Mécanique quantique – L3 FIP

Correction du TD 7 - Cryptographie quantique

Avertissement : dans tout ce qui suit, afin d'alléger les notations, on écrit S_z pour désigner indifféremment la composante selon (Oz) du spin de la particule A ou B, le contexte suffisant à expliciter la particule considérée. S n'est jamais à prendre au sens du spin **total** *du système des deux particules (sauf dans le commentaire de l'équation 3). Si vous ne voyez pas ce que cette phrase veut dire (ça viendra sinon au S2), pas la peine de vous prendre la tête avec cet avertissement !*

1 Propriétés de l'état $|\Psi_c\rangle$

1.1 Propriétés de symétrie

1. Il suffit d'inverser les relations trouvées dans le TD 3 :

$$|+\rangle_{\mathbf{u}} = +\cos\frac{\theta}{2}|+\rangle_z + \sin\frac{\theta}{2}e^{i\phi}|-\rangle_z \quad (1)$$

$$|-\rangle_{\mathbf{u}} = -\sin\frac{\theta}{2}|+\rangle_z + \cos\frac{\theta}{2}e^{i\phi}|-\rangle_z. \quad (2)$$

2. Après quelques petits calculs, on trouve :

$$|\Psi_c\rangle = \frac{1}{\sqrt{2}}\left(|+-\rangle_{\mathbf{u}} - |-+\rangle_{\mathbf{u}}\right). \quad (3)$$

L'état $|\Psi_c\rangle$ a donc la même expression dans la base propre de $S_{\mathbf{u}}$ que dans celle de S_z, ce qui n'est pas étonnant a posteriori puisqu'il s'agit de l'état singulet $|S=0, M=0\rangle$ des deux spins couplés, invariant par rotation (voir le cours sur l'addition de moments cinétiques, au cours du second semestre). Toutes les prévisions que l'on peut faire pour des mesures de composantes de spin ne dépendent donc pas du choix de l'axe de mesure.

1.2 Corrélations entre les mesures

3. On peut trouver les deux résultats + et −, chacun avec la probabilité $\frac{1}{2}$.
4. Le sous-espace associé au résultat + pour la particule A est celui engendré par $|++\rangle$ et $|+-\rangle$: état de la particule A fixé, mais état de B libre.
5. Il faut alors projeter le ket $|\Psi_c\rangle$ sur le sous-espace associé, c'est-à-dire appliquer le projecteur $P = |++\rangle\langle++| + |+-\rangle\langle+-|$, puis normer le ket.
6. Non, évidemment.
7. A priori, on peut trouver les 4 couples, par exemple $(+-)$, avec la probabilité $|\langle+- \mid \Psi_c\rangle|^2$. En pratique, deux des produits scalaires sont nuls, et on trouve uniquement les couples $(+-)$ et $(-+)$, chacun avec la probabilité $\frac{1}{2}$.
8. Si les deux particules étaient indépendantes, on devrait avoir par exemple :

$$P_{+-} = P_+ P_-. \quad (4)$$

9. Oui, dans ce cas, les probabilités à une particule se multiplient effectivement pour donner la probabilité conjointe. Prenons en effet :

$$|\Psi_{\mathrm{nc}}\rangle = |\Psi_A\rangle \otimes |\Psi_B\rangle = (\alpha\,|+\rangle + \beta\,|-\rangle) \otimes (\gamma\,|+\rangle + \delta\,|-\rangle)\,.$$

On voit tout de suite que par exemple :

$$P_{++} = |\alpha\gamma|^2 = P_{1+}P_{2+}. \tag{5}$$

L'état $|\Psi_{\mathrm{c}}\rangle$ du système constitué des deux particules est donc qualifié d'*intriqué*, car on ne peut pas écrire l'état individuel de chaque particule : le ket ne se factorise pas (essayez !) et seul l'état du système *global* est défini, si bien que les résultats des mesures effectuées sur les deux particules ne sont pas indépendants.

10. Oui, la corrélation subsiste bien sûr s'ils mesurent tous les deux S_x : on a vu que $|\Psi_{\mathrm{c}}\rangle$ avait la même expression dans toutes les bases. Elle ne subsiste pas par contre si Alice mesure S_x et Bernard S_z : en effet, si Alice mesure S_x et trouve par exemple $+$, le système est projeté dans l'état $|+-\rangle_x$. Bernard a alors une chance sur 2 de mesurer $+$, et pareil pour $-$: il n'y a plus aucune corrélation entre les résultats. Dans le cas où il mesure une composante intermédiaire entre les deux, il subsiste une corrélation partielle : la probabilité qu'il mesure $-$ est supérieure à celle de mesurer $+$, et dépend de l'angle θ entre les axes utilisés (calcul facile, que je vous recommande).

2 Interception et discrétion

On va répondre ici à la question suivante : puisque la mesure de S_z leur donne des clés complémentaires, pourquoi songer à utiliser également S_x ? Pour garder le secret sur la clé, évidemment !

11. En effet, s'ils utilisent systématiquement la composante S_z et que l'espionne finit par l'apprendre, rien ne l'empêche en principe de d'intercepter la clé. En effet, supposons qu'Alice a trouvé $+$ comme résultat de mesure de S_z : la paire de spins est alors projetée dans l'état $|+-\rangle$. Si Eve mesure également S_z, elle va trouver $-$ avec certitude, cela sans modifier le ket (puisqu'il est initialement déjà dans l'état propre $|-\rangle$ de S_z), ni bien sûr le résultat de la mesure que peut ensuite effectuer Bernard.
12. On a plusieurs cas :
    - **Alice et Bernard n'utilisent pas le même axe** (un cas sur 2).
      Ils n'attendent aucune corrélation entre leurs résultats, et on peut montrer facilement (essayez) que l'intervention d'Eve ne change rien à l'affaire.
    - **Alice, Bernard et Eve utilisent le même axe** (un cas sur 4).
      On se trouve dans le même cas (même si c'est accidentellement) que dans la question 1.2.1, donc Eve ne modifie pas le résultat des mesures effectuées par Bernard.
    - **Alice et Bernard utilisent le même axe, mais pas Eve** (un cas sur 4).
      Exemple : Alice mesure S_z et trouve $+$: le système est donc dans l'état $|+-\rangle$.
      Si Eve mesure S_x, elle a une chance sur 2 de mesurer $+$, et la même probabilité de mesurer $-$. Supposons qu'elle trouve $+$: le spin B est alors dans l'état $|-\rangle_x$, et en mesurant S_z, Bernard a une chance sur 2 de trouver $+$, et pareil pour $-$, alors que sans l'intervention d'Eve, il était certain de mesurer $-$.

En moyenne, pour les cas où Alice et Bernard s'attendent à une corrélation (et où, du coup, ils peuvent chercher à la vérifier sur une patrtie de leurs résulatts de mesure), Eve a 75% de chances de passer inaperçue :

— dans 50% des cas, elle mesure la même composante (et donc ne modifie pas les résultats)
— dans le cas contraire, elle a encore 50% de chances de passer inaperçue (même en modifiant intermédiaire l'état du spin)

3 Description du protocole BB84

13. A priori, ils ne peuvent espérer une corrélation entre leurs résultats de mesure (j'ai mesuré $-$, donc tu as mesuré $+$, ...) que quand ils mesurent la même composante, donc dans 50 % des cas.
14. Eve peut espérer ne pas modifier les résultats :
    — si elle mesure la même composante qu'eux deux (50 % des cas où ils mesurent la même composante)
    — dans 50 % des cas où elle ne mesure pas la même composante (donc 25 % de cas supplémentaires).
15. Non : savoir *a posteriori* les axes qu'ils ont choisis est sans intérêt pour Eve : si elle n'a pas fait le bon choix d'axes, le mal est fait de toute façon !
16. En l'absence d'espionne, environ la moitié des mesures d'Alice et Bernard (mais ils savent quelle moitié !) doit donner des résultats opposés. La présence d'Eve doit se détecter par un résultat contraire dans environ un cas sur 4. Ils peuvent donc tester une partie de leur clé : si une fraction (de l'ordre de 25 %) des bits mesurés ne sont pas opposés, c'est qu'ils sont sur écoute.
17. En utilisant une série de 1000 paires, ils peuvent tabler sur environ 500 bits corrélés. S'ils en utilisent 100 pour tester la confidentialité de la ligne, et qu'ils ne détectent aucune erreur, c'est bon signe, car s'ils étaient espionnés, la probabilité de ne pas le détecter serait alors seulement de $\left(\frac{3}{4}\right)^{100}$. Les 400 bits qui restent peuvent alors servir de clé confidentielle.

4 Réalisation expérimentale

4.1 Correspondance entre spin $\frac{1}{2}$ et polarisation

18. On peut intercaler sur le trajet du faisceau un cube séparateur de polarisation, qui transmet les photons d'une certaine polarisation linéaire, et défléchit (à 90°) la polarisation perpendiculaire, et mettre un photomultiplicateur (détecteur rapide et très sensible) dans chacune de ces deux voies de sortie.
19. Si le photon n'est pas dans un des *états propres de l'observable mesurée* (autrement dit, ici, s'il n'est pas polarisé selon un des axes propres du cube polariseur), la loi de Malus classique (appliquée ici au niveau du photon unique) redonne bien les probabilités de mesures habituelles pour des spins $\frac{1}{2}$.

20. Les polarisations rectilignes à 45° (ou circulaires) se décomposent sur les polarisations linéaires exactement de la même façon que les états propres de S_x (ou S_y) sur ceux de S_z.

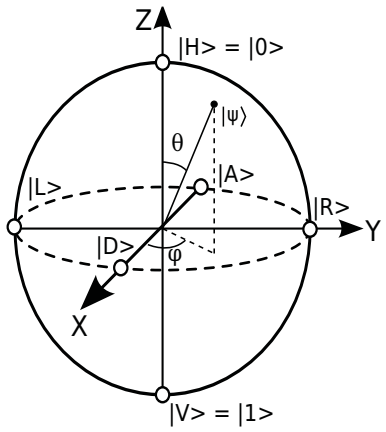

FIGURE 1 – Illustration de la correspondance entre spin $\frac{1}{2}$ et polarisation : A et D correspondent aux polarisations rectilignes diagonale et antidiagonale, L et R aux deux polarisation circulaires droite (R pour *right*) et gauche (L pour *left*). Voir l'article 'Jones calculus' sur Wikipedia.

4.2 Equivalence avec le protocole $BB84$ original

21. En fait, ici, c'est le premier qui fait une mesure de S_z (Alice par exemple) qui fixe l'orientation des spins individuels, et prépare alors également l'état de la particule reçue par son partenaire.
22. *Whenever Alice makes a measurement on photon A, photon B is projected into the orthogonal state which is then analyzed by Bob, or vice versa.*

4.3 De l'intérêt de paires de photons

23. Le risque est qu'Eve puisse collecter un photon en en laissant passer (au moins) un autre vers Bernard, et donc mesurer la polarisation de l'impulsion sans affecter les résultats des mesures effectuées par Bernard.

4.4 Choix aléatoire des axes

Le choix *vraiment* aléatoire des axes est bien sûr un problème crucial. Si Alice et Bernard se contentent de faire tic - S_z - tac - S_x, Eve peut finir par s'en douter.
En pratique, réaliser un générateur aléatoire à partir de machines déterministes comme des ordinateurs n'est pas évident, et on se contente habituellement de signaux pseudo-aléatoires obtenus en sommant des sinusoïdes dont les périodes sont dans des rapports non rationnels.

24. Ici, on utilise le caractère intrinsèquement aléatoire de la mécanique quantique, en préparant un photon dans un état type $|+\rangle_x$ et en mesurant S_z : on a alors un *vrai* signal aléatoire.

It may seem perverse to use a computer, that most precise and deterministic of all machines conceived by th human mind, to produce "random" numbers. More than perverse, it may seem to be a conceptual impossibility. Any program, after all, will produce output that is entirely predictable, hence not truly "random".
Nevertheless, practical computer "random number generators" are in common use. We will leave it to philosophers of the computer age to resolve the paradox in a deep way. One sometimes hears computer-generated sequences termed quasi-random, while the word random is reserved for the output of an intrinsically random physical process, like the elapsed time between clicks of a Geiger counter placed next to a sample of some radioactive element.
(*Numerical Recipes*, début du chapitre 7 sur les nombres aléatoires).

4.5 Problèmes de timing

25. La synchronisation des deux expériences est réalisée avec des horloges atomiques, qui sont synchronisées au début de l'expérience et doivent le rester à l'échelle de la nanoseconde durant toute la durée de la distribution de la clé.

26. Maintenir une précision meilleure que 1 ns sur une minute, cela veut dire avoir une précision relative de l'ordre de 10^{-11} : à ce rythme, l'horloge se dérèglerait de moins d'une milliseconde par an ! Difficile donc à réaliser avec une montre (même à quartz), mais facilement accessible avec des horloges atomiques commerciales, qui utilisent des raies atomiques comme étalons de fréquence (à noter que la définition légale de la seconde est basée sur une transition du ^{133}Cs).

4.6 Pertes du système. Efficacité globale

27. Les pertes dans les fibres sont très importantes. On ne détecte une paire que si *aucun* des deux photons partenaires n'est perdu dans la fibre, ce qui explique que le taux de détection double est beaucoup plus faible que le taux simple.

28. Si on suppose que les pertes dans les deux fibres sont indépendantes (ce qui paraît assez raisonnable) :

$$\Gamma_1 = \Gamma\eta, \tag{6}$$
$$\Gamma_2 = \Gamma\eta^2, \tag{7}$$

ce qui permet de remonter aux chiffres donnés dans l'article.

29. La probabilité que deux paires soient émises dans la même fenêtre temporelle est alors :

$$P = \Gamma\tau, \tag{8}$$

(en prenant par exemple l'origine des temps au moment où une paire est émise) où τ est la durée temporelle de la fenêtre. Ici, $P \simeq 3\ 10^{-3}$: la probabilité qu'Alice effectue sa mesure sur un photon et que Bernard effectue la sienne sur celui d'une autre paire est donc négligeable.

30. Sur une durée T, le nombre de bits qu'Alice et Bernard peuvent espérer se transmettre vaut :
$$N = \frac{1}{2}\Gamma_2 T \tag{9}$$
(le facteur $\frac{1}{2}$ provenant du choix aléatoire des axes). Pour $T = 1$ min, $N \simeq 50\,000$.

31. Le taux d'erreur peut s'expliquer par exemple par des problèmes d'alignement des détecteurs. Si on mesure non pas S_z, mais S_u où le vecteur $\mathbf{u}$ fait un angle, même faible, avec (Oz), les corrélations entre les deux mesures sont dégradées.

4.7 Codage d'une image

32. Prenons le cas d'une image en noir et blanc. A chaque point est alors associé un bit (0 pour blanc, 1 pour noir). Chaque bit de la clé sert à coder un bit (donc un point) de l'image, dans un ordre défini à l'avance (par exemple, ligne par ligne). La clé, de même longueur que l'image à coder, peut donc elle-aussi être représentée sous la forme d'une image (comme c'est fait dans l'article). On utilise l'addition (modulo 2) comme principe de codage : si le bit de la clef est 0, le pixel est inchangé, si le bit de la clé vaut 1, on permute la couleur du pixel. L'intérêt de cette méthode, c'est que le décodage est très simple : il suffit de faire la même chose que pour coder : modulo 2, $1 + 1 = 0 + 0 = 0$! C'est le même principe qui est utilisé ici, si ce n'est que dans le cas d'une image en couleurs, à chaque point est associé un plus grand nombre de bits (mais là-encore, l'ensemble des bits utilisés pour un pixel code une couleur qui permet de représenter la clé sous la forme d'une image).

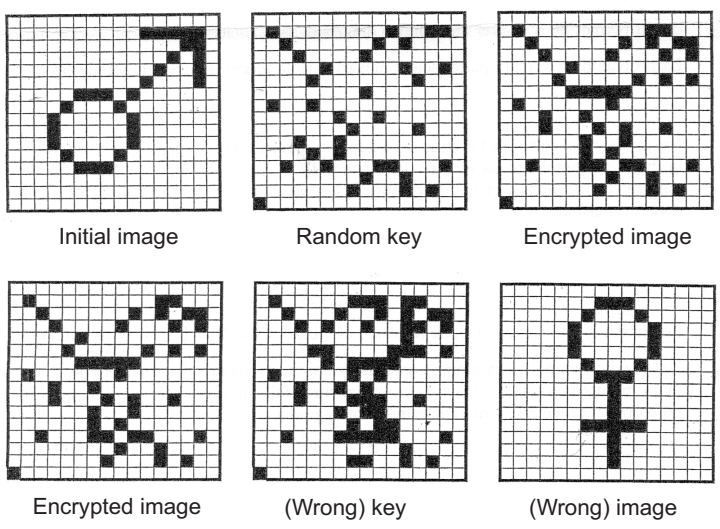

FIGURE 2 – Illustration de la puissance du protocole *one-time pad* : une erreur sur la clé permet de transformer n'importe quel message en n'importe quel autre message.