer ses photons et les polariser selon les bases choisies, alors qu'à la droite du canal quantique on retrouve les composantes de l'appareil de Bob. La composante électro-optique appelée "Pockels cell" se retrouvant à chacun des extrémités du canal agit comme un filtre polarisant. Si l'on choisit d'utiliser les bases rectilinéaire et circulaire comme paires de propriétés complémentaires c'est parce que la tension requise [2] pour faire passer le "Pockels cell" d'une base à l'autre est minimum pour ce choix.

Le premier prototype réalisé par Bennett et Brassard en 1989 et auquel ont contribué John Smolin, maintenant à l'université de la Californie, pour les com-

FIG. 6 – *Un canal quantique et les appareils des deux utilisateurs*



posantes optiques et électroniques ainsi que François Bessette et Louis Salvail de l'université de Montréal, pour le programme informatique, avait les caractéristiques suivantes:

- Le canal quantique était un canal optique sous-vide rectiligne de 32 cm.
- Le prototype était contrôlé par un programme contenant des sous-routines pour simuler Alice, Bob et au besoin, Ève.
- Les choix de polarisation des photons et les choix de bases pour mesurer la polarisation des photons étaient faits à partir d'une disquette contenant une suite de bits aléatoires générés de la façon suivante:
  1. Sauvegarde des données physiques fournies par les enregistrements aléatoires des photo-détecteures.
  2. Obtention d'une distribution uniforme des 0 et 1 en utilisant l'algorithme de von Neumann.
  3. Addition modulo 2 des bits résultants avec des bits pseudo-aléatoires générés par ordinateur.
- Les photo-détecteurs avaient une efficacité de 9% avec un taux de "dark counts" de $1500/s$.
- L'intensité des impulsions lumineuses était de $\mu = 0{,}17$ photons par impulsion.
- Les routines pour simuler l'espionnage sur le canal quantique permettaient les attaques "intercept/resend" et "beam splitting" pour un espion muni de photo-détecteurs efficaces à 100%.

Supposons que l'on désire faire une expérience avec ce prototype. On peut d'abord effectuer le calcul théorique suivant: si 85000 impulsions lumineuses sont produites avec une intensité de $\mu = 0{,}17$, alors ≈ 14167 photons seront envoyés à Bob. Les photo-détecteurs de Bob n'étant efficaces qu'à 9%, alors seulement ≈ 1275 photons devraient être détectés. Toutefois, Bob ne faisant le bon choix de base qu'une fois sur deux, alors seulement ≈ 638 photons pourront être utilisés comme données.

En fait, Bennett et Brassard ont réalisé cette expérience le vendredi 13 (!) avril 1990 et ont obtenu les résultats suivant: 640 photons furent reçus correctement et

dans la bonne base par Bob. Les données d'Alice contenaient 242 bits de valeur 1 pour ces 640 bits correspondant (la distribution n'est pas uniforme). Les 640 bits de données de Bob contenaient 28 erreurs soit un taux d'erreur de 4.375%. Après la correction de ces 28 erreurs, Alice et Bob avaient estimé que le taux d'erreur était de 4.5%, et le nombre de bits restants était de 419. Alice et Bob avaient ensuite estimé qu'Ève possédait

$$k = 640\left(\frac{0{,}17}{2} + 2(0{,}045)\right) = 112 + 28 = 140 \text{ bits d'information,}$$

où les 28 bits supplémentaires sont dus à la distribution non uniforme de 1 et de 0. Finalement, après avoir appliqué une fonction de condensation à leur clef impure, Alice et Bob ont obtenu une clef secrète de 219 bits.

Le prototype et les expériences menées à partir de ce dernier montrent qu'il est possible de réaliser physiquement le protocole. À Genève, un autre prototype pour ce protocole fut construit et utilisait comme canal quantique un solénoïde de 1km de fibres optiques. Toutefois les propriétés des fibres optiques connues aujourd'hui limitent l'utilisation du protocole, car le signal déjà de faible intensité s'atténue en parcourant la fibre optique. Il sera donc, sur de longues distances, indétectable à la sortie du canal. De plus, le principe même interdit que les impulsion lumineuses soient amplifiées avant d'être envoyées dans une fibre optique, ou que cette fibre optique contienne des répétiteurs qui lisent le signal et le réémettent. Ainsi, pour mieux réussir, il faudrait réaliser des progrès dans la qualité des fibres optiques ou encore utiliser des canaux de transmission sous-vide complètement rectilignes, ce qui n'a de sens que dans l'espace mais qui permettrait la transmission du signal sur une distance aussi grande que l'on veut.

4 Conclusion

Lors des analyses faites dans les sections précédentes, nous n'avons pas considéré la possibilité qu'Ève puisse intercepter et modifier des messages échangés entre Alice et Bob par le canal classique. En fait ce problème ne relève pas de la cryptographie quantique, mais un partenariat entre la cryptographie classique et la cryptographie quantique permet de résoudre ce problème d'une façon inattendue. La cryptographie classique propose, pour assurer l'authenticité des messages échangés par le canal classique, qu'Alice et Bob utilise l'algorithme de Wegnam-Carter [3, 5] pour étiqueter leurs messages. Cet algorithme nécessite une clef secrète partagée par Alice et Bob qui sera utilisée bit par bit et devra être renouvelée. La cryptographie quantique propose donc de permettre à Alice et Bob d'échanger cette clef secrète chaque fois qu'il sera nécessaire, en plus de toutes les autres clefs qu'Alice et Bob auront besoin pour chiffrer leurs messages, et ce d'une façon tout à fait sécuritaire. Toutefois, un tout petit problème subsiste: il faut, afin d'initier ce cycle d'échange infini, qu'Alice et Bob aient préalablement et d'une façon quelconque,

échanger une toute petite clef qui sera la première à être utilisée pour l'algorithme d'authentification!

References

[1] C.H. Bennett. Quantum cryptography: Uncertainty in the service of privacy. *Science*, 257:752–753, August 1992.

[2] C.H. Bennett, G. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. *Advanges in Cryptology - Eurocrypt '90 Proceedings*, pages 351–366, May 1990.

[3] C.H. Bennett, G. Brassard, and A.K. Ekert. Quantum cryptography. *Scientific American*, pages 50–57, October 1992.

[4] C.H. Bennett, G. Brassard, and J.-M. Robert. Privacy emplification by public discussion. *SIAM Journal on Computing*, 2:210–229, April 1988.

[5] G. Brassard. *Modern Cryptology*, volume 325 of *Lecture Notes in Computer Science*, chapter 6, pages 79–90. Springer-Verlag, 1988.

[6] G. Brassard. Quantum information processings: The good, the bad and the ugly. *Advances in Cryptology - CRYPTO '97*, pages 237–241, 1997.

[7] J.-P. Delahaye. Cryptographie quantique. *Pour la science*, pages 101–106, Août 1992.

[8] A.K. Ekert. What is quantum cryptography. Disponible à l'adresse internet donnée plus bas, March 1995.

[9] A.K. Ekert. Quantum cryptography for keepings secrets. *New Scientist*, pages 24–28, January 1993.

[10] A. Muller, J. Breguet, and N. Gisin. Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1km. *Europhysics Letters*, 23:383–388, August 1993.

Une version de [2] ainsi que les images du présent document sont disponibles en deux parties aux adresses `http://www.cyberbeach.net/~jdwyer/quantum_crypto/quantum1.htm`, et `http://www.cyberbeach.net/~jdwyer/quantum_crypto/quantum2.htm`. Le texte de [8] est disponible à l'adresse `http://www.qubit.org/intros/crypt.html`. Une bibliographie très complète sur la cryptographie quantique écrite par Gilles Brassard et revue par Claude Crépeau est disponible à l'adresse `http://www.cs.mcgill.ca/~jford/crepeau/CRYPTO/Biblio_QC.html`. Finalement, le tutoriel de F. Hendle utilisé pour l'exemple de la section 3.2 est disponible à l'adresse `http://www.cs.dartmouth.edu/~henle/Quantum/` et le document écrit par J. Ford accompagnant ce tutoriel est disponible à l'adresse `http://www.cs.dartmouth.edu/~jford/crypto.html`.