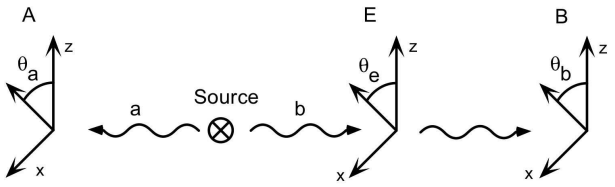
A. Introduction à la cryptographie quantique. La cryptographie quantique est une tentative de mise en oeuvre des prédicats de la mécanique quantique afin d'assurer la confidentialité, l'intégrité et la non-interception de transmissions de données. Les fondements de la cryptographie quantique ont été établis, entre autres, par les travaux de 1984 de Charles H. Bennett et Gilles Brassard. Les premières idées ont été posées par Stephen Wiesner dans les années 1960.

Dans cet exemple simplifié, on suppose que Alice (A) veut transmettre un message à Bob (B) en envoyant des particules de spin 1/2. La mesure par Bob de la composante du spin selon $\hat{z}$ donne nécessairement $\pm\hbar/2$, analogue à un bit d'information 0 ou 1. Nous allons montrer qu'un espion (E) ne peut pas lire le message **sans être détecté** en vertu du principe quantique qu'une mesure modifie le système sur lequel elle s'exerce (principe de réduction du paquet d'onde, cours page 117 et 123).



1) **Etat intriqué de deux spins.** Alice dispose d'une source S qui produit une paire (a,b) de particules de spin 1/2, préparée dans l'état de spin: $|\Sigma>$ ci-dessous. Ces particules sont séparées spatialement (voir figure ci-dessus).

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

Alice mesure d'abord la composante de spin de a suivant l'axe $\hat{z}$. Quels sont les résultats de la mesure, les probabilités correspondantes et l'état de la paire (a,b) après cette mesure en fonction des résultats obtenus ?

2) Après la mesure d'Alice, Bob mesure la composante du spin de b suivant l'axe $\hat{z}$. Déterminer les résultats de mesures possibles de Bob et leurs probabilités, en fonction du résultat d'Alice.

3) **Détection d'un espion.** On suppose qu'un "espion" situé entre la source S et Bob, mesure la composante du spin b suivant un axe u_e d'angle θ_e (l'espion ne connaît pas l'axe de mesure choisi par Alice et Bob).

- a) En fonction des résultats d'Alice, quels sont les résultats de mesure de l'espion et leurs probabilités ?
- b) Après cette mesure par l'espion, Bob mesure le spin de b suivant $\hat{z}$. Que trouve-t-il, avec quelle probabilité, en fonction du résultat trouvé par l'espion ?
- c) Quelle est la probabilité $P(\theta_e)$ qu'Alice et Bob trouvent le même résultat ?

On rappelera l'expression des états propres $|\sigma_u=\pm>$ de l'opérateur associé à la mesure de la composante de spin selon l'axe u_e en fonction des états propres $|\sigma_z=\pm>$.

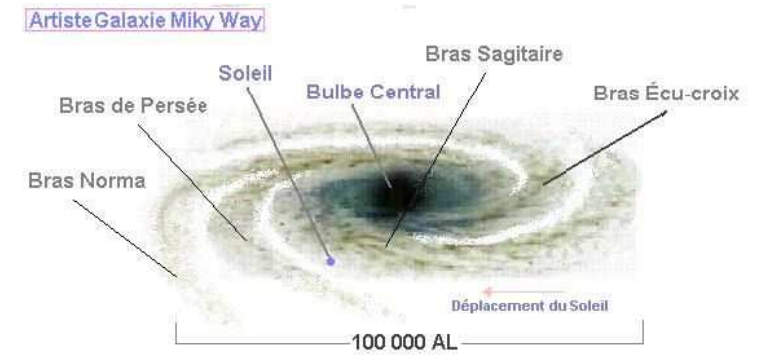
4) Alice envoie de façon séquentielle N particules b à Bob. Bob "sacrifie" αN mesures ($\alpha\sim 0.5$) en annonçant publiquement les résultats de ses mesures pour ces αN particules reçues. Quelle est la probabilité pour qu'un espion ne soit pas détecté (on prendre αN=100) ? On admettra que: $\int_0^{2\pi}[cos^4(\theta/2)+sin^4(\theta/2)]d\theta/2\pi=3/4$.

Si aucun espion n'est détecté, Alice peut dire publiquement à Bob quelles particules considérer pour reconstruire un message à partir des résultats $(++-+--++\ ...)$ des mesures de Bob pour ces particules reçues. Pour éviter le cas accidentel où l'espion aligne son polariseur selon l'axe $\vec{z}$, Alice et Bob en pratique vont choisir de façon aléatoire les axes $\vec{z}$ ou $\vec{x}$. La même analyse peut être conduite en montrant que $|\Sigma>$ peut aussi s'écrire:

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

B. Raie à 21 cm de l'atome d'hydrogène. De 5 à 10% de la masse totale de notre Galaxie se présente sous forme d'hydrogène atomique présent dans le milieu interstellaire. Dans ce milieu très dilué, les collisions sont trop peu nombreuses et la température effective trop faible pour permettre aux électrons d'être excité de l'état fondamental $E_n = -1Ry/n^2$ (n=1) aux états excités ($n \geq 2$) si bien qu'on ne peut pas détecter les raies Balmer, Lyman, etc. vues dans les PC précédentes.

En revanche, l'interaction $\hat{W}_{e-p}$ de type dipole-dipole entre les moments magnétiques de spin de l'électron et du proton conduit à une levée de dégénérescence du fondamental. Les niveaux crées sont très proches en énergie permettant la promotion d'électrons à faible température et l'émission de photons par relaxation. Cette "raie d'émission à 21 cm", prédite en 1914, fut détectée en 1951 et permit de définir la structure spirale de notre Galaxie.



La position du Soleil dans notre galaxie, La Voie Lactée.

1) Nous avons étudié en cours la structure des états propres $< \mathbf{r}|nlm >= R_{nl}(r)Y_{lm}(\theta,\phi)$ de l'hydrogène. Nous ajoutons aujourd'hui les degrés de liberté "internes" de spin de l'électron et du proton. En l'absence d'interaction $\hat{W}$, quelle est la dégénérescence de l'état fondamental $\mathcal{E}_0$?

2) Dans l'espace des spins $\mathbf{S}_p$ et $\mathbf{S}_e$ du proton et de l'électron, l'interaction dipole-dipole s'écrit:

$$\hat{W} = A\hat{\mathbf{S}}_e \cdot \hat{\mathbf{S}}_p/\hbar^2, \quad \text{avec} \quad A = 5,87.10^{-6} \text{ eV, soit:} \quad \lambda = hc/A = 21 \text{ cm}^{-1}$$

Diagonaliser $\hat{W}$ dans le sous espace $\mathcal{E}_0$ pour obtenir les corrections à l'énergie du fondamental. On utilisera:

$$\hat{\mathbf{S}}_e \cdot \hat{\mathbf{S}}_p = \hat{S}_{ez}\hat{S}_{pz} + \hat{S}_{ex}\hat{S}_{px} + \hat{S}_{ey}\hat{S}_{py} = \hat{S}_{ez}\hat{S}_{pz} + \frac{1}{2}(\hat{S}_{e+}\hat{S}_{p-} + \hat{S}_{e-}\hat{S}_{p+})$$

où nous avons introduit les opérateurs: $\hat{S}_\pm = \hat{S}_x \pm i\hat{S}_y$ agissant comme suit sur les états de spin $|\pm>$ (cours page 208): $S_+|+>= 0$, $S_+|->= \hbar|+>$, $S_-|->= 0$, $S_-|+>= \hbar|->$.

3) Montrer que la diagonalisation de $\hat{W}$ fait apparaître les états triplets (S=1) et singulets (S=0) ci-dessous:

$$\begin{aligned}
|S=0, M=0> &= (|e:+>|p:->-|e:->|p:+>)/\sqrt{2} \\
|S=1, M=1> &= |e:+>|p:+> \\
|S=1, M=0> &= (|e:+>|p:->+|e:->|p:+>)/\sqrt{2} \\
|S=1, M=-1> &= |e:->|p:->
\end{aligned}$$

où S et M sont définis par les valeurs propres de $(\mathbf{S}^2, \hat{S}_z)$ où $\hat{\mathbf{S}} = \hat{\mathbf{S}}_e + \hat{\mathbf{S}}_p$ est le spin total:

$$\hat{\mathbf{S}}^2|S,M>= \hbar^2 S(S+1)|S,M> \qquad \text{et} \qquad \hat{S}_z|S,M>= \hbar M|S,M>$$