Mechanika Kwantowa dla doktorantów
22 zestaw – 11.4.2006

Kryptografia kwantowa

1. Jak poprzednio definiujemy wektor
$$\vec{n}_\varphi = \cos\varphi\,\vec{n}_z + \sin\varphi\,\vec{n}_x.$$
i operator spinu zrzutowany na $\vec{n}_\varphi$
$$S_\varphi = \vec{S}\cdot\vec{n}_\varphi.$$
Znamy prawdopodobieństwa $P_\pm$ otrzymania w wyniku pomiaru S_φ wartości $\pm\hbar/2$. Natychmiast po tym pomiarze dokonujemy pomiaru S_z (czyli $\varphi = 0$). Jakie są możliwe wyniki tych pomiarów i ile wynoszą prawdopodobieństwa ich otrzymania, w zależności od wyniku pierwszego pomiaru?

   Zakładamy teraz, że stan początkowy jest stanem własnym S_z. Następnie dokonujemy pomiaru S_φ. Jakie są prawdopodobieństwa otrzymania w kolejnym pomiarze tej samej wartości S_z, której odpowiadał stan początkowy?

2. Stan początkowy cząstek a i b o spinie 1/2 jest
$$|\Sigma\rangle = \frac{1}{\sqrt{2}}\left\{|\sigma_z = +1\rangle_a\,|\sigma_z = +1\rangle_b + |\sigma_z = -1\rangle_a\,|\sigma_z = -1\rangle_b\right\}. \tag{1}$$
Pokazać, że ten stan można też zapisać jako
$$|\Sigma\rangle = \frac{1}{\sqrt{2}}\left\{|\sigma_x = +1\rangle_a\,|\sigma_x = +1\rangle_b + |\sigma_x = -1\rangle_a\,|\sigma_x = -1\rangle_b\right\}. \tag{2}$$
Cząstki przygotowane w stanie (**??**,**??**) rozlatują się w dwu przeciwnych kierunkach. Alicja mierzy składową spinu cząstki a wzdłuż osi $\vec{n}_{\theta_a}$. Jakie są możliwe wyniki pomiarów i odpowiadające im prawdopodobieństwa w dwu przypadkach: $\theta_a = 0$ (oś z) lub $\theta_a = \pi/2$ (oś x). Jak wyglądają stany cząstek $a \otimes b$ po dokonaniu przez Alicję w.w. pomiarów w zależności od otrzymanych wyników (tj. oś z wynik $\pm\hbar/2$, oś x wynik $\pm\hbar/2$)?

   Po dokonanym przez Alicję pomiarze, Bolek mierzy składową spinu cząstki b wzdłuż osi $\vec{n}_{\theta_b}$. Jakie są możliwe wyniki pomiarów Bolka i odpowiadające im prawdopodobieństwa w zależności od wyników otrzymanych przez Alicję? Kiedy Alicja i Bolek otrzymają z prawdopodobieństwem 1 ten sam wynik?

3. Rozważmy przypadek, kiedy $\theta_a = 0$. Przypuśćmy, że agent S, ukryty między źródłem a Bolkiem mierzy spin cząstki b wzdłuż osi n_{θ_s}. Jakie wyniki otrzyma agent S w zależności od wyników otrzymanych przez Alicję? Następnie po pomiarze dokonanym przez agenta S, Bolek mierzy spin b dla kąta $\theta_b = 0$. Jakie wyniki otrzymuje

Bolek w zależności od wyników pomiarów agenta? Jakie są prawdopodobieństwa ich otrzymania?

Jakie jest prawdopodobieństwo $P(\theta_s)$, że Alicja i Bolek otrzymają te same rezultaty, po pomiarze dokonanym przez agenta S? Jaka jest wartość oczekiwana $P(\theta_s)$, jeżeli agent S wybiera kąt θ_s w sposób przypadkowy z przedziału $[0, 2\pi]$ z jednorodnym rozkładem prawdopodobieństwa? Jaka jest wartość oczekiwana $P(\theta_s)$, jeżeli agent S wybiera kąt $\theta_s = 0$ lub $\theta_s = \pi/2$ z prawdopodobieństwami 1/2?

4. Aby przekazać poufną informację (informacja to sekwencja bitów $++--+\ldots$) Alicja i Bolek przyjmują następującą procedurę:

   (a) Alicja i Bolek decydują najpierw, względem których osi dokonywać będą pomiarów (synchronizacja układów współrzędnych).

   (b) Alicja, która ma kontrolę nad źródłem Z, przygotowuje uporządkowaną sekwencję $N \gg n$ dwójek spinów w stanie (**??**), gdzie n jest liczbą bitów w przesyłanej wiadomości. Alicja wysyła Bobowi cząstki b a sama zachowuje cząstki a.

   (c) Na każdej cząstce, która do nich dociera, Alicja i Bolek dokonują pomiaru składowej x lub z spinu. Każde z nich wybiera kierunek x lub z w sposób przypadkowy z prawdopodobieństwem 1/2. Dla danej pary spinów (a, b) nie ma korelacji między wyborem osi przez Alicję i przez Bolka. Oboje zapisują otrzymane wyniki.

   (d) Bob wybiera ułamek F z N dokonanych pomiarów. We wszystkich tych przypadkach przekazuje Alicji przez telefon oś pomiaru i jego wynik. W praktyce $F \sim 1/2$.

   (e) W wybranych przez Bolka przypadkach, Alicja porównuje swoje wyniki z wynikami Bolka i w ten sposób stwierdza, czy w proces przekazywania wiadomości wmieszał się agent S. Jeśli odkrywa agenta, to zawiadamia policję lub CBŚ, a proces przekazywania informacji zostaje zakończony. Jeżeli agent nie został wykryty to:

   (f) Alicja otwarcie przyznaje, że agenta nie było, a Bolek przekazuje jej przez telefon osie względem których mierzył spin w pozostałych przypadkach. Jednak nie podaje wyników pomiarów.

   (g) ....

Jak musi wyglądać punkt (g) aby dokonała się poufna transmisja informacji do Bolka bez dodatkowego wysyłania spinów (tj. tylko na podstawie sekwencji już wysłanych N spinów). Proszę skomentować skuteczność zaproponowanej procedury. Jak Alicja moe stwierdzić obecność agenta? Jakie jest prawdopodobieństwo niewykrycia agenta (np. dla $FN = 200$)? Czy agent może się "zamaskować"jeśli zna usytuowanie osi wybranych przez Alicję i Bolka?