Mécanique quantique – L2

Antoine Bourget - Alain Comtet - Antoine Tilloy

Séance du 31 octobre 2014 - `www.phys.ens.fr/~tilloy`

TD 5 : Cryptographie

On va utiliser les propriétés d'un système de deux spins $\frac{1}{2}$ pour transmettre un code secret en en garantissant la confidentialité. Le dispositif consiste en une source de paires de particules dans l'état

$$|\Psi_{\mathrm{c}}\rangle = \frac{1}{\sqrt{2}}(|A+\rangle_z |B-\rangle_z - |A-\rangle_z |B+\rangle_z) = \frac{1}{\sqrt{2}}(|+-\rangle - |-+\rangle).$$

Les deux particules partent dans des directions opposées. On se limitera dans la suite aux seuls degrés de liberté de spin des deux particules (le degré de liberté orbital servant uniquement à acheminer les particules vers les détecteurs à partir de la zone où elles sont créées initialement). La composante du moment cinétique de la première est lue par Alice, l'autre par Bernard. Ils peuvent choisir de mesurer cette composante selon deux axes : (Ox) ou (Oz).

1 Propriétés de l'état $|\Psi_{\mathrm{c}}\rangle$

1.1 Propriétés de symétrie

1. Donner l'expression des états $|\pm\rangle_{\mathbf{u}}$ en fonction des états $|\pm\rangle$.
2. En déduire l'expression de $|\Psi_{\mathrm{c}}\rangle$ dans cette nouvelle base. Quelle conclusion peut-on en tirer ?

1.2 Corrélations entre les mesures

Alice effectue une mesure de la composante S_z du spin de la particule A.

3. Quels résultats peut-elle trouver, et avec quelles probabilités ?
4. Quel est le sous-espace associé au résultat + ?
5. On suppose qu'elle trouve + comme résultat de mesure. Quel est le ket décrivant le système immédiatement après la mesure ?
6. Y a-t-il une différence si c'est Bernard qui effectue les mesures ?

On suppose maintenant qu'Alice et Bernard effectuent leur mesure (de S_z) *l'un après l'autre* (par exemple, Alice juste avant Bernard) sur le système initialement dans l'état $|\Psi_{\mathrm{c}}\rangle$.

7. Quels couples de résultats peut-on trouver, et avec quelles probabilités ?
8. Commenter la façon dont les probabilités se combinent par rapport à celles déterminées aux questions précédentes.

9. La situation serait-elle différente si on partait d'un état $|\Psi_{\text{nc}}\rangle$ de la forme :

$$|\Psi_{\text{nc}}\rangle = |\Psi_A\rangle \otimes |\Psi_B\rangle \ ?$$

Commenter alors le nom d'*état intriqué* (*entangled* en anglais) donné à $|\Psi_{\text{c}}\rangle$.

10. Cette corrélation des résultats de mesure subsiste-t-elle s'ils mesurent tous les deux S_x ? Et s'ils mesurent des composantes différentes ?

2 Interception et discrétion

La lecture des composantes S_z fournit donc à Alice et Bernard des clés complémentaires ($++--+--+$..., ou 1101001... en langage binaire). On suppose maintenant qu'une espionne, prénommée Eve (pour *eavesdropper* : personne indiscrète, en anglais), s'interpose sur le chemin de la particule destinée à Bernard et lit elle-aussi la composante du spin selon un des deux axes, juste après Alice, mais juste avant Bernard.

11. Montrer que si Eve sait qu'ils utilisent la composante S_z, elle peut intercepter le code sans modifier les résultats des mesures effectuées par Alice et Bernard.
12. Alice et Bernard décident de mesurer la composante du spin selon un axe choisi au hasard, sans se concerter, sur une série de paires de particules intriquées. Dans quel cas Eve est-elle susceptible de modifier les résultats des mesures effectuées par Bernard ?

3 Description du protocole BB84

On suppose qu'Alice et Bernard effectuent leurs mesures sur des composantes choisies aléatoirement, composantes dont ils ne se donnent la liste qu'*après* avoir effectué la totalité des mesures (sans donner les résultats des mesures associées). Eve ne peut elle-aussi que choisir aléatoirement la composante qu'elle mesure.

13. Dans quel pourcentage de cas peuvent-ils espérer une corrélation entre leurs mesures ?
14. Dans quel pourcentage de cas Eve peut-elle espérer ne pas modifier les résultats des mesures effectuées par Bernard ?
15. Ont-ils besoin d'une ligne sûre pour se transmettre la liste des composantes qu'ils ont choisies ?
16. Comment Alice et Bernard peuvent-ils utiliser une partie de la clé qu'ils obtiennent pour vérifier la confidentialité de la ligne ?
17. Montrer qu'en utilisant une série de 1000 paires de photons, ils peuvent espérer se transmettre une clé de 400 bits avec une probabilité $(\frac{3}{4})^{100}$ d'être *sur écoute* sans qu'ils ne l'aient détecté.

4 Réalisation expérimentale [Facultatif]

Une fois le vecteur d'onde **k** fixé, les deux états de polarisation possibles d'un photon (qui peuvent se décomposer sur différents système d'axes) constituent son seul degré de liberté. Cette (profonde) analogie entre un spin $\frac{1}{2}$ et la polarisation d'un photon unique est mise à profit dans l'expérience que décrit l'article pour implémenter le protocole que l'on vient d'établir.
Les différentes questions suivent (plus ou moins) le déroulement de l'article.

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

On admet que les polarisations linéaires sur deux axes à 90° l'un de l'autre sont les analogues des états $|\pm\rangle$:

$$\begin{aligned} |H\rangle &\longleftrightarrow |+\rangle \\ |V\rangle &\longleftrightarrow |-\rangle\,. \end{aligned}$$

18. Comment peut-on mesurer la polarisation d'un photon unique ?
19. Vérifier que cette analogie conduit aux mêmes résultats de mesures que son équivalent en termes de spins $\frac{1}{2}$.
20. Quels sont alors des équivalents aux états $|\pm\rangle_x$?

4.2 Equivalence avec le protocole BB84 original

Le protocole BB84 original n'utilisait pas des paires de particules intriquées, mais des photons uniques, dont Alice préparait aléatoirement l'état de polarisation qui était lu (tout aussi aléatoirement) par Bernard (ou Bob, pour nos amis anglophones).

21. Quel est le lien avec le protocole utilisé ici ?
22. Quelle phrase de l'article y fait allusion ?

4.3 De l'intérêt de paires de photons

On utilise ici des paires de photon créées par conversion paramétrique (un photon d'énergie $\hbar\omega_0$ est transformé par un effet d'optique non linéaire en deux photons d'énergie $\hbar\omega_0/2$), mais ce protocole est généralement implémenté avec des impulsions lumineuses atténuées (qui contiennent un nombre variable de photons : souvent 0, parfois 1, parfois 2 ...).

23. Quel est dans ce cas le risque, désigné sous le nom de *beamsplitter attack* dans l'article ?

4.4 Choix aléatoire des axes

Un problème important consiste également à s'assurer que le choix des axes de mesure est vraiment aléatoire, sans quoi Eve peut le deviner.

24. Quel type de générateur de signaux aléatoires (*random signal generators*) est utilisé ici, et sur quoi est-il basé ?

4.5 Problèmes de timing

Les deux partenaires étant éloignés l'un de l'autre au moment où ils effectuent leur mesure, il est important que leurs horloges soient synchronisées pour qu'ils effectuent leurs mesures sur des photons appartenant à la même paire, condition indispensable pour que les mesures soient corrélées. La résolution temporelle des différents détecteurs qui interviennent fait qu'à chaque instant, la sortie de la détection est sensible aux événements des 4 ns précédentes (fenêtre glissante). En pratique, on supposera que le temps est discrétisé, avec un incrément de 4 ns.

25. Comment la synchronisation des horloges est-elle effectuée ?
26. Est-elle facile à maintenir sur la durée de l'expérience ?

4.6 Pertes du système. Efficacité globale

Les photons sont transmis par une fibre optique qui permet de les acheminer facilement, mais présente l'inconvénient d'absorber la majorité de la lumière à la longueur d'onde à laquelle on sait réaliser des paires de photons. C'est d'ailleurs pour cette raison qu'on préfère généralement utiliser des impulsions laser atténuées, que l'on sait créer à des longueurs d'onde plus favorables. Chaque partenaire mesure un taux simple de détection de photons $\Gamma_1 = 35\ 000\ \mathrm{s}^{-1}$, mais la plupart des photons détectés à une extrémité n'ont pas de partenaires détectés à la même date à l'autre extrémité. Le taux de détection en coïncidence est uniquement de $\Gamma_2 = 1\ 700\ \mathrm{s}^{-1}$.

27. Pourquoi ?
28. Quelle hypothèse simple sur les pertes permet de remonter aux chiffres de l'article, c'est-à-dire un taux de production des paires (au niveau de la source) $\Gamma = 7 \times 10^5\ \mathrm{s}^{-1}$ et une transmission des fibres $\eta = 5\ \%$?
29. Les événements de type *double paire* jouent-ils alors un rôle ?
30. Quelle est la longueur de la clé qu'Alice et Bob peuvent espérer se transmettre en une minute ?
31. En l'absence d'espionnage, qu'est-ce qui peut expliquer le taux d'erreur observé sur la clé (résultats de mesure qui ne sont pas corrélés, même si elles ont été effectuées selon les mêmes axes) ?

En pratique, des algorithmes simples permettent de passer d'une clé donnée à une autre, moins longue mais avec un taux d'erreur inférieur. Ici, on passe de 80 000 bits avec 2,5 % d'erreur à 49 984 bits avec 0,4 % d'erreur.

4.7 Codage d'une image

32. Expliquer (brièvement) le principe du codage de l'image, et la simplicité de son décodage.