UNE ILLUSTRATION DES POSTULATS DE LA MECANIQUE QUANTIQUE

LA CRYPTOGRAPHIE QUANTIQUE

La *cryptographie* est l'art – vieux comme le monde – de communiquer au moyen de conventions assurant que le message transmis est à l'abri des indiscrétions. L'idée la plus naturelle est d'utiliser un *codage* des messages confidentiels : toute lettre de l'alphabet est remplacée biunivoquement par un autre signe (nombre – d'où l'expression *message chiffré* – image, symbole exotique *etc.*). Le lexique donnant la correspondance biunivoque s'appelle la *clé* et c'est elle qui doit rester absolument confidentielle. Ce procédé porte précisément le nom de *cryptographie à clé secrète.*

Il existe aussi des procédés dits *à clé publique*, l'idée étant que certaines opérations mathématiques s'effectuent trivialement dans un sens et exigent un travail colossal dans l'autre : par exemple, il est facile de multiplier deux nombres premiers, alors que la factorisation d'un (grand) nombre N en ses premiers entiers exigent un temps de calcul croissant en gros exponentiellement avec N .

L'élément crucial est la **confidentialité de la clé** permettant de coder et de décoder le message transmis, étant entendu que celui-ci peut à la limite être rendu public. Tout le problème est donc de d'assurer la sécurité du message initial définissant la clé.

Toute transmission classique d'information peut être interceptée passivement, c'est-à-dire sans modification de la teneur du message ; bien sûr, il peut y avoir d'énormes difficultés techniques à surmonter pour y parvenir, mais c'est en principe possible : l'écoute d'une ligne téléphonique perturbe en un sens la ligne – donc ouvre la voie à la révélation de l'écoute – mais on peut réduire cet effet révélateur pour rendre l'écoute quasiment indétectable. Au contraire, parce qu'une mesure quantique perturbe en général le système objet de la mesure, l'observation indésirable peut être en principe facilement détectée.

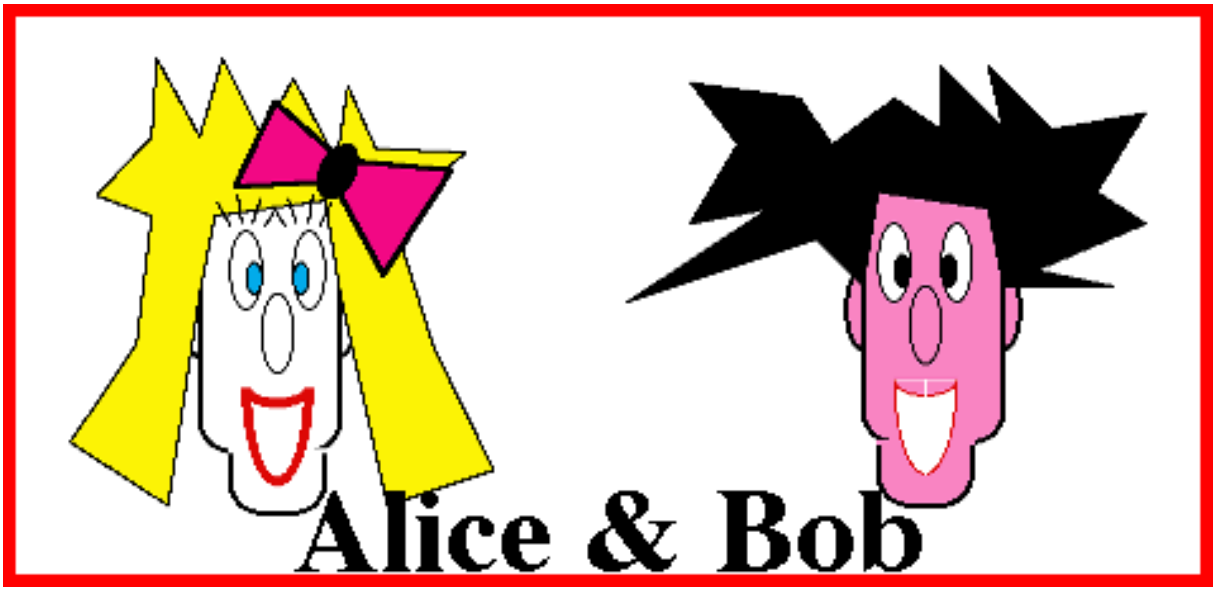
La mesure ne provoque pas *toujours* une « perturbation incontrôlable », comme on le voit souvent écrit. Si l'état du système est, avant la mesure, propre de l'observable mesurée, il l'est encore après : en pareil cas, la mesure est « non-destructive ».

La mécanique quantique permet ainsi de construire des procédures permettant de savoir si, lors d'une transmission, on est écouté ou non. Il s'agit ici de se borner à donner quelques idées de base, étant entendu qu'il existe une littérature énorme sur le sujet, où divers scénarios sont envisagés et décrits.

La littérature a pris l'habitude d'appeler Alice et Bob les deux personnes communiquant entre elles et souhaitant se mettre à l'abri des malversations d'un « espion ». Ce dernier est souvent appelé Eve (ce nom vient de *to eavesdrop = écouter aux portes !).*

Dans la suite, on considère un premier exemple, formel, posant les idées essentielles montrant comment la mécanique quantique permet de concevoir des protocoles révélant *à coup sûr* la présence d'une écoute indésirable. Deux exemples utilisant soit un atome àtrois niveaux, soit des spins $\frac{1}{2}$ sont ensuite exposés en détail. Dans un dernier temps, on examine le point le plus essentiel, à savoir comment transmettre la clé en toute confidentialité, suivant

la proposition d'Ekert (A. K. Ekert, « *Quantum Crytography Based on Bell's Theorem* » Phys.Rev.Let., **68**, 661 (1991))



1. Principes et exemples de la détection d'une écoute indésirable

Principes :

L'idée de base est simple et met en jeu des séquences de mesures successives d'observables qui ne commutent pas. De façon un peu abstraite, les choses se présentent comme suit. Soit $\hat{A}$ et $\hat{B}$ deux observables incompatibles :

$$\left[\hat{A},\hat{B}\right]\neq 0 \quad (1)$$

dont l'une, A pour fixer les idées, est une constante du mouvement :

$$\left[\hat{A},\hat{H}\right]=0 \quad (2)$$

alors que $\hat{B}$ n'en est pas une. A un certain instant , $t=0$, on mesure $\hat{A}$ et on trouve a_m, l'une des valeurs propres de $\hat{A}$; on sait d'avance que la probabilité d'obtenir cette valeur est égale à $\left|\left\langle a_m\middle|\psi(t=0)\right\rangle\right|^2$. Juste après cette mesure, l'état du système est $\left|\psi(t=0+0)\right\rangle=\left|a_m\right\rangle$. Si aucune autre mesure n'est effectuée jusqu'à l'instant t, (dans ces conditions, le système évolue librement par l'équation de Schrödinger), une nouvelle mesure de $\hat{A}$ à cet instant donne le résultat a_m cette fois avec certitude. En effet, l'état à l'instant t est $\left|\psi(t)\right\rangle=\hat{U}(t)\left|a_m\right\rangle$, mais comme $\hat{A}$ et $\hat{H}$ commutent, l'état $\left|a_m\right\rangle$ produit par la réduction du paquet d'onde consécutive à la première mesure de $\hat{A}$, est également propre de $\hat{H}$ (on suppose ici pour l'instant, pour simplifier la discussion, qu'il n'existe aucune dégénérescence) ; il en résulte que $\left|\psi(t)\right\rangle=e^{-\frac{i}{\hbar}E_m t}\left|a_m\right\rangle$ et que la deuxième mesure de $\hat{A}$ produit la même valeur a_m avec probabilité 1. Si les deux mesures sont effectuées par deux opérateurs distincts, ces derniers doivent donc constater que leurs résultats

sont toujours identiques, quand la même séquence est répétée un grand nombre de fois, à la limite infini.

Imaginons maintenant au contraire que, entre la première mesure de $\hat{A}$ et la seconde, à l'instant $t_1\,(0<t_1<t)$, une tierce personne mesure $\hat{B}$, qui n'est pas une constante du mouvement. Cet »espion » trouve l'une des valeurs propres de $\hat{B}$, b_n, et l'état issu de cette mesure est (on continue à supposer qu'il n'existe pas de dégénérescence) $\left|\psi\left(t=t_1+0\right)\right\rangle=\left|b_n\right\rangle$. Il ne s'agit pas d'un état stationnaire, puisque $\hat{H}$ et $\hat{B}$ ne commutent pas ; à l'instant t, cet état est devenu :

$$\left|\psi\left(t\right)\right\rangle=\sum_{m'}c_{m'}e^{-\frac{i}{\hbar}E_{m'}\left(t-t_1\right)}\left|a_{m'}\right\rangle \quad ; \quad c_{m'}=\left\langle a_{m'}\middle|b_n\right\rangle \quad ; \quad t_1<t \quad (3)$$

Dans ces conditions, la mesure de $\hat{A}$ à l'instant t postérieur à t_1 peut alors produire *l'une quelconque* des valeurs propres $a_{m'}$ - la probabilité de trouver $a_{m'}$ est $P_{m'}=\left|c_{m'}\right|^2$; le résultat brut est que les résultats obtenus par Alice et Bob effectuant les deux mesures de $\hat{A}$ ne sont plus nécessairement identiques. En fait, lorsque la séquence est répétée un grand nombre de fois, il suffit que *l'un* de leurs résultats soit différents pour qu'ils puissent affirmer avec certitude qu'ils sont victimes d'une écoute et que la sécurité de leur transmission n'est pas assurée.

Exemples :

Exemple 1 :

Précisons les idées précédentes dans un cas concret, où d'ailleurs le Hamiltonien présente de la dégénérescence. Soit un atome à trois niveaux $\left\{\left|p\right\rangle\right\}$ (un fondamental $p=0$ et deux niveaux excités dégénérés, $p=1,2$) :

$$\hat{H}=\hbar\omega\left(-\left|0\right\rangle\left\langle 0\right|+\left|1\right\rangle\left\langle 1\right|+\left|2\right\rangle\left\langle 2\right|\right) \quad (4)$$

$\hat{A}$ est une observable donnée par :

$$\hat{A}=a\left(\left|0\right\rangle\left\langle 0\right|+i\left|1\right\rangle\left\langle 2\right|-i\left|2\right\rangle\left\langle 1\right|\right) \quad \left(a\in\Re\right) \quad (5)$$

$\hat{A}$ commute visiblement avec $\hat{H}$, c'est donc une constante du mouvement. Ses valeurs propres sont $+a$ (dégénérescence 2) et $-a$ (non-dégénérée). Les vecteurs propres de $\hat{A}$ (qui sont aussi vecteurs propres de $\hat{H}$) sont les $\left|\psi_{\alpha\beta}\right\rangle\left(\alpha,\beta=\pm\right)$:

$$\begin{cases}\left|+a,1\right\rangle=\left|0\right\rangle\equiv\left|\psi_{-+}\right\rangle\\ \left|+a,2\right\rangle=\dfrac{1}{\sqrt{2}}\left(\left|1\right\rangle-i\left|2\right\rangle\right)\equiv\left|\psi_{++}\right\rangle\\ \left|-a\right\rangle=\dfrac{1}{\sqrt{2}}\left(-i\left|1\right\rangle+\left|2\right\rangle\right)\equiv\left|\psi_{+-}\right\rangle\end{cases} \quad (6)$$

Le premier indice de $\left|\psi_{\alpha\beta}\right\rangle$ renvoie à la valeur propre $\pm\hbar\omega$ de $\hat{H}$, le second au signe de la valeur propre $\pm a$ de $\hat{A}$.

L'observable $\hat{B}$ est prise sous la forme :

$$\hat{B} = b\left(|0\rangle\langle 1| + |1\rangle\langle 0| + |2\rangle\langle 2|\right) \quad (b \in \Re) \quad (7)$$

clairement : $\left[\hat{A}, \hat{B}\right] \neq 0$; $\left[\hat{H}, \hat{B}\right] \neq 0$ (8)

Les valeurs propres de $\hat{B}$ sont $+b$ (dégénérescence 2) et $-b$ (non dégénérée) ; les vecteurs propres sont :

$$\begin{cases} |+b,1\rangle = |2\rangle \\ |+b,2\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \\ |-b\rangle = \frac{1}{\sqrt{2}}\left(-|0\rangle + |1\rangle\right) \end{cases} \quad (9)$$

Maintenant, Alice et Bob effectuent des mesures de $\hat{A}$ aux instants 0 et t. Compte tenu de la dégénérescence en énergie, l'opération de mesure peut porter sur un ensemble complet d'observables qui commutent, ce que constituent $\hat{A}$ et $\hat{H}$; à l'issue d'une telle opération, l'état du système est parfaitement défini. Si aucune mesure de $\hat{B}$ n'est faite entre-temps, les résultats des deux observateurs coïncident dans tous les cas.

En revanche, soit une mesure de $\hat{B}$ effectuée à l'instant t_1 compris entre 0 et t. Pour fixer les idées, on suppose que le premier observateur a trouvé $+\hbar\omega$ et $+a$; l'état de départ est donc $|\psi(0+)\rangle = |\psi_{++}\rangle$. Compte tenu des décompositions ci-dessus, l'état à l'instant t_1 est :

$$|\psi(t_1)\rangle = e^{-i\omega t_1}\frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2}}\left(|+b,2\rangle + |-b\rangle\right) - i|+b,1\rangle\right] \quad (10)$$

Il en résulte que la mesure à t_1 donne $+b$ avec la probabilité $\frac{3}{4}$, $-b$ avec la probabilité $\frac{1}{4}$. Dans le premier cas, l'état à $t_1 + 0$ est :

$$|\psi(t_1 + 0)\rangle = \frac{\sqrt{2}}{\sqrt{3}}\left[\frac{1}{\sqrt{2}}|+b,2\rangle - i|+b,1\rangle\right] \quad (11)$$

Un calcul simple montre que cet état devient, à l'instant t :

$$|\psi(t)\rangle = \frac{\sqrt{2}}{\sqrt{3}}\left[\frac{1}{2}e^{+i\omega(t-t_1)}|\psi_{-+}\rangle + \frac{3}{2\sqrt{2}}e^{-i\omega(t-t_1)}|\psi_{++}\rangle - \frac{i}{2\sqrt{2}}e^{-i\omega(t-t_1)}|\psi_{+-}\rangle\right] \quad (12)$$

Pour cette « histoire », le deuxième observateur va trouver les valeurs $(-\hbar\omega, +a), (+\hbar\omega, +a)$ et $(+\hbar\omega, -a)$ avec les probabilités respectives $\frac{1}{6}, \frac{3}{4}$ et $\frac{1}{12}$, au lieu de trouver à coup sûr le même résultat que le premier observateur.

Si la mesure intermédiaire donne $-b$, on a successivement :

$$|\psi(t_1 + 0)\rangle = |-b\rangle \quad (13)$$

qui devient :

$$|\psi(t)\rangle = \frac{1}{\sqrt{2}}e^{i\omega(t-t_1)}|\psi_{-+}\rangle + \frac{1}{2}e^{-i\omega(t-t_1)}|\psi_{++}\rangle + \frac{i}{2\sqrt{2}}e^{-i\omega(t-t_1)}|\psi_{+-}\rangle \quad (14)$$

Le deuxième observateur va trouver les valeurs $(-\hbar\omega, +a), (+\hbar\omega, +a)$ et $(+\hbar\omega, -a)$ avec les probabilités respectives $\frac{1}{2}, \frac{1}{4}$ et $\frac{1}{4}$.

Ainsi, au coup par coup, Alice et Bob peuvent trouver des résultats différents. La probabilité qu'ils trouvent des résultats identiques est une probabilité conditionnelle :

$$P_{\text{résultats identiques}} \equiv P\left(++;t\middle|++,t=0\right) \quad (15)$$

qui peut s'exprimer suivant la relation de chaîne habituelle (relation dite de Bachelier-Chapman-Kolmogorov).

$$P\left(++;t\middle|++;0\right)=\sum_{\varepsilon=\pm1}P\left(++;t\middle|\varepsilon b;t_1\right)P\left(\varepsilon b;t_1\middle|++;0\right) \quad (16)$$

Cette dernière expression est la somme sur toutes les « trajectoires » possibles (la somme représente l'addition des probabilités d'événements mutuellement exclusifs), une mesure intermédiaire ayant été faite. (lorsqu' aucune mesure intermédiaire n'est faite, la probabilité est le module au carré d'une *somme d'amplitudes*. Ici compte tenu de la réduction du paquet d'onde lié à la mesure de $\hat{B}$ à t_1, la probabilité est une *somme de probabilités*, chacune de celles-ci étant le module au carré d'une amplitude.) On a donc ici :

$$P\left(++;t\middle|++;0\right)=\frac{3}{4}\times\frac{3}{4}+\frac{1}{4}\times\frac{1}{4}=\frac{5}{8} \quad (17)$$

Le choix d'un autre résultat pour la première mesure du couple $\left(\hat{H},\hat{A}\right)$ conduit au même type de conclusion : en raison de la mesure effectuée par un tiers, la probabilité que les résultats soient identiques est loin d'être égale à 1 ; le calcul montre qu'elle vaut $\frac{1}{2}$ si la première mesure à donné $\left(-\hbar\omega,+a\right)$ et $\frac{5}{8}$ si on a d'abord trouvé $\left(+\hbar\omega,-a\right)$. Dans tous les cas, au bout de quelques expériences, Alice et Bob peuvent avec une quasi-certitude affirmer qu'ils sont écoutés.

(Toutes les probabilités exhibées ne dépendant pas du temps. En effet :

- quand il s'agit de mesures de $\hat{A}$, toutes les réductions de paquet d'onde produisent des états stationnaires
- en ce qui concerne la mesure de $\hat{B}$: l'état sur lequel on mesure est propre de $\hat{A}$ et $\hat{H}$, c'est encore un état stationnaire et donc les probabilités de trouver les valeurs $\pm b$ sont indépendantes du temps. Enfin à l'issu de la mesure de $\hat{B}$ à t_1 est $\left|b,i=1,2\right\rangle$ ou $\left|-b\right\rangle$. Lors de la mesure de $\hat{A}$ et $\hat{H}$ à $t>t_1$, les probabilités sont de la forme $\left|\left\langle\psi_{\alpha\beta}\middle|\hat{U}\left(t-t_1\right)\middle|b,i=1,2\right\rangle\right|^2$ ou $\left|\left\langle\psi_{\alpha\beta}\middle|\hat{U}\left(t-t_1\right)\middle|-b\right\rangle\right|^2$; $\hat{U}$ agissant sur le bra produit une simple phase temporelle qui disparaît du module au carré.)

Exemple 2 :

Une autre procédure utilise l'envoi de spins $\frac{1}{2}$ par Alice et Bob (d'autres versions sont possibles ; par exemple, on peut disposer d'une source fabriquant des paires de spins d'état bien défini, l'un des spins étant envoyé vers Alice, l'autre vers Bob ; un espion mesurant le spin allant vers Bob va induire des différences entre les résultats des mesures des deux observateurs) . Le spin $\frac{1}{2}$ est une variable binaire qui se prête donc bien au codage : on peut mettre en correspondance biunivoque l'écriture binaire d'un nombre avec une configuration de spins $++-+-+-\cdots+$.Ici, pour un Hamiltonien à symétrie sphérique, toutes les composantes $\hat{S}_u$ des spins sont des constantes du mouvement ; les observables incompatibles en jeu sont bien évidemment les différentes composantes cartésiennes de $\hat{\vec{S}}$, satisfaisant les relations caractéristiques d'un moment cinétiques :

$$\hat{\vec{S}} \wedge \hat{\vec{S}} = i\hbar \hat{\vec{S}} \Leftrightarrow \left[\hat{S}_x, \hat{S}_y \right] = i\hbar \hat{S}_x, \text{ etc} \cdots \quad (18)$$

En vertu de la relation $\hat{\vec{S}} = \frac{\hbar}{2} \hat{\vec{\sigma}}$, on peut raisonner avec les trois composantes de $\hat{\vec{\sigma}}$. Par ailleurs, puisque les composantes du spin sont des constantes du mouvement, seule une mesure intermédiaire d'une composante incompatible est susceptible de modifier, lors d'une mesure ultérieure, la valeur trouvée au départ.

Alice choisit de mesurer la composante suivant Oz, trouve donc à chaque fois ± 1 et envoie le spin mesuré à Bob. Celui-ci mesure la composante de $\hat{\vec{S}}$ le long d'un axe OZ faisant l'angle θ avec l'axe Oz d'Alice et situé dans le plan xOz (Alice et Bob sont d'avance convenus d'une même orientation de leurs repères locaux). L'observable que mesure Bob est donc :

$$\hat{\sigma}_Z = \cos\theta \, \hat{\sigma}_z + \sin\theta \, \hat{\sigma}_x \quad ; \quad \left[\hat{\sigma}_z, \hat{\sigma}_Z \right] = 2i \sin\theta \hat{\sigma}_y \quad (19)$$

Bien évidemment, Alice et Bob ne vont pas trouver les mêmes résultats, puisqu'ils mesurent deux observables qui ne commutent pas – sauf si $\theta = 0$. Les états propres de $\hat{\sigma}_Z$, qui a évidemment pour valeurs propres ± 1, sont :

$$\begin{cases} |+\rangle_Z = \cos\frac{\theta}{2} |+\rangle_z + \sin\frac{\theta}{2} |-\rangle_z \\ |-\rangle_Z = -\sin\frac{\theta}{2} |+\rangle_z + \cos\frac{\theta}{2} |-\rangle_z \end{cases} \quad (20)$$

comme on le vérifie facilement. Ceci étant donné, on voit que si Alice a trouvé $+1$ - et envoie à Bob un spin dans l'état $|+\rangle_z$ - , celui-ci peut trouver $+1$ ou -1, avec les probabilités respectives $\cos^2\frac{\theta}{2}$ et $\sin^2\frac{\theta}{2}$. Bien sûr, si $\theta = 0$, Alice et Bob trouvent *toujours* les mêmes résultats. Si Bob mesure suivant un axe tourné de $\frac{\pi}{2}$ (appelons-le $Ox, OZ = Ox$), alors :

$$\begin{cases} |+\rangle_x = \frac{1}{\sqrt{2}} \left(|+\rangle_z + |-\rangle_z \right) \\ |-\rangle_x = \frac{1}{\sqrt{2}} \left(-|+\rangle_z + |-\rangle_z \right) \end{cases} \quad (21)$$

dans ces conditions, si Alice a trouvé $+$, *etc, :* Bob ne trouve comme Alice que dans 50% des cas.

Maintenant, un espion situé sur le trajet du spin procède à des mesures suivant un axe faisant l'angle ϕ avec Oz ; l'observable que mesure l'espion est donc :

$$\hat{\sigma}_e = \cos\phi \, \hat{\sigma}_z + \sin\phi \, \hat{\sigma}_x \quad (22)$$

observable dont les vecteurs propres sont :

$$\begin{cases} |+\rangle_e = \cos\frac{\phi}{2} |+\rangle_z + \sin\frac{\phi}{2} |-\rangle_z \\ |-\rangle_e = -\sin\frac{\phi}{2} |+\rangle_z + \cos\frac{\phi}{2} |-\rangle_z \end{cases} \quad (23)$$

Pour fixer les idées, on raisonne après une mesure d'Alice ayant donné $+1$, de sorte que l'espion effectue une mesure sur l'état $|+\rangle_z$: il trouve donc :

$$\begin{cases} +1 \text{ avec la probabilité } \cos^2\dfrac{\phi}{2} \\ -1 \text{ avec la probabilité } \sin^2\dfrac{\phi}{2} \end{cases}$$

Puis Bob procède à la mesure de $\hat{\sigma}_Z$: si l'espion a trouvé $+1$, Bob trouve $+1$ ou -1 avec les probabilités respectives $\cos^2\dfrac{\theta-\phi}{2}$ et $\sin^2\dfrac{\theta-\phi}{2}$. Si l'espion a trouvé -1, Bob trouve -1 ou $+1$ avec les probabilités respectives $\cos^2\dfrac{\theta-\phi}{2}$ et $\sin^2\dfrac{\theta-\phi}{2}$. En définitive, la probabilité pour que Alice et Bob aient le même résultat $+1$ est donc :

$$P_\phi\left(+,\theta\middle|+,0\right)=\cos^2\frac{\phi}{2}\cos^2\frac{\theta-\phi}{2}+\sin^2\frac{\phi}{2}\sin^2\frac{\theta-\phi}{2} \quad (24)$$

En particulier, si Alice et Bob sont convenus de mesurer le long du même axe $Oz\,(\theta=0)$, la probabilité de coïncidence de leurs résultats est :

$$P_\phi\left(+,\theta\middle|+,0\right)=\cos^4\frac{\phi}{2}+\sin^4\frac{\phi}{2}=\frac{1}{2}\left(1+\cos^2\phi\right) \quad (25)$$

Au total, pour faire parvenir un message de n bits, Alice doit envoyer Nn spins, N étant pris très grand de sorte que les fréquences statistiques puissent être confondues avec les lois limites de probabilités. Bob peut retourner à Alice tous ses spins, par une voie dont la confidentialité a été établie antérieurement ; le produit Nn étant forcément très grand – et la probabilité (25) étant évidemment plus petite que 1 - (sauf si l'espion connaît l'angle choisi par Alice et Bob) - , les deux observateurs vont très vite s'apercevoir s'ils sont écoutés ou non.

L'espion, ne connaissant pas la direction commune d'observation d'Alice et Bob, peut décider de tirer au hasard la sienne, en prenant l'angle ϕ uniformément distribué entre 0 et 2π. La probabilité de coïncidence moyennée est :

$$P_\phi\left(+,0\middle|+,0\right)=\int_0^{2\pi}\frac{d\phi}{2\pi}P_\phi\left(+,0\middle|+,0\right)=\frac{3}{4} \quad (26)$$

Cette modification ne change pas grand chose au fait que sur un grand nombre d'envois, l'espion va être démasqué à coup (presque) sûr.

2. Communication de la clé entre Alice et Bob :

Les exemples traités ci-dessus illustrent la possibilité de savoir si la ligne est écoutée ou non mais n'en définissent pas pour autant un mode de transmission sûr de la clé de cryptage : être en mesure d'affirmer avec certitude que la ligne n'est pas écoutée est déjà un immense progrès ; encore faut-il à un moment ou à un autre trouver les moyens d'échanger la clé elle-même. Ekert a proposé le scénario qui suit, exposé d'abord dans sa version simple, puis dans une version raffinée utilisant des paires de spin couplées *à la EPR*.

Dans sa version la plus simple, Alice envoie à Bob des spins polarisés. L'état de polarisation de chaque spin résulte d'une mesure faite par Alice et ayant produit un certain résultat $\pm\dfrac{\hbar}{2}$, noté simplement $\pm$ dans la suite. Celle-ci tire au hasard sa direction de mesure ;

pour simplifier, on suppose que cette direction est soit Ox (notée $\leftrightarrow$), soit Oz (notée $\updownarrow$). Donc, pour chaque spin, Alice

1. tire au hasard sa direction de mesure, Ox ou Oz
2. note son résultat, $+$ ou $-$
3. envoie le spin à Bob (sans commentaire !)

Une séquence possible est la suivante :

$$\begin{array}{cccccccccccccccccccc} \updownarrow & \updownarrow & \leftrightarrow & \updownarrow & \leftrightarrow & \leftrightarrow & \leftrightarrow & \updownarrow & \leftrightarrow & \leftrightarrow & \updownarrow & \updownarrow & \updownarrow & \leftrightarrow & \updownarrow & \leftrightarrow & \leftrightarrow & \updownarrow & \updownarrow & \leftrightarrow \\ + & - & - & - & + & + & - & + & - & - & + & + & - & + & + & - & + & - & - & + \end{array} \quad (27)$$

Pour chaque spin reçu, Bob fait une mesure du spin en tirant lui aussi au hasard sa direction d'observation (il se trompe donc dans un cas sur deux) :

• quand il choisit le même axe q'Alice, il trouve le même résultat qu'elle :

$$P\left(\text{Bob}, Oz, +\middle|\text{Alice}, Oz, +\right) = 1 \qquad P\left(\text{Bob}, Oz, -\middle|\text{Alice}, Oz, +\right) = 0 \quad (28)$$

$$P\left(\text{Bob}, Oz, +\middle|\text{Alice}, Oz, -\right) = 0 \qquad P\left(\text{Bob}, Oz, -\middle|\text{Alice}, Oz, -\right) = 1 \quad (29)$$

• quand Bob « se trompe » d'axe, il ne trouve (statistiquement) le même résultat qu'Alice que dans la moitié des cas (voir 21) :

$$P\left(\text{Bob}, Oz, +\middle|\text{Alice}, Oz, +\right) = \frac{1}{2} \qquad P\left(\text{Bob}, Oz, -\middle|\text{Alice}, Oz, +\right) = \frac{1}{2} \quad (30)$$

$$P\left(\text{Bob}, Oz, +\middle|\text{Alice}, Oz, -\right) = \frac{1}{2} \qquad P\left(\text{Bob}, Oz, -\middle|\text{Alice}, Oz, -\right) = \frac{1}{2} \quad (31)$$

et de même en permutant x et z. Compte tenu de la séquence d'Alice (27), un exemple de séquence pour Bob, *en l'absence d'espion*, est le suivant :

$$\begin{array}{cccccccccccccccccccc} \updownarrow & \leftrightarrow & \updownarrow & \updownarrow & \leftrightarrow & \leftrightarrow & \updownarrow & \leftrightarrow & \leftrightarrow & \updownarrow & \updownarrow & \leftrightarrow & \updownarrow & \leftrightarrow & \updownarrow & \updownarrow & \leftrightarrow & \updownarrow & \leftrightarrow & \updownarrow \\ + & + & - & - & + & + & + & + & - & - & + & - & - & + & + & - & + & - & - & + \end{array} \quad (32)$$

Toutes les mesures étant faites, Alice fait part publiquement (on entend par là que la communication ne nécessite aucune confidentialité) à Bob de tous ses *choix* d'axes, mais, pour l'instant, ne dit évidemment rien de ses *résultats* ; réciproquement, Bob lui communique ses axes. Ceci permet d'éliminer tous les cas où le hasard a fait que les axes n'étaient pas les mêmes pour Alice et Bob : (33)

$$\begin{array}{lcccccccccccccccccccc} \text{Alice} & \updownarrow & \updownarrow & \leftrightarrow & \updownarrow & \leftrightarrow & \leftrightarrow & \leftrightarrow & \updownarrow & \leftrightarrow & \leftrightarrow & \updownarrow & \updownarrow & \updownarrow & \leftrightarrow & \updownarrow & \leftrightarrow & \leftrightarrow & \updownarrow & \updownarrow & \leftrightarrow \\ \text{Bob} & \updownarrow & \leftrightarrow & \updownarrow & \updownarrow & \leftrightarrow & \leftrightarrow & \updownarrow & \leftrightarrow & \leftrightarrow & \updownarrow & \updownarrow & \leftrightarrow & \updownarrow & \leftrightarrow & \updownarrow & \updownarrow & \leftrightarrow & \updownarrow & \leftrightarrow & \updownarrow \\ \textbf{Retenus} & + & & - & + & + & & & - & & + & & - & + & + & & & + & - & & \end{array}$$

A ce stade (et toujours en l'absence d'espion), chacun sait que pour tous les *bits* retenus, il a dû trouver les mêmes résultats que l'autre (chacun sait ce qu'à trouvé l'autre sans y être allé voir et sans communication explicite !) , mais ne sait pas ce qu'il en est au juste (si c'est faux, un espion écoute !).

Pour le savoir, Alice communique maintenant à Bob *une partie* de ses résultats ; connaissant les choix d'axes et les résultats d'Alice pour un assez grand nombre de cas, un test statistique permet alors à Bob de savoir avec une faible probabilité d'erreur si la

communication a été écoutée ou non. Si la confidentialité est alors établie, la séquence des *autres* résultats constituent la clé codant une lettre convenue d'avance : *sans rien communiquer d'autre*, Alice et Bob savent qu'ils ont trouvé la même chose à chaque fois puisqu'ils ont utilisé les mêmes axes. Finalement, comme la clé est constituée sans l'échange de rien d'autre, aucun moyen n'existe d'altérer la confidentialité de celle-ci !

Une autre version consiste à utiliser une source de particules produisant des paires (a,b) de spins $\frac{1}{2}$ dans l'état singulet :

$$|0\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle\right) \quad (34)$$

développé sur les états propres de $\hat{S}_{z(a)}$ et $\hat{S}_{z(b)}$. Après séparation des particules, l'une allant vers Alice, l'autre vers Bob, les deux observateurs procèdent à des mesures de la composante du spin le long de *Ox* ou de *Oz* , directions toutes deux perpendiculaires à la direction de propagation des particules. Dans la suite on note $|\rightarrow\rangle$ et $|\leftarrow\rangle$ respectivement les états propres $\pm\frac{\hbar}{2}$ de $\hat{S}_x$. Compte tenu de :

$$\begin{cases} |\rightarrow\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle + |\downarrow\rangle\right) \\ |\leftarrow\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle - |\downarrow\rangle\right) \end{cases} \quad (35)$$

l'état singulet (34) s'écrit aussi :

$$|0\rangle = \frac{1}{\sqrt{2}}\left(|\leftarrow\rightarrow\rangle - |\rightarrow\leftarrow\rangle\right) \quad (36)$$

Soit d'abord la séquence où Alice et Bob mesurent le long de la même direction, $\hat{S}_z$ par exemple. La première, Alice effectue une mesure, de $\hat{S}_z$ par exemple ; si elle trouve $+\frac{\hbar}{2}$, l'état des deux particules après cette mesure est la projection de (34), soit $|\uparrow\downarrow\rangle$. Il en résulte que quand Bob va mesurer $\hat{S}_z$ par la suite, il trouvera $-\frac{\hbar}{2}$ avec certitude (la mesure permet ainsi d'obtenir instantanément des informations sur ce qui se passe ailleurs : c'est ici que réside le paradoxe EPR). Si Alice trouve $-\frac{\hbar}{2}$, Bob trouvera $+\frac{\hbar}{2}$: leurs résultats sont donc à coup sûr opposés. Il en va de même si ce sont des mesures de $\hat{S}_x$ qui sont effectuées : le même raisonnement vaut avec (36). En définitive, quand Alice et Bob mesurent la même composante, leurs résultats sont toujours « anticorrélés ». Physiquement et en résumé, sachant que l'état est singulet et qu'Alice a trouvé le spin dans un sens, Bob ne peut trouver que le spin opposé.

Si Alice mesure $\hat{S}_z$ et Bob $\hat{S}_x$, les choses vont autrement. Si Alice a trouvé $+\frac{\hbar}{2}$, l'état après cette mesure est $|\uparrow\downarrow\rangle$ et se décompose suivant :

$$\frac{1}{2}\left(|\rightarrow\rightarrow\rangle - |\rightarrow\leftarrow\rangle + |\leftarrow\rightarrow\rangle - |\leftarrow\leftarrow\rangle\right) \quad (37)$$

Bob trouvera donc pour $\hat{S}_x$ les deux valeurs $\pm\frac{\hbar}{2}$ avec équiprobabilité. Il en va de même si Alice trouve $-\frac{\hbar}{2}$.

Ainsi, dans tous les cas, chacun sait (*a priori* sans communication des résultats : c'est le miracle EPR) ce que l'autre a trouvé. Le même scénario que ci-dessus peut alors être repris (communication des axes et d'une partie des résultats pour tester la confidentialité de la ligne).

Remarque :

Il faut bien voir que l'espion éventuel ne peut pas extraire quoi que ce soit d'utile : dans la phase d'envoi, les spins ne véhiculent aucune information en eux-mêmes. En fait, l'information ne devient réalité qu'après la mise en œuvre du scénario décrit ci-dessus.

EXERCICE DE COMPREHENSION

Références bibliographiques :

- *"La mécanique quantique au secours des agents secrets"* La Recherche **22**, 790 (Juin 1991).
- « *Quantum Cryptography* » Scientific American **267**, 26, (Novembre 1992).

On rappelle que le but de la cryptographie est d'envoyer à un correspondant un message en minimisant les risques de voir ce message intercepté par un tiers. Ce problème montre comment la mécanique quantique peut fournir une procédure répondant à ce besoin. Plus précisément, on suppose ici qu'Alice (A) souhaite envoyer à Bob (B) une certaine information que l'on suppose codée en binaire :

$$+\,+\,-\,-\,-\,+\,+\,-\,+\cdots \qquad (1)$$

On notera n le nombre de bits de ce message. Alice ne veut transmettre ce message que si elle s'est préalablement assurée que la communication n'est pas écoutée par un « espion ».

Chaque fois que cela sera possible, on présentera les résultats sous forme de tableaux comme dans l'énoncé de la question **3.b.ii**.

1. On considère une particule de spin $\frac{1}{2}$. L'observable de spin est $\hat{\vec{S}} = \frac{\hbar}{2}\hat{\vec{\sigma}}$ où les $\vec{\sigma}$ sont les matrices de Pauli.

On note $|\sigma_z = +1\rangle$ et $|\sigma_z = -1\rangle$ les états propres de $\hat{S}_z$ avec les valeurs propres respectives $+\frac{\hbar}{2}$ et $-\frac{\hbar}{2}$.

On suppose que l'état de spin de la particule est $|\sigma_z = +1\rangle$. On effectue la mesure de la composante du spin suivant un axe u situé dans le plan xOz et défini par le vecteur unitaire

$$\vec{e}_u = \cos\theta\,\vec{e}_z + \sin\theta\,\vec{e}_x \qquad (2)$$

faisant un angle θ avec l'axe z.

On rappelle que l'observable associée à cette mesure est

$$\hat{\vec{S}}.\vec{e}_u = \frac{\hbar}{2}\left(\cos\theta\,\hat{\sigma}_z + \sin\theta\,\hat{\sigma}_x\right) \qquad (3)$$

1.a. Montrer que les résultats de mesure possibles sont $+\frac{\hbar}{2}$ et $-\frac{\hbar}{2}$.

1.b. Montrer que les états propres de l'observable (3) sont de la forme

$$|\sigma_u = +1\rangle = \cos\phi\,|\sigma_z = +1\rangle + \sin\phi\,|\sigma_z = -1\rangle$$
$$|\sigma_u = -1\rangle = -\sin\phi\,|\sigma_z = +1\rangle + \cos\phi\,|\sigma_z = -1\rangle$$

et exprimer ϕ en fonction de θ.

En déduire les probabilités $P_u^{\pm}$ de trouver $+\frac{\hbar}{2}$ et $-\frac{\hbar}{2}$ suivant u (si l'état mesuré est $|\sigma_z = +1\rangle$).

1.c. Quels sont les états de spin après une mesure ayant donné $+\frac{\hbar}{2}$ ou $-\frac{\hbar}{2}$?

2. Immédiatement après cette mesure, on mesure la composante du spin suivant l'axe z.

2.a. Donner les résultats possibles et leurs probabilités en fonction du résultat obtenu précédemment le long de u (observable (3)).

2.b. Montrer que la probabilité de retrouver la même valeur $S_z = +\frac{\hbar}{2}$ que dans l'état initial $|\sigma_z = +1\rangle$ est :

$$P_{++}(\theta) = \frac{1+\cos^2\theta}{2}$$

2.c. En supposant maintenant que l'état initial soit $|\sigma_z = -1\rangle$, quelle est, dans la même séquence de mesures, la probabilité $P_{--}(\theta)$ de retrouver $S_z = -\frac{\hbar}{2}$ dans la dernière mesure ?

3. On dispose d'une source S qui produit une paire (a,b) de particules de spins $\frac{1}{2}$, préparée dans l'état : $|\Psi\rangle = \Phi(\vec{r}_a,\vec{r}_b)|\Sigma\rangle$ où l'état de spin des 2 particules est

$$|\Sigma\rangle = \frac{1}{\sqrt{2}}\left(|\sigma^{\,a}_{\,z} = +1\rangle \otimes |\sigma^{\,b}_{\,z} = +1\rangle + |\sigma^{\,a}_{\,z} = -1\rangle \otimes |\sigma^{\,b}_{\,z} = -1\rangle\right) \quad (4)$$

c'est-à-dire que les variables spatiales et les variables de spin sont indépendantes. Dans tout le problème, on ne s'intéresse qu'aux mesures de spin. Dans l'expression (4), $|\sigma_u^a = \pm 1\rangle$ (en l'occurrence $u = z$) désignant les états propres de la composante le long de u du spin de la particule a, de même pour b.

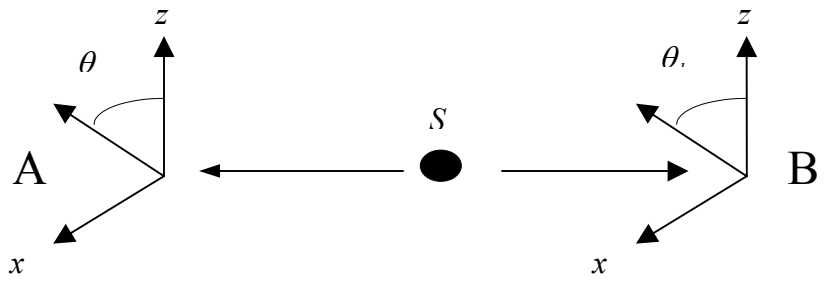


Figure 1. *Source S émettant une paire (a,b)de particules de spin $\frac{1}{2}$. Alice mesure la composante du spin a suivant un axe θ_a et Bob mesure la composante du spin b suivant un axe θ_b.*

3.a. Montrer que cet état peut également s'écrire :

$$|\Sigma\rangle = \frac{1}{\sqrt{2}}\left(|\sigma_x^a = +1\rangle \otimes |\sigma_x^b = +1\rangle + |\sigma_x^a = -1\rangle \otimes |\sigma_x^b = -1\rangle\right) \quad (5)$$

3.b. La paire de particules (a,b) étant préparée dans l'état de spin (4)-(5), ces particules sont séparées spatialement (figure 1) *sans que l'état de spin soit affecté* (avant qu'une mesure n'intervienne).

i. Alice mesure *d'abord* la composante du spin de a suivant un axe u_a d'angle θ_a.
Quels sont les résultats de mesure et les probabilités correspondantes dans les deux cas $\theta_a = 0 (z)$ et $\theta_a = \frac{\pi}{2}(x)$?

ii. *Le résultat de cette question est essentiel pour la suite, on pourra se contenter de l'admettre.*
Justifier qu'après cette mesure d'Alice l'état de spin des deux particules est :

Axe	Résultat	Etat
z	$+\frac{\hbar}{2}$	$\|\sigma_z^a = +1\rangle \otimes \|\sigma_z^b = +1\rangle$
z	$-\frac{\hbar}{2}$	$\|\sigma_z^a = -1\rangle \otimes \|\sigma_z^b = -1\rangle$
x	$+\frac{\hbar}{2}$	$\|\sigma_z^a = +1\rangle \otimes \|\sigma_z^b = +1\rangle$
x	$-\frac{\hbar}{2}$	$\|\sigma_z^a = -1\rangle \otimes \|\sigma_z^b = -1\rangle$

En déduire qu'on peut désormais ignorer la particule a pour ce qui concerne les mesures de spin sur b.

On rappelle que si $|\Psi\rangle = |u\rangle \otimes |v\rangle$ est un tenseur factorisable et $\hat{C} = \hat{A} \otimes \hat{B}$ où A et B agissent respectivement dans les espaces de $|u\rangle$ et de $|v\rangle$ alors

$$\langle \Psi | \hat{C} | \Psi \rangle = \langle u | \hat{A} | u \rangle . \langle v | \hat{B} | v \rangle$$

3.c. *Après* cette mesure d'Alice, Bob mesure la composante du spin de b suivant un axe u_b d'angle θ_b.
Déterminer les résultats de mesure possible de Bob et leurs probabilités, en fonction du résultat d'Alice, dans les quatre configurations suivantes :

i. $\theta_a = 0 \quad , \quad \theta_b = 0$

ii. $\theta_a = 0 \quad , \quad \theta_b = \frac{\pi}{2}$

iii. $\theta_a = \frac{\pi}{2} \quad , \quad \theta_b = 0$

iv. $\theta_a = \frac{\pi}{2} \quad , \quad \theta_b = \frac{\pi}{2}$

Dans quel(s) cas la mesure sur a et celle sur b donnent-elles le même résultat ? avec quelle probabilité ?

3.d. On se place dans la situation $\theta_a = 0$. On suppose qu'un « espion » situé entre la source S et Bob, fait une mesure de la composante du spin b suivant un axe u_c d'angle θ_c (figure 2). (On utilisera les résultats des questions **1.** et **2.**).

i. Quels sont, en fonction de θ_c et du résultat de la mesure d'Alice, les résultats de mesure de l'espion et leurs probabilités ?

ii. Après cette mesure de l'espion, Bob mesure le spin de b suivant l'axe défini par $\theta_b = 0$, que trouve-t-il, avec quelle probabilité, en fonction du résultat trouvé par l'espion ?

iii. Quelle est la probabilité $P(\theta_e)$ qu 'Alice et Bob trouvent le même résultat ?

iv. Quelle est la moyenne de $P(\theta_e)$ si l'espion choisit au hasard θ_e avec une probabilité uniforme sur $[0,2\pi]$? Quelle est cette même moyenne s'il choisit seulement les deux valeurs $\theta_e = 0$ et $\theta_e = \frac{\pi}{2}$ avec la même probabilité $p = \frac{1}{2}$ pour chacune ?

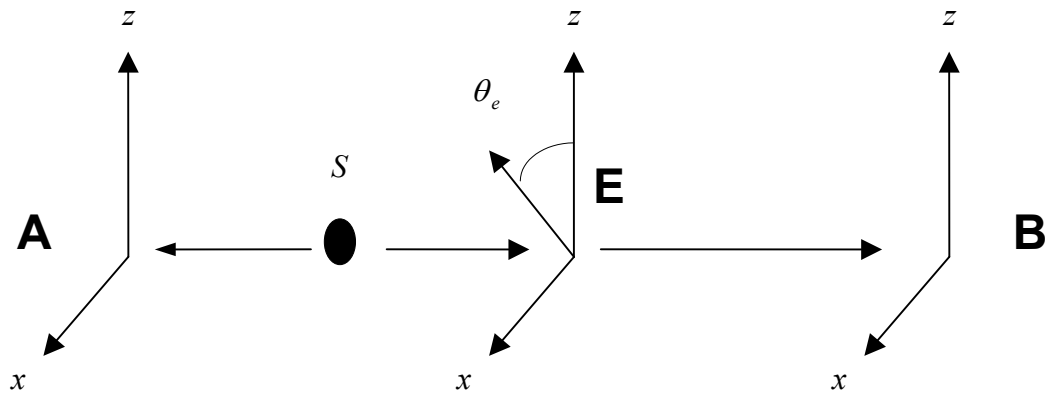


Figure 2. : *Un espion, situé entre la source S et Bob, fait une mesure d'une composante du spin b suivant un axe θ_e avant que Bob ne mesure la composante de ce spin suivant l'axe θ_b.*

4. On souhaite utiliser les résultats qui précèdent à la transmission confidentielle d'information. Alice et Bob utilisent alors la procédure détaillée dans l'encadré ci-dessous. Commenter cette procédure, en s'attachant plus particulièrement à répondre aux questions suivantes :

4.a. Comment Alice peut-elle se convaincre de la présence d'un espion ?

4.b. Quelle est la probabilité qu'un espion présent ne soit pas détecté ? Application numérique *FN*=200.

4.c. L'espion gagne-t-il en « invisibilité » s'il connaît le système d'axe *Oxz* retenu par Alice et Bob et déterminant les directions d'analyse (*étape 1)* ?

4.d. Discuter sur les deux « expériences » décrites ci-dessous l'existence d'un espion (*Tables et 2).* On montrera que la communication 2 a certainement été espionnée. On calculera la probabilité qu'un espion ait opéré sans être détecté dans la communication 1.

4.e. Compléter la phrase manquante *(n°7)* en indiquant comment Alice peut envoyer son message (1) à Bob, sans utiliser d'autres paires de spins que les N paires déjà produites et analysées par Bob et elle-même. En utilisant la table 3, indiquer comment dans l'expérience 1 ci-dessus, Alice peut transmettre à Bob le message $\{+,-\}$.

1. Alice et Bob décident d'un choix d'axes x et z qui leur serviront de directions d'analyse.

2. Alice, qui dispose de la source **S** prépare une séquence ordonnée de $N >> n$ paires de spins $\frac{1}{2}$ dans l'état (4) (n : nombre de bits du message). Elle envoie les spins b à Bob, et garde les spins a.

3. Alice et Bob font, pour chacun des spins dont ils disposent, la mesure de la composante x ou z. Le choix entre x et z se fait de manière aléatoire et équiprobable pour chaque spin, et il n'y a pas de corrélation pour un spin donné, entre la composante choisie par Alice et celle choisie par Bob. Ils stockent chacun l'ensemble de leur résultats.

4. Bob sélectionne une partie ***FN*** de ses mesures et il communique publiquement à Alice (par radio, ...) la direction d'analyse choisie et le résultat obtenu pour chacune des mesures de cet ensemble. En pratique, $F \approx 0{,}5$.

5. Alice compare pour cet ensemble ***FN*** ses directions et ses résultats avec ceux que vient de lui communiquer Bob. Elle peut alors détecter la présence éventuelle d'un espion. Si un espion est repéré, la procédure s'arrête et une recherche « physique » de l'espion doit avoir lieu. Sinon

6. Alice annonce publiquement qu'elle est convaincue de ne pas avoir été écoutée et Bob lui transmet, toujours publiquement, ses directions d'analyse pour les $(1-F)N$ spins restants. En revanche, il ne communique pas ses résultats correspondants.

?.....

Spin n°	1	2	3	4	5	6	7	8	9	10	11	12
Axe d'analyse	X	X	Z	X	Z	Z	X	Z	Z	Z	X	X
Résultat	+	-	+	+	-	-	+	+	+	-	+	-

Spin n°	1		3	4			7			10	11	
Axe d'analyse	X		X	Z			X			X	X	
Résultat	+		-	-			+			+	+	

Table 1. : Expérience **1** réalisée avec $N = 12$ paires de spins. (a) Ensemble des choix d'axes et des résultats obtenus par Alice. (b) Choix d'axes et résultats communiqués publiquement par Bob (*Etape 4*).

Spin n°	1	2	3	4	5	6	7	8	9	10	11	12
Axe d'analyse	X	Z	Z	Z	X	X	Z	X	X	Z	X	Z
Résultat	+	+	-	+	+	-	+	+	-	-	+	+
Spin n°		2			5			8	9		11	12
Axe d'analyse		X			X			X	Z		Z	Z
Résultat		+			+			-	+		+	-

Table 2. : Expérience **1** réalisée avec $N = 12$ paires de spins. (a) Ensemble des choix d'axes et des résultats obtenus par Alice. (b) Choix d'axes et résultats communiqués publiquement par Bob (*Etape 4*).

Spin n°	2	5	6	8	9	12
Axe d'analyse	X	X	X	Z	X	X

Table 3. : Choix d'axes communiqués publiquement par Bob dans le cadre de l'expérience 1, après qu'Alice se soit déclarée confiante de ne pas avoir été écoutée (*Etape 6*).

Corrigé

1.

$$\hat{S}_u = \frac{\hbar}{2}\hat{\sigma}_u = \hat{\vec{S}}.\vec{e}_u = \frac{\hbar}{2}\left(\hat{\sigma}_z\cos\theta + \hat{\sigma}_x\sin\theta\right) = \frac{\hbar}{2}\left[\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\cos\theta + \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\sin\theta\right] = \frac{\hbar}{2}\underbrace{\begin{pmatrix}\cos\theta & \sin\theta\\ \sin\theta & -\cos\theta\end{pmatrix}}_{\hat{\sigma}_u}$$

1.a. Valeurs propres : $\pm\frac{\hbar}{2}$

1.b. Vecteurs propres : ceux de $\hat{\sigma}_u$ soit : $\begin{cases}\left|\sigma_u = +1\right\rangle = \cos\frac{\theta}{2}\left|\sigma_z = +1\right\rangle + \sin\frac{\theta}{2}\left|\sigma_z = -1\right\rangle\\ \left|\sigma_u = -1\right\rangle = -\sin\frac{\theta}{2}\left|\sigma_z = +1\right\rangle + \cos\frac{\theta}{2}\left|\sigma_z = -1\right\rangle\end{cases}$

$$\Rightarrow \phi = \frac{\theta}{2} \text{ et } P_u^{\pm} = \left|\left\langle\sigma_u = \pm 1\middle|\sigma_z = +1\right\rangle\right|^2 \Rightarrow \begin{cases}P_u^{+1} = \cos^2\frac{\theta}{2} = \cos^2\phi\\ P_u^{-1} = \sin^2\frac{\theta}{2} = \sin^2\phi\end{cases}$$

1.c. D'après le principe de réduction du paquet d'ondes :
si la mesure a donné $+\frac{\hbar}{2}$ l'état de spin est $\left|\sigma_u = +1\right\rangle$, de même : $-\frac{\hbar}{2} \to \left|\sigma_u = -1\right\rangle$.

2.a.

- *Mesure suivant u :* $+\frac{\hbar}{2}$

$$P_z\left(\pm\frac{\hbar}{2}\right) = \left|\left\langle\sigma_z = \pm 1\middle|\sigma_u = +1\right\rangle\right|^2 \Rightarrow \begin{cases}P_z^{+}\left(+\frac{\hbar}{2}\right) = \cos^2\frac{\theta}{2}\\ P_z^{+}\left(-\frac{\hbar}{2}\right) = \sin^2\frac{\theta}{2}\end{cases}$$

- *Mesure suivant u :* $-\frac{\hbar}{2}$

$$P_z\left(\pm\frac{\hbar}{2}\right) = \left|\left\langle\sigma_z = \pm 1\middle|\sigma_u = -1\right\rangle\right|^2 \Rightarrow \begin{cases}P_z^{-}\left(+\frac{\hbar}{2}\right) = \sin^2\frac{\theta}{2}\\ P_z^{-}\left(-\frac{\hbar}{2}\right) = \cos^2\frac{\theta}{2}\end{cases}$$

2.b. On retrouve $S_z = +\frac{\hbar}{2}$ avec la probabilité :

$P_u^{+}P_z^{+}\left(+\frac{\hbar}{2}\right) = \cos^4\frac{\theta}{2}$ si la mesure sur u donne $+\frac{\hbar}{2}$ et

$P_u^{-}P_z^{-}\left(+\frac{\hbar}{2}\right) = \sin^4\frac{\theta}{2}$ si la mesure sur u donne $-\frac{\hbar}{2}$

soit : $P_{++} = \cos^4\frac{\theta}{2} + \sin^4\frac{\theta}{2} = \frac{1+\cos^2\theta}{2}$

2.c. Les résultats intermédiaires sont inversés, mais la probabilité est la même :

$$P_{--} == \frac{1+\cos^2\theta}{2}$$

3.a. On a :

$\left|\sigma_x = \pm 1\right\rangle = \frac{1}{\sqrt{2}}\left[\left|\sigma_z = +1\right\rangle \pm \left|\sigma_z = -1\right\rangle\right]$ et par conséquent en remplaçant dans (5)

$$|\Sigma\rangle = \frac{1}{2\sqrt{2}}\left[\left(\left|\sigma_z^a = +1\right\rangle + \left|\sigma_z^a = -1\right\rangle\right)\otimes\left(\left|\sigma_z^b = +1\right\rangle + \left|\sigma_z^b = -1\right\rangle\right) + \left(\left|\sigma_z^a = +1\right\rangle - \left|\sigma_z^a = -1\right\rangle\right)\otimes\left(\left|\sigma_z^b = +1\right\rangle - \left|\sigma_z^b = -1\right\rangle\right)\right]$$

(Les termes croisés s'éliminent).

3.b. i. Alice trouve $\pm\frac{\hbar}{2}$ avec $P = \frac{1}{2}$ dans chaque cas. Cela peut soit paraître évident, soit s'obtenir en notant que le projecteur sur l'état propre $\left|\sigma_z^a = 1\right\rangle$ étendu à l'espace produit tensoriel est $\hat{P}_+^a = \left|\sigma_z^a = +\right\rangle\left\langle\sigma_z^a = 1\right| \otimes \hat{I}^b$ et que $P\left(+\frac{\hbar}{2}\right) = \left\langle\Sigma\left|\hat{P}_+^a\right|\Sigma\right\rangle = \frac{1}{2}$ (de même pour $P\left(-\frac{\hbar}{2}\right)$

ii. Réduction du paquet d'ondes.

Axe z : on part de la formule (4), les projections normalisées sur les états propres de $\hat{S}_z^a$ sont

$$\left|\sigma_z^a = 1\right\rangle \otimes \left|\sigma_z^b = 1\right\rangle \text{ et } \left|\sigma_z^a = -1\right\rangle \otimes \left|\sigma_z^b = -1\right\rangle$$

de même pour une mesure le long de x.

Tout résultat de mesure sur b (probabilité, valeur moyenne) fera intervenir des valeurs moyennes d'opérateurs du type $\hat{I}^a \otimes \hat{B}^b$ où B est un projecteur, un opérateur de spin etc...

Puisque les états considérés sont factorisés, les expressions correspondantes pour les mesures de spin sur b seront de la forme

$$\begin{aligned}&\left(\left\langle\sigma_z^a = 1\right| \otimes \left\langle\sigma_z^b = 1\right|\right)\hat{I}^a \otimes \hat{B}^b\left(\left|\sigma_z^a = 1\right\rangle \otimes \left|\sigma_z^b = 1\right\rangle\right)\\ &= \left\langle\sigma_z^a = 1\middle|\sigma_z^a = 1\right\rangle.\left\langle\sigma_z^b = 1\middle|\hat{B}\middle|\sigma_z^b = 1\right\rangle\\ &= \left\langle\sigma_z^b = 1\middle|\hat{B}\middle|\sigma_z^b = 1\right\rangle\end{aligned}$$

où l'état a n'intervient pas.

3.c.

	Alice	**Bob**
(i.) $\theta_a = 0 \quad \theta_b = 0$	$+\frac{\hbar}{2}$ $-\frac{\hbar}{2}$	$+\frac{\hbar}{2} \quad p = 1$ $-\frac{\hbar}{2} \quad p = 1$
(ii.) $\theta_a = 0 \quad \theta_b = \frac{\pi}{2}$	$+\frac{\hbar}{2}$ $-\frac{\hbar}{2}$	$\pm\frac{\hbar}{2} \quad p = \frac{1}{2}$ à chaque fois $\pm\frac{\hbar}{2}$ " "
(iii.) $\theta_a = \frac{\pi}{2} \quad \theta_b = 0$	identique à **(ii.)**	
(iv.) $\theta_a = \frac{\pi}{2} \quad \theta_b = \frac{\pi}{2}$	identique à **(i.)**	

Dans les cas **(i.)** et **(iv.)** Alice et Bob trouvent à coup sûr le même résultat.

3.d.

i.

Alice	Espion	Probabilité
$+\frac{\hbar}{2}$	$+\frac{\hbar}{2}$	$\cos^2\frac{\theta_e}{2}$
	$-\frac{\hbar}{2}$	$\sin^2\frac{\theta_e}{2}$
$-\frac{\hbar}{2}$	$+\frac{\hbar}{2}$	$\sin^2\frac{\theta_e}{2}$
	$-\frac{\hbar}{2}$	$\cos^2\frac{\theta_e}{2}$

ii.

Espion	Bob	Probabilité
$+\frac{\hbar}{2}$	$+\frac{\hbar}{2}$	$\cos^2\frac{\theta_e}{2}$
	$-\frac{\hbar}{2}$	$\sin^2\frac{\theta_e}{2}$
$-\frac{\hbar}{2}$	$+\frac{\hbar}{2}$	$\sin^2\frac{\theta_e}{2}$
	$-\frac{\hbar}{2}$	$\cos^2\frac{\theta_e}{2}$

iii. $P_{++} = P_{--} = \cos^4\frac{\theta_e}{4} + \sin^4\frac{\theta_e}{4} = \frac{1\cos^2\theta_e}{2}$

iv. $\frac{1}{2\pi}\int_0^{2\pi} P(\theta_e)d\theta_e = \frac{3}{4}$

$P(0)=1$, $P\left(\frac{\pi}{2}\right)=\frac{1}{2}$, soit en moyenne $\overline{p}=\frac{3}{4}$ si les deux valeurs $\theta_e = 0$ et $\theta_e = \frac{\pi}{2}$ sont équiprobables.

4.a. Nécessairement si $\theta_a = \theta_b$, les résultats d'Alice et Bob doivent être les mêmes. Si *une seule* mesure avec $\theta_a = \theta_b$ est différente, la présence d'un espion est certaine. Si $\theta_a \neq \theta_b$, en moyenne la moitié des résultats sont les mêmes, la moitié sont opposés.

4.b. Pour que l'espion ait la chance de rester invisible, il faut que Bob et Alice aient enregistré les mêmes résultats de mesure chaque fois qu'ils ont choisi la même direction de mesure. Sur les 8 cas possibles dans un événement, un seul est défavorable.

La probabilité : $\left(\frac{7}{8}\right)^{FN}$ est très faible si *FN* est grand. Pour $FN = 200$ on a $\left(\frac{7}{8}\right)^{200} \approx 2{,}5\times10^{-12}$.

4.c. Etonnamment (voir le résultat **3.d.iv.**) l'espion ne « gagne » rien à tenter de connaître le système d'axe (Oxz) choisi par Alice et Bob.

4.d. Table 2 : Les mesures 8 et 12 où les axes sont les mêmes donnent des résultats opposés : cherchez l'espion !

Table 1 : au contraire les mesures 1,7,11 (axe x) donnent bien les mêmes valeurs et sont compatibles avec l'absence d'espionnage. Toutefois le nombre N utilisé est bien faible, la probabilité qu'un espion ait opéré mais soit passé inaperçu est $\left(\frac{3}{4}\right)^3 \approx 40\%$.

4.e. Alice sélectionne parmi les $(1-F)N$ mesures restantes une suite où les axes sont les mêmes et où la suite des résultats de mesure correspond à son message. Elle communique en clair à Bob les numéros de ces mesures, Bob lit sur ses données le message en question.
Dans le cas présent, Alice communique en clair les n° 8 et 12 sur lesquels Bob lit $+-$.

Commentaire :

Ce procédé (utilisant des paires de photons corrélés en polarisation et non des spins $\frac{1}{2}$) est actuellement en cours de réalisation dans des laboratoires de recherche (par exemple chez IBM).