Physique quantique

La cryptographie quantique

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 :

$$++--++-+$$

au moyen des états de spin d'une particule de spin $\frac{1}{2}$. 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 ».

On note $\mathcal{B}_i = \{|i+\rangle, |i-\rangle\}$ les états propres de S_i (observable de spin selon l'axe i avec $i = x, y, z$), de valeur propre respective $\pm\hbar/2$. On note $\vec{S} = (S_x, S_y, S_z)$ l'observable complète de spin selon les 3 axes.

1 Préambule

On suppose la particule initialement dans l'état $|z+\rangle$. On effectue la mesure de la composante du spin selon l'axe $\vec{u} = cos\theta\vec{e}_x + sin\theta\vec{e}_z$. On rappelle que l'observable associée est

$$S_u = cos\ \theta \cdot S_x + sin\ \theta \cdot S_z$$

Q1. Montrer que les résultats possibles sont $\pm\hbar/2$. Exprimer les états propres de S_u en fonction de θ dans la base $\mathcal{B}_z$.

Q2. En déduire les probabilités $p_u^{\pm}$ de trouver $\pm\hbar/2$ suivant $\vec{u}$, la particule étant toujours dans l'état $|z+\rangle$.

Q3. Quels sont, d'après le postulat de *réduction du paquet d'onde*, les états de spin de la particule après une mesure ayant donné $+\hbar/2$ (resp. $-\hbar/2$) ?

Immédiatement après cette mesure selon $\vec{u}$, on mesure la composante du spin suivant l'axe z.

Q4. Donner les résultats possibles et leur probabilité en fonction du résultat obtenu précédemment suivant l'axe $\vec{u}$.

Q5. Déterminer (en fonction de θ) la probabilité de retrouver la même valeur $S_z = +\hbar/2$ que dans l'état initial $|z+\rangle$.

Q6. Reprendre les questions précédentes en supposant que la particule est initialement dans l'état $|z-\rangle$ (on se contentera d'une brève justification).

2 Système de deux particules de spin $\frac{1}{2}$

Pour mettre en place la liaison « sécurisée », on dispose d'une source S (en pratique commandée par Alice) qui produit une paire **corrélée** (a, b) de particules de spin $\frac{1}{2}$, dans l'état $|\psi\rangle = \varphi(\vec{r}_a, \vec{r}_b)\,|\Sigma\rangle$ (c'est-à-dire que les variables spatiales et les variables de spin sont indépendantes) où l'état de spin du **système à deux particules** est :

$$|\Sigma\rangle = \frac{1}{\sqrt{2}}\left(|z_a+\rangle \otimes |z_b+\rangle + |z_a-\rangle \otimes |z_b-\rangle\right)$$

et où $|\Sigma\rangle \in \mathcal{E}_s^a \otimes \mathcal{E}_s^b$, espace construit par produit (tensoriel) des espaces d'état (réduits au spin) des particules a et b . Dans toute la suite, on ne s'intéresse qu'aux mesures de spin.

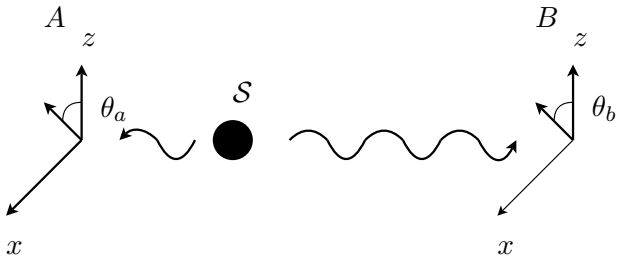

FIG. 1 – Source S émettant une paire corrélée (a, b) de particules de spin $\frac{1}{2}$. Alice mesure la composante du spin de a suivant un axe θ_a et Bob mesure la composante du spin de b suivant un axe θ_b.

Q7. Montrer que cet état peut également s'écrire (on utilisera la décomposition de $|z\pm\rangle$ sur la base $\mathcal{B}_x$) :

$$|\Sigma\rangle = \frac{1}{\sqrt{2}}\left(|x_a+\rangle \otimes |x_b+\rangle + |x_a-\rangle \otimes |x_b-\rangle\right)$$

La paire de particules (a, b) étant préparée dans l'état précédent, ces particules sont séparées spatialement (figure 1) **sans que l'état de spin ne soit affecté** lors du « transport » jusqu'à l'analyseur de polarisation.

Q8. Alice mesure **d'abord** la composante du spin de a suivant un axe $\vec{u}_a$ d'angle θ_a. Quels sont les *résultats de mesure*, les *probabilités* correspondantes et les *états du système immédiatement après la mesure* dans les deux cas : $\theta_a = 0$ (axe z), $\theta_a = \pi/2$ (axe x).

Q9. Montrer qu'on peut désormais ignorer l'état de la particule a pour ce qui concerne les mesures ultérieures de spin sur b (on pourra par exemple étudier l'influence de l'état de a sur la valeur moyenne du spin de b).

Après cette mesure d'Alice, Bob mesure la composante du spin de b selon un axe $\vec{u}_b$ d'angle θ_b.

Q10. Déterminer les résultats de mesure possible de Bob et leur probabilité, en fonction du résultat d'Alice, dans les quatre configurations suivantes :
- $\theta_a = 0,\ \theta_b = 0$
- $\theta_a = 0,\ \theta_b = \pi/2$
- $\theta_a = \pi/2,\ \theta_b = 0$

– $\theta_a = \pi/2,\ \theta_b = \pi/2$
Dans quel(s) cas la mesure sur a et celle sur b donnent-elles le même résultat ? Avec quelle probabilité ?

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 $\vec{u}_e$ d'angle θ_e (figure 2).

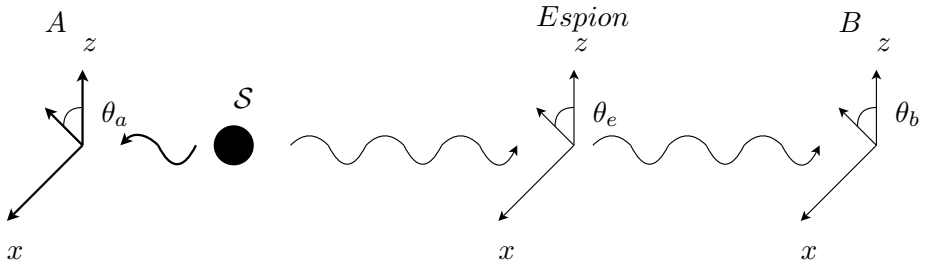

FIG. 2 – Un espion, situé entre la source S et Bob, fait une mesure d'une composante du spin b suivant un axe θ_e avant que Bob ne mesure la composante de ce spin suivant l'axe θ_b.

Q11. Quels sont, en fonction de θ_e et du résultat de mesure d'Alice, les résultats de mesure de l'espion et leurs probabilités ?

Q12. 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 ?

Q13. Quelle est la probabilité $\mathcal{P}(\theta_e)$ qu'Alice et Bob trouvent le même résultat ?

Q14. Quelle est la moyenne de $\mathcal{P}(\theta_e)$ 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 $\theta_e = \pi/2$ avec la même probabilité $p = 1/2$ pour chacune ?

3 Transmission confidentielle d'information

On souhaite utiliser les résultats précédents à la transmission confidentielle d'information. Alice et Bob utilisent alors la procédure détaillée ci-après :

1. Alice et Bob décident d'un choix d'axes x et z qui leur serviront de direction d'analyse.
2. Alice, qui dispose de la source S, prépare une séquence ordonnée de $N \gg n$ paires de particules. Elle envoie les particules b à Bob et « garde » les particules a.
3. Alice et Bob font, pour chacune des particules dont ils disposent, la mesure de la composante x ou z du spin. Le choix entre x et z se fait de manière aléatoire et équiprobable pour chaque particule, et il n'y a pas de corrélation, pour une particule donnée, entre la composante choisie par Alice et celle choisie par Bob. Ils stockent chacun l'ensemble de leurs résultats.

4. Bob sélectionne une partie FN de ses mesures et il communique publiquement à Alice (par ICQ, portable, signaux de fumée...) la direction d'analyse choisie et le résultat obtenu pour chacune des mesures de cet ensemble. En pratique, $F \sim 0,5$.
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 $(1-F)N$ mesures restantes. En revanche, il ne communique pas ses résultats correspondants.
7. ...

Commenter cette procédure, en s'attachant plus particulièrement à répondre aux questions suivantes :

Q15. Comment Alice peut-elle se convaincre de la présence d'un espion ?

Q16. Quelle est la probabilité qu'un espion ne soit pas détecté ? Application numérique : $FN = 200$.

Q17. L'espion gagne-t-il en invisibilité s'il connaît le système d'axe Oxz retenu par Alice et Bob ?

Q18. Discuter sur les deux « expériences » décrites ci-dessous l'existence d'un espion (tables 1 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.

Q19. Compléter la phrase manquante (numéro 7) en indiquant comment Alice peut envoyer son message 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, Alice peut transmettre à Bob le message $\{+,-\}$.

Expérience 1 réalisée avec $N = 12$ paires de particules :
Résultats obtenus par Alice :

Particule numéro	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	$+$	$-$	$+$	$+$	$-$	$-$	$+$	$+$	$+$	$-$	$+$	$-$

Résultats obtenus et communiqués publiquement par Bob à Alice (étape 4) :

Particule numéro	1		3	4			7			10	11	
Axe d'analyse	x		x	z			x			x	x	
Résultat	$+$		$-$	$-$			$+$			$+$	$+$	

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) :

Particule numéro	2	5	6	8	9	12
Axe d'analyse	x	x	x	z	x	x

Expérience 2 réalisée avec $N = 12$ paires de particules :
Résultats obtenus par Alice :

Particule numéro	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	$+$	$+$	$-$	$+$	$+$	$-$	$+$	$+$	$-$	$-$	$+$	$+$

Résultats obtenus et communiqués publiquement par Bob à Alice (étape 4) :

Particule numéro		2			5			8	9		11	12
Axe d'analyse		x			x			x	z		z	z
Résultat		$+$			$+$			$-$	$+$		$+$	$-$

4 Annexe : résultats importants sur l'état quantique d'un système de particules

Soit un **système** constitué de deux particules 1 et 2, de vecteur d'état $|\varphi(1)\rangle \in \mathcal{E}_1$ et $|\varphi(2)\rangle \in \mathcal{E}_2$. L'état quantique **du système** est décrit dans l'espace *produit tensoriel* $\mathcal{E}_{12} = \mathcal{E}_1 \otimes \mathcal{E}_2$. On note

$$|\psi\rangle = |\varphi(1)\rangle \otimes |\varphi(2)\rangle \in \mathcal{E}_1 \otimes \mathcal{E}_2$$

un état du système.

Base orthonormée de l'espace produit : soient $|\varphi(1)\rangle = \sum_i a_i |u_i(1)\rangle$ et $|\varphi(2)\rangle = \sum_j b_j |v_j(2)\rangle$ les décompositions des vecteurs d'état de chaque particule sur une base orthonormée de leur espace d'état. Alors, par définition, on a la décomposition suivante du vecteur d'état **du système complet** :

$$|\varphi(1)\rangle \otimes |\varphi(2)\rangle = \sum_{i,j} a_i b_j |u_i(1)\rangle \otimes |v_j(2)\rangle$$

La famille $\{|u_i(1)\rangle \otimes |v_j(2)\rangle\}$ constitue une base orthonormée de l'espace produit.

Produit scalaire : le produit scalaire de deux vecteurs $|\varphi(1)\rangle \otimes |\varphi(2)\rangle$ et $|\varphi'(1)\rangle \otimes |\varphi'(2)\rangle$ de $\mathcal{E}_1 \otimes \mathcal{E}_2$ est par définition le scalaire :

$$\left(\langle\varphi'(1)| \otimes \langle\varphi'(2)|\right) | \left(|\varphi(1)\rangle \otimes |\varphi(2)\rangle\right) = \langle\varphi'(1)|\,\varphi(1)\rangle\,\langle\varphi'(2)|\,\varphi(2)\rangle$$

Produit d'opérateurs/d'observables : Soit $A(1)$ opérant dans $\mathcal{E}_1$ et $B(2)$ opérant dans $\mathcal{E}_2$. Alors, par définition, l'opérateur noté $A(1) \otimes B(2)$ agit dans $\mathcal{E}_1 \otimes \mathcal{E}_2$ de la manière suivante :

$$(A(1) \otimes B(2))(|\varphi(1)\rangle \otimes |\varphi(2)\rangle) = A(1)\,|\varphi(1)\rangle \otimes B(2)\,|\varphi(2)\rangle$$

En particulier, on appelle **extension de A(1) à l'espace produit** l'opérateur $\tilde{A} = A(1) \otimes \mathbf{1}(2)$.

Représentation matricielle d'un produit d'opérateurs : soit $A(1)_{ij}$ (resp. $B(2)_{kl}$) les éléments de matrice de l'opérateur $A(1)$ (resp. $B(2)$) dans une base orthonormée de $\mathcal{E}_1$ (resp. $\mathcal{E}_2$). Alors la matrice représentant l'opérateur $A(1) \otimes B(2)$ dans la base orthonormée de $\mathcal{E}_1 \otimes \mathcal{E}_2$ construite par produit tensoriel des bases de $\mathcal{E}_1$ et $\mathcal{E}_2$ est le tenseur de rang 4 : $(A(1) \otimes B(2))_{ijkl} = A(1)_{ij} B(2)_{kl}$. Ceci résulte des deux définitions précédentes (produit scalaire, produit d'opérateurs).

Application des postulats au système constitué de deux particules : il suffit de construire les observables du système complet par produit tensoriel des observables de chacune des particules (en fonction de ce que l'expérience mesure effectivement, bien sûr...). Ensuite, les valeurs et vecteurs propres de ces observables permettent de déterminer les résultats possibles d'une mesure, les probabilités correspondantes...

Dans le cas (cf. TD) où la mesure ne porte que sur **une seule des deux particules**, l'observable correspondante est simplement **l'extension de l'observable** associée à la particule « mesurée » **à l'espace produit**.

Enfin, ces résultats se généralisent bien entendu au cas d'un système constitué de plus de deux particules.