MÉCANIQUE QUANTIQUE

COURS 12 & 13 – INTRODUCTION À L'INFORMATION QUANTIQUE

QUENTIN GLORIEUX

3P001 – UNIVERSITÉ PIERRE ET MARIE CURIE 2015-2016

INTRODUCTION À L'INFORMATION QUANTIQUE

- Notion de qubit
- Etats séparables, états intriqués
- Argument EPR : La mécanique quantique est elle complète ?
- Portes quantiques et théorème de non-clonage
- Applications (cours 13)
  - Codage dense
  - Cryptographie quantique
  - Téléportation quantique

RAPPELS

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

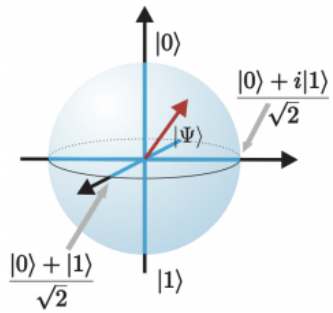
$$|\psi\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$$

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$\mathrm{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$



CLONAGE D'UN QUBIT

Peut on cloner un état quantique (un qubit) inconnu ?

- Il semble que la porte CNOT fasse cette opération :

$$\mathrm{CNOT}\,|0\rangle|0\rangle \to |0\rangle|0\rangle$$
$$\mathrm{CNOT}\,|1\rangle|0\rangle \to |1\rangle|1\rangle$$

L'état du premier qubit 1 est copié sur le deuxième qubit.

- Ce n'est pas vrai de manière générale :

$$W_{\mathrm{CNOT}}(\alpha\,|0\rangle + \beta\,|1\rangle)\,|0\rangle \to \alpha\,|0\rangle\,|0\rangle + \beta\,|1\rangle\,|1\rangle \neq (\alpha\,|0\rangle + \beta\,|1\rangle)(\alpha\,|0\rangle + \beta\,|1\rangle)$$

- Si le qubit est connu, on peut le copier autant de fois que l'on souhaite (préparation d'états quantiques cf RMN).

THÉORÈME DE NON-CLONAGE

- Théorème : Pour un état quantique inconnu quelconque, il n'est pas possible de faire une copie parfaite de cet état (sans détruire l'état initial)
- Preuve :
  - On fait un démonstration par l'absurde.
  - Supposons qu'il existe une transformation unitaire $\mathcal{U}_{clone}$ qui clone un système dans un état inconnu.
  - Pour deux états $|\psi\rangle, |\phi\rangle$ on a : $\mathcal{U}_{\text{clone}} |\psi\rangle |0\rangle = |\psi\rangle |\psi\rangle$
    $\mathcal{U}_{\text{clone}} |\phi\rangle |0\rangle = |\phi\rangle |\phi\rangle$
  - Que se passe t'il pour l'état $|\sigma\rangle = \frac{1}{\sqrt{2}}(|\psi\rangle + |\phi\rangle)$?

$$\mathcal{U}_{\text{clone}} |\sigma\rangle |0\rangle = \mathcal{U}_{\text{clone}} \frac{1}{\sqrt{2}}(|\psi\rangle + |\phi\rangle) |0\rangle = \frac{1}{\sqrt{2}}(|\psi\rangle |\psi\rangle + |\phi\rangle |\phi\rangle)$$
$$\neq |\sigma\rangle |\sigma\rangle = \frac{1}{2}(|\psi\rangle |\psi\rangle + |\psi\rangle |\phi\rangle + |\phi\rangle |\psi\rangle + |\phi\rangle |\phi\rangle)$$

CODAGE DENSE

Combien de bits d'information classique peut on envoyer avec un qubit ?

- Principe du codage dense :
  - Alice et Bob partagent une paire de qubits intriqués prenons par exemple : $\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$
  - Alice peut faire 4 opérations différentes sur son qubit : I, X, Z, XZ
  - Les 4 états obtenus sont :

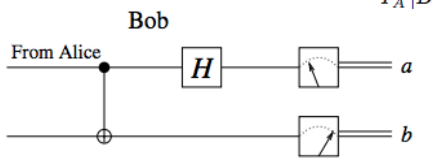
$$I_A |B_{00}\rangle = \frac{1}{\sqrt{2}}(|0^A\rangle |0^B\rangle + |1^A\rangle |1^B\rangle) = |B_{00}\rangle ,$$
$$X_A |B_{00}\rangle = \frac{1}{\sqrt{2}}(|1^A\rangle |0^B\rangle + |0^A\rangle |1^B\rangle) = |B_{01}\rangle ,$$
$$Z_A |B_{00}\rangle = \frac{1}{\sqrt{2}}(|0^A\rangle |0^B\rangle - |1^A\rangle |1^B\rangle) = |B_{10}\rangle ,$$
$$Y_A |B_{00}\rangle = \frac{i}{\sqrt{2}}(|1^A\rangle |0^B\rangle - |0^A\rangle |1^B\rangle) = i |B_{11}\rangle$$

CODAGE DENSE

$$I_A |B_{00}\rangle = \frac{1}{\sqrt{2}}(|0^A\rangle |0^B\rangle + |1^A\rangle |1^B\rangle) = |B_{00}\rangle ,$$
$$X_A |B_{00}\rangle = \frac{1}{\sqrt{2}}(|1^A\rangle |0^B\rangle + |0^A\rangle |1^B\rangle) = |B_{01}\rangle ,$$
$$Z_A |B_{00}\rangle = \frac{1}{\sqrt{2}}(|0^A\rangle |0^B\rangle - |1^A\rangle |1^B\rangle) = |B_{10}\rangle ,$$
$$Y_A |B_{00}\rangle = \frac{i}{\sqrt{2}}(|1^A\rangle |0^B\rangle - |0^A\rangle |1^B\rangle) = i |B_{11}\rangle$$

Ces 4 états sont orthogonaux.

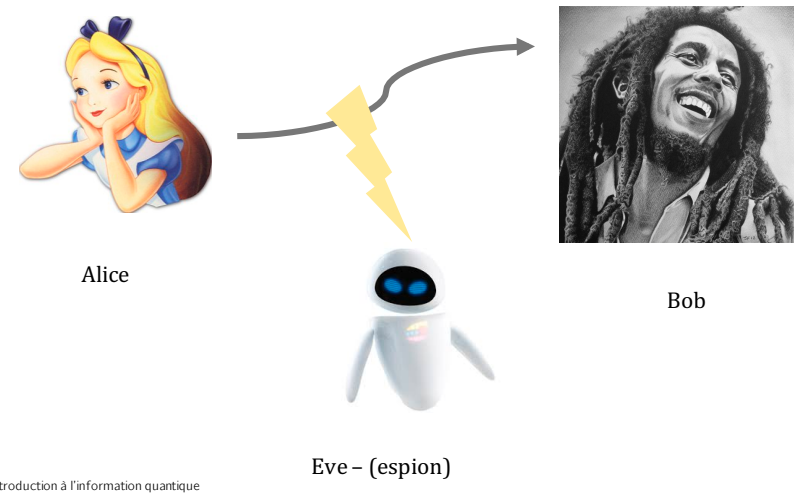
On peut les distinguer avec certitude.



$$|B_{00}\rangle \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(|00^B\rangle + |10^B\rangle) \xrightarrow{H} |00^B\rangle ,$$
$$|B_{01}\rangle \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(|11^B\rangle + |01^B\rangle) \xrightarrow{H} |01^B\rangle$$
$$|B_{10}\rangle \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(|00^B\rangle - |10^B\rangle) \xrightarrow{H} |10^B\rangle ,$$
$$i |B_{11}\rangle \xrightarrow{\text{CNOT}} \frac{i}{\sqrt{2}}(|11^B\rangle - |01^B\rangle) \xrightarrow{H} -i |11^B\rangle$$

ALICE, BOB ET EVE

Les personnages de la cryptographie quantique :



CRYPTOGRAPHIE QUANTIQUE

Afin de coder des messages il est utile de partager une clé secrète.

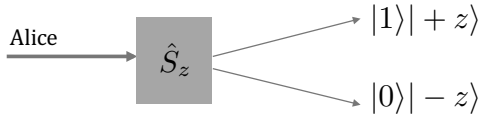
C'est le but de la cryptographie quantique.

Message	*0*	*1*	*1*	*0*	*1*	*1*	*0*	*0*	*0*
CLE	*1*	*1*	*0*	*0*	*0*	*1*	*0*	*1*	*0*
Message codé									

- Alice possède le message et la clé. Elle peut créer le message codé.
- Si Bob posséde la clé et le message codé il peut alors obtenir le message.
- La difficulté est dans le partage de la clé de cryptage.

TRANSFERT DE CLE SECRETE

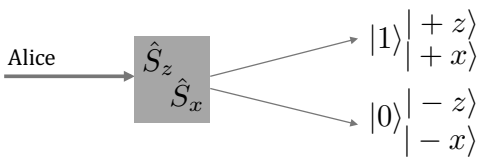
- Alice envoie vers Bob un faisceau de particules de spin $\frac{1}{2}$ après les avoir préparée dans un appareil de Stern et Gerlach selon z.



- Bob reçoit la particule et fait une mesure selon l'axe z.
  Il mesure donc le spin de la particule envoyée par Alice.
- Lors d'une mesure de $+\hbar/2$, Bob ajoute un 1 dans sa clé secrète et s'il mesure $-\hbar/2$, il ajoute un 0 dans sa clé secrète.
- Ce protocole n'a rien de quantique et peut être espionné.

PROTOCOLE BB 84

- On modifie le protocole précédent en donnant le choix à Alice d'orienter son appareil de S&G selon x ou selon z.



-

Numéro de la particule	1	2	3	4	5	6	7	8
Axe choisi par Alice (gardé secret)	z	z	x	z	z	x	x	z
Etat choisi par Alice (gardé secret)	+	−	+	−	−	−	+	−
Axe choisi par Bernard (diffusé publiquement)	z	x	x	z	x	z	x	x
Etat mesuré par Bernard (diffusé publiquement)	+	−	+	−	−	+	+	+
Mesure utile ?	oui	non	oui	oui	non	non	oui	non

ESPION ET CLONAGE

- Si Eve essaie d'espionner le message, dans 50% des cas elle va choisir un appareil de S&G orienté différemment d'Alice.
- Alice et Bob peuvent verifier la présence d'un espion, grace aux erreurs introduites par Eve lors d'un espionnage (théorème de non-clonage).
- En cas d'absence d'erreur, ils peuvent commencer le transfert de clé secrète. Probabilité de non détection : $(3/4)^m \sim 10^{-50}$ pour m=400

Numéro de la particule	9	10	11	12	13	14	15	16
Axe choisi par Alice (gardé secret)	x	z	x	z	z	x	z	z
Etat choisi par Alice (gardé secret)	+	−	+	+	−	−	+	−
Axe choisi par Bernard (diffusé publiquement)	z	z	x	x	z	z	z	x
Etat mesuré par Bernard (gardé secret)	−	−	+	+	−	+	+	+
Mesure utile ?	non	oui	oui	non	oui	non	oui	non

PROTOCOLE B92

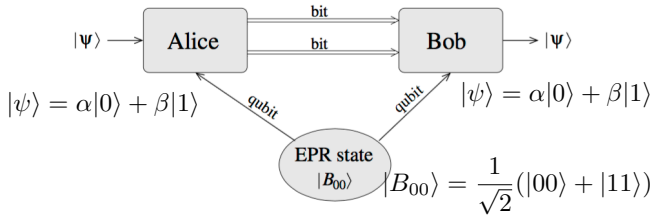
Il existe bien d'autres protocoles. C'est tout le travail de la recherche dans ce domaine.

- Par exemple B92 :
  - Alice envoie le bit 0 si elle envoie $|-z\rangle$ et 1 si elle envoie $|+x\rangle$
  - Bob code son bit dans le choix aléatoire de sa base de mesure. Il code 0 pour la base selon x et 1 pour la base selon z
  - Bob ajoute un bit de contrôle qui dépend du résultat de sa mesure. Ce bit de controle vaut 1 pour $|+z\rangle$ ou $|-x\rangle$ et 0 pour $|-z\rangle$ ou $|+x\rangle$
  - Si le bit de controle est 1 alors, Alice et Bob ont partagé un bit secret.
  - Si Eve tente d'espionner elle sera démasquée comme précédemment

TÉLÉPORTATION QUANTIQUE

- Alice et Bob partage chacun un élement d'une paire intriquée.

$$|B_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$



- Alice souhaite de plus téleporter l'état quantique de son qubit $|\psi\rangle$ à Bob.
- Alice ne connait pas l'état de son qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
  - Impossible de mesurer localement
  - Impossible de cloner

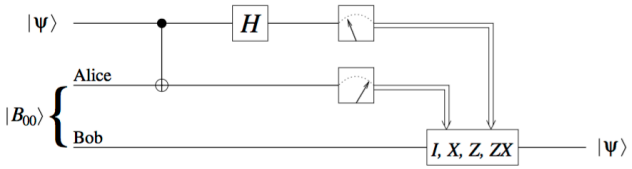
PROTOCOLE

Si on considère maintenant l'état du système à 3 qubits

- celui d'Alice et celui de Bob (la paire intriquée) $|B_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- le qubit qu'Alice souhaite téleporter $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

On a le systeme global : $|\psi_3^{(0)}\rangle = |\psi\rangle\,|B_{00}\rangle = \frac{1}{\sqrt{2}}[\alpha\,|0\rangle(\,|0^{\mathrm{A}}\rangle\,|0^{\mathrm{B}}\rangle + |1^{\mathrm{A}}\rangle\,|1^{\mathrm{B}}\rangle)$
$+\beta\,|1\rangle(\,|0^{\mathrm{A}}\rangle\,|0^{\mathrm{B}}\rangle + |1^{\mathrm{A}}\rangle\,|1^{\mathrm{B}}\rangle)]$

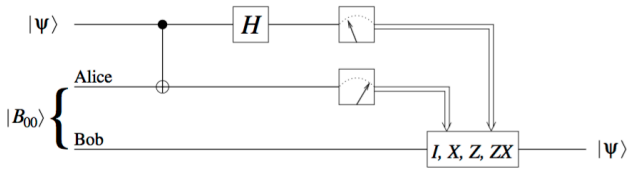
On applique le circuit suivant :



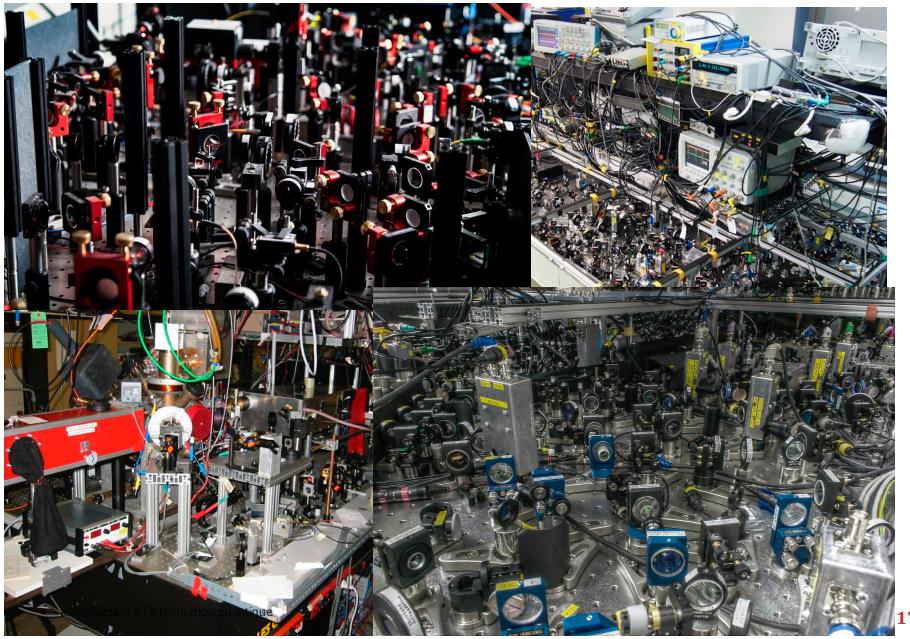
PROTOCOLE

- $|\psi_3^{(0)}\rangle = |\psi\rangle\,|B_{00}\rangle = \frac{1}{\sqrt{2}}[\alpha\,|0\rangle(\,|0^{\mathrm{A}}\rangle\,|0^{\mathrm{B}}\rangle + |1^{\mathrm{A}}\rangle\,|1^{\mathrm{B}}\rangle)$
  $+\beta\,|1\rangle(\,|0^{\mathrm{A}}\rangle\,|0^{\mathrm{B}}\rangle + |1^{\mathrm{A}}\rangle\,|1^{\mathrm{B}}\rangle)]$
- $|\psi_3^{(1)}\rangle = \frac{1}{\sqrt{2}}\,[\alpha\,|0\rangle(\,|0^{\mathrm{A}}\rangle\,|0^{\mathrm{B}}\rangle + |1^{\mathrm{A}}\rangle\,|1^{\mathrm{B}}\rangle) + \beta\,|1\rangle(\,|1^{\mathrm{A}}\rangle\,|0^{\mathrm{B}}\rangle + |0^{\mathrm{A}}\rangle\,|1^{\mathrm{B}}\rangle)]$
- $|\psi_3^{(2)}\rangle = \frac{1}{2}[\alpha(\,|0\rangle + |1\rangle)(\,|0^{\mathrm{A}}\rangle\,|0^{\mathrm{B}}\rangle + |1^{\mathrm{A}}\rangle\,|1^{\mathrm{B}}\rangle)$
  $+\beta(\,|0\rangle - |1\rangle)(\,|1^{\mathrm{A}}\rangle\,|0^{\mathrm{B}}\rangle + |0^{\mathrm{A}}\rangle\,|1^{\mathrm{B}}\rangle)]$

$$|\psi_3^{(2)}\rangle = \frac{1}{2}[\,|00^{\mathrm{A}}\rangle(\alpha\,|0^{\mathrm{B}}\rangle + \beta\,|1^{\mathrm{B}}\rangle) + |01^{\mathrm{A}}\rangle(\alpha\,|1^{\mathrm{B}}\rangle + \beta\,|0^{\mathrm{B}}\rangle)$$
$$+\,|10^{\mathrm{A}}\rangle(\alpha\,|0^{\mathrm{B}}\rangle - \beta\,|1^{\mathrm{B}}\rangle) + |11^{\mathrm{A}}\rangle(\alpha\,|1^{\mathrm{B}}\rangle - \beta\,|0^{\mathrm{B}}\rangle)]$$



IMPLEMENTATION EXPÉRIMENTALE



MECANIQUE QUANTIQUE : UN BILAN

A savoir en Mécanique ondulatoire :

- Description en terme de fonction d'onde
  - Lien de transformation de Fourier entre x et p
  - Paquet d'onde, ondes planes
- Equation de Schrodinger indépendant du temps
  - Exemple de la marche de potentiel
  - Exemple du puit de potentiel
  - Exemple du puit harmonique
  - Exemple du double puit

MECANIQUE QUANTIQUE : UN BILAN

A savoir sur la représentation de Dirac :

- Principe de la mécanique quantique
- Systèmes à deux états
  - Exemple de la molécule d'ammoniac en représentation de Dirac
  - Diagonalisation de matrice 2x2
  - Opérateurs d'évolution
- Utilisation des commutateurs
  - Théorème d'Erhenfest
  - Regles de commutation
- Notions d'ECOC
  - Identifier un ECOC
- Oscillateur harmonique en notation de Dirac
  - a et a^+ , opérateur nombre, états nombres, états cohérents

MECANIQUE QUANTIQUE : UN BILAN

A savoir sur la notion de spin $\frac{1}{2}$:

- Moment cinétique orbital et intrinsèque
  - Interaction classique d'un moment magnétique avec un champ magnétique
  - Expérience de Stern et Gerlach
  - Sphère de Bloch
- Résonnance magnétique nucléaire
  - Configuration expérimentale
  - Résolution des équations d'évolution en présence d'un champ magnétique oscillant
- Principe généraux d'un moment cinétique en MQ :
  - Algebre du moment cinétique
  - Moment cinétique en représentation sphérique

MECANIQUE QUANTIQUE : UN BILAN

A savoir sur les cours d'ouverture :

- Information quantique
  - Description d'un spin $\frac{1}{2}$ sous la forme d'un qubit
  - Possibles implémentations
  - Sphère de Bloch
  - INTRICATION

- Structure de l'atome d'hydrogène.