Zadania domowe z Informatyki kwantowej

Seria 3

9 XI 2005

Zadanie 1 Czy istnieje operacja unitarna zmieniająca stany bazowe qubitu w następujący sposób:

$$\begin{cases} |0\rangle & \rightarrow & \sqrt{\frac{1}{3}}\,|0\rangle + \sqrt{\frac{2}{3}}\,|1\rangle \\ |1\rangle & \rightarrow & \sqrt{\frac{2}{3}}\,|0\rangle - \sqrt{\frac{1}{3}}\,|1\rangle \end{cases}$$

Jeśli tak to napisz macierz unitarną 2×2 dokonującą tej operacji, a jeśli nie to uzasadnij dlaczego nie istnieje.

Zadanie 2 Rozważmy model atomu trójpoziomowego. Stany atomu są wektorami w trójwymiarowej przestrzeni wektorowej. Oznaczmy przez: $|0\rangle, |1\rangle, |2\rangle$, bazę składającą się z wektorów będących stanami o określonej energii, odpowiednio: E_0, E_1, E_2. W chwili początkowej atom znajdował się w stanie:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

Następnie w wyniku ingerencji laboranta poddany został ewolucji opisanej macierzą unitarną:

$$U = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{\sqrt{2}} & -\frac{1}{2} & \frac{1}{2} \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}$$

W jakim stanie znajduje się atom po ingerencji laboranta. Na koniec laborant dokonuje pomiaru energii atomu. Jakie są prawdopodobieństwa zmierzenia energii E_0, E_1, E_2?

Zadanie 3 Alicja i Bolek wpadli pewnego dnia na pomysł, żeby podczas rozsyłania sekretnego klucza przy pomocy protokołu BB84, zamiast używać stanów polaryzacyjnych fotonów: $|0°\rangle, |90°\rangle$ (baza 1) oraz $|45°\rangle, |135°\rangle$ (baza 2) użyć stanów polaryzacyjnych: $|0°\rangle, |90°\rangle$ (baza 1), $|30°\rangle, |120°\rangle$ (baza 2).

Zakładając, że podsłuchiwacz będzie podsłuchiwał używając nowych baz, stwierdź czy taki protokół będzie bezpieczniejszy czy mniej bezpieczny od tradycyjnego protokołu. W tym celu policz ile bitów (uzyskanych w zgodnych bazach) Alicja i Bolek muszą ujawnić, żeby mieć 99.9% pewności, że nikt nie podsłuchiwał. Ignorujemy naturalne zakłocenia jakie mogą zachodzić w kanale i zakładamy, że wszelka niezgodność w wynikach Alicji i Bolka wynika z obecności podsłuchiwacza. W przypadku tradycyjnego protokołu liczba bitów koniecznych do ujawnienia wynosiła 24.

Powodzenia!

Marek Kuś
Rafał Demkowicz-Dobrzański[1]

[1] zadania są dostępne pod adresem: www.cft.edu.pl/~demko/zadania.html

Odpowiedzi

1. Istnieje bo operacja zachowuje iloczyn skalarny. $U = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & \sqrt{2} \\ \sqrt{2} & -1 \end{bmatrix}$
2. $|\psi\rangle = U|0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$, $p_0 = 1/2, p_1 = 1/2, p_2 = 0$
3. 33 bity, więc jest mniej bezpieczny niż tradycyjny sposób