2022-09-06

1.2 Les États de Bells

Les états de Bell (aussi appelés états EPR) sont une base à deux qbits. Il représente les états intriquées.

$$\left.\begin{aligned} |\psi^{\pm}\rangle &= \tfrac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \\ |\Psi^{\pm}\rangle &= \tfrac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right) \end{aligned}\right\} \text{État propres de } X_A X_B \text{ et } Z_A Z_B$$

Rappel

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

(Ce sont donc des états propres de σ_z)

En effets, si je comprends bien $|0\rangle$ et $|1\rangle$ sont des états propres de σ_z et $|0\rangle = \sigma_x |1\rangle = \sigma_x^2 |0\rangle$, donc σ_x ne fait que changer le signe de $|\Psi\rangle$ et $|\Phi\rangle$

On peut qualifier les états de Bells par rapport à l'action de XX et ZZ

$ZZ\backslash XX$	$+1$	-1
$+1$	$\|\Psi^+\rangle$	$\|\Psi^-\rangle$
-1	$\|\Psi^+\rangle$	$\|\Psi^-\rangle$

Alice et Bob peuvent faire passer l'état d'un à l'aute en faisant un ou l'autre une mesure (transformation locale). Ex :

$$\left|\Phi^+\right\rangle = X_A I_B \left|\Psi^+\right\rangle = I_A X_B \left|\Psi^+\right\rangle$$

Les état de Bell, étant des états intriqués, ne peuvent pas s'écrire comme le produit tensoriel de deux états.

L'information contenue dans les états de Bell est contenue dans l'intrication et non dans l'état des qbits individuellement.

$$\left\langle\Phi^+\right| Z_a \left|\Phi^+\right\rangle = \left\langle\Phi^-\middle|\Phi^-\right\rangle = 0$$
$$\left\langle\Phi^+\right| X_a \left|\Phi^+\right\rangle = \left\langle\Phi^-\middle|\Psi^+\right\rangle = 0$$
$$\left\langle\Psi^+\right| Y_A \left|\Psi^+\right\rangle = 0$$

(les valeurs de X,Y et Z sont complètement aléatoires...)

On ne peut pas assigner d'état pur à l'état du qbit d'Alice (ou Bob). On a besoin d'une matrice densité (ρ)

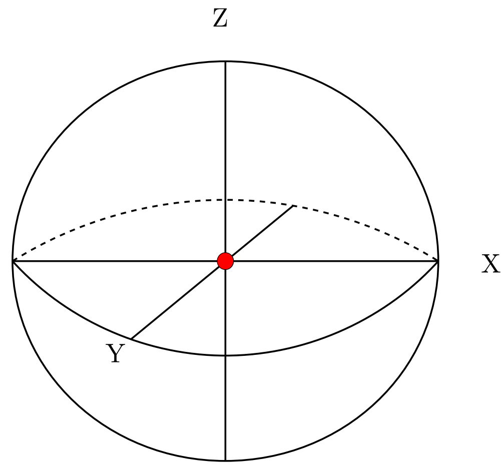

FIGURE 1 – Bell bloch boule

1.3 Encodage dense

A veut envoyer un message à B. Les deux sont liés par un canal quantique.

A envoie à B un qbit. Dans ce sénario, un seul bit peut être envoyé. A priori Bob ne connais pas la base dans lequel le qbit est encodé

Dans ce sénario on obtiens qu'un bit meme pas non ?

Peut-on faire mieux si on prend en compte de l'inrication ?

On suppose que Bob et Alice se partage un état de Bell ($|\Psi^+\rangle$). (Chacun un qbits)

Alice applique une transformation sur son qbits (qui est dans un état de bell). Si elle veut envoyer (00) , elle va appliquer $\mathbb{1}$ à $|\Psi^+\rangle$. Si elle veut envoyer (10) $X_A |\Psi^+\rangle$. (01) : $Z_a |\Psi^+\rangle$. (11) : $Z_A X_A |\Phi^+\rangle = |\Psi^-\rangle$ Alice envoie ensuite la moitié de sa paire à Bob.

Bob peut ensuite mesurer les qbits dans la base de la paire et obtenir 2 bits d'information.

L'information a le bonus d'être encrypté. Si on intercepte le 2eme qbits seulement, il ne gagne aucune information.

$$\boxed{e + q \geq 2c}$$

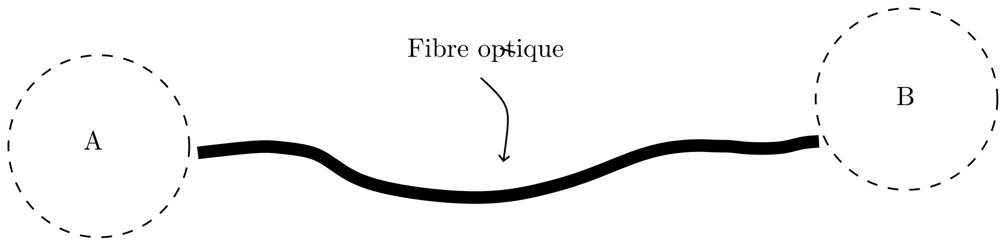

FIGURE 2 – canal quantique

1.4 Cryptographie Quantique (Elert "91, Bennet, Brassard '84)

Cryptographique classique : $\{0,1\}\mathbb{Z}_2$

$$\oplus : \text{addition} \quad \text{mod } 2 \qquad |\otimes| = 0 \qquad 2b = 0$$

<u>One-time pad</u>

Si A et B partagent une chaîne de bits aléatoires secrète (une clé $c \in \mathbb{Z}_2^n$), ils peuvent échanger un message indéchiffrable

A :

$\mathbf{c} = (c_1, c_2, \cdots, c_n) \otimes \mathbf{I} = (i_1, i_2, \cdots i_n) = \mathbf{m} = (m_1, m_2, \cdots m_n)$

B :

$\mathbf{m} = (m_1, m_2, \cdots m_n) \otimes \mathrm{c} = (\mathrm{c}_1, c_2, \cdots, c_n) = \mathbf{I} = (i_1, i_2, \cdots i_n)$

Sans connaître la clef, le message **m** est totalement aléatoire et ne contiens donc aucune information.

<u>cryptographie quantique</u>

Supposons que Alice et Bob partagent un grand nombre de $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Pour chaque paire, A et B mesurent aléatoirement X ou Z.

Il annoncent publiquement quel mesurent chacun a fait sur quel qbits mais pas le résultats qu'ils ont obtenus. Il gardent seulement les résultats des qbits pour lesquels ils ont fait la même mesure. Ils ont donc 100% de corrlélation pour les résultats qu'ils gardent (les autres (ces avec des mesures différents) n'aurait pas été corrélé du tout). Les résultats qu'ils obtiennent forment donc une clef puisque A et B ont tout deux exactement la même chose et sont les seuls à l'avoir.

Robustesse à une attaque de cette méthode

Ève aurait peu intéragir avec les états de Bell de sorte que les pairs soient aussi intriqué avec E. Elle aurait pu attendre l'annonce des mesures pour prendre les sienne et donc obtenir la clef aussi.

De manière générale

$$|\Gamma_{ABE}\rangle = |00\rangle_{AB} \otimes |e_{00}\rangle_E + |01\rangle_{AB} \otimes |e_{01e}\rangle + |10\rangle_{AB} \otimes |e_{10}\rangle + |11\rangle_{AB} \otimes |e_{11}\rangle_E$$

Supposons que A et B peuvent vérifier que $Z_A Z_B = 1$, i.e. les corrélations sont parfaites dans le cas ZZ.

$$\implies |\Gamma_{ABE}\rangle = |00\rangle \otimes |e_{01}\rangle + |11\rangle \otimes |e_{11}\rangle$$

idem pour XX

$$\implies |\Gamma_{ABE}\rangle = (|00\rangle + |11\rangle) \otimes |e\rangle$$

Si A et B sont un état propre de XX et ZZ, ils n'ont plus aucune intrication (corrélation) avec E

$$\implies \text{la clef est secrete}$$

Comment vérifier que les corrélations sont parfaites ?

On peu sacrifier une partie de la clef. Ils publient une partie de leur résultat et vérifie s'il ont une correlation parfaite.

Si elle l'est, la clef est sécuritaite, sinon les états on été traffiqués, il abandonnent.

Ils doivent décider de la portion à sacrifier après l'envoie afin que Eve n'evite pas sélectivement certaines paires.

Distribution de clé BB84

(résumé Ekart)

- A prépare un état $\{|0\rangle\}, |1\rangle, |+\rangle, |0\rangle$ et l'envoie à B.
- Pour chaque qubit, B choisit une base au hasard et mesure dans cette base.
- A et B publient les bases choisies.
- Les résultats aves les bases identiques constituent la clé

A mesure $Z \rightarrow |00\rangle$ ou $|11\rangle$ mesure $X \rightarrow |{+}{+}\rangle$ ou $|{-}{-}\rangle$

Chacun des ces cas est aléatoire avec 25%.

BB84 A prépare $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|11\rangle + |00\rangle) = \frac{1}{\sqrt{2}}(|{+}{+}\rangle + |{-}{-}\rangle)$

A envoie a B cet état

A et B publient et comparent les choix de bases.<

Avantage Ekert

Basé sur intrication, test direct(inégalité de Bell). Pas besoin de faire confiance au système

Avantage BB84 : Pas besoin d'intrication donc plus facile à réalise.

Différence entre Ève et l'environement

Les deux sont très similaires. A vrai dire toute la discussion qu'on a eu jusqu'à maintenant est valide pour les deux.
Par conte l'environement est toujours présent.
Si les corrélation qu'on mesure sont fortes mais pas parfaites on peut faire de la correction d'erreur.

1.5 Théorème de non-clônage

Il est impossible de copier L,information quantique. (Utile de connaître cette contraite lorsqu'on pense aux algorithmes/protocols quantiques). Cette proprité découle directement de la linéarité en MQ.

On cherche une transformation unitaire U telle que

$$U|\psi\rangle|0\rangle = |\Psi\rangle|\Psi\rangle$$

$$\begin{aligned} U|00\rangle &= |00\rangle \\ U|10\rangle &= |11\rangle \end{aligned}$$

Appliquer U sur un état général

$$\begin{aligned} U|\psi\rangle|0\rangle &= u\left(\alpha|0\rangle + \beta|1\rangle\right)|0\rangle \\ &= \alpha|00\rangle + \beta|11\rangle \neq |\psi\rangle|\psi\rangle \end{aligned}$$

puisque

$$|\psi\rangle|\psi\rangle = \left(\alpha|0\rangle + \beta|1\rangle\right)\left(\alpha|0\rangle + \beta|1\rangle\right) = \alpha^2|00\rangle + \alpha\beta\left(|01\rangle + |10\rangle\right) + \beta^2|11\rangle$$

On peu copier un état connu d'avance

On peut aussi montrer cette proprité en utilisant le fait qu'une transformation uniraire préserve le recouvrement des fonction d'onde.

Prenons $|\psi\rangle, |\varphi\rangle$ et appliquons une transformation unitaire

$$|\psi'\rangle = V|\psi\rangle \quad |\varphi'\rangle = v|\varphi\rangle$$

$$\langle\psi|\varphi'\rangle = \langle\psi|V^\dagger V|\varphi\rangle = \langle\psi|\varphi\rangle$$

Maintenat une opération qui copie agirait comme $U\left|\psi 0\right\rangle = \left|\psi\psi\right\rangle \quad U\left|\varphi 0\right\rangle = \left|\varphi\varphi\right\rangle$

$$\langle\psi\psi|\varphi\varphi\rangle = \langle\psi|\varphi\rangle^2 \quad \langle\psi\psi|\varphi\varphi\rangle = \left\langle\psi 0\right| u^\dagger u \left|\varphi 0\right\rangle = \langle\psi|\varphi\rangle\langle 0|0\rangle = \langle psi|\varphi\rangle$$

En général $\langle\psi|\varphi\rangle^2 \neq \langle\psi|\varphi\rangle$

$$\implies U\text{n'existe pas}$$

1.6 Téléportation quantique

On peut utiliser des ressources quantique pour faire de la communication classique. La téléportation c'est l'inverse.

A veut envoyer un état $\left|\psi\right\rangle$ a B 1) Elle connaît l'état : transmet 2 nombres réels ($\geq 2c$) 2) Elle ne connaît pas l'état : Elle peut mesurer $\{\left|0\right\rangle, \left|1\right\rangle\}$ (ou dans tout autres base) et transmet le résultat de la mesure à B

$$\bar{F} = \left|\langle\psi_B\left|\psi_A\right\rangle|\right|^2 = \frac{2}{3}$$

C'est mieux qu'un état aléatoire où $F = \frac{1}{\alpha}$

Protocole de téléportation quantique

Supossons que A et B partagent un état ψ^+

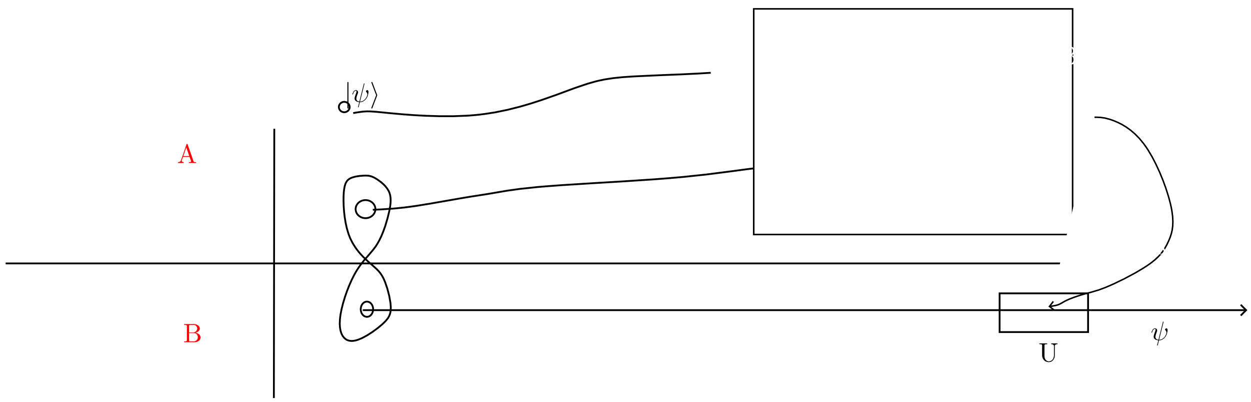

Figure 3 – Téléportation quantique