Estymowanie, Klonowanie, Podsłuchiwanie

Seria 2

Zadanie 1 Wiemy, że nie możliwa jest operacja klonowania produkująca dwie kopie nieznanego stanu kwantowego z jednej jego kopii: $|\psi\rangle \mapsto |\psi\rangle \otimes |\psi\rangle$. A czy jeśli już na początku mamy dwie kopie nieznanego stanu $|\psi\rangle$, czy możliwe jest wyprodukowanie jego trzech kopii? Innymi słowy czy możliwa jest transformacja, która dla dowolnego stanu $|\psi\rangle$ działa w następujący sposób:

$$|\psi\rangle \otimes |\psi\rangle \otimes |0\rangle \mapsto |\psi\rangle \otimes |\psi\rangle \otimes |\psi\rangle$$

Odpowiedź powinna zawierać coś więcej niż tylko stwierdzenie tak lub nie.

Zadanie 2 Poniżej podanych jest kilka stanów dwóch qubitów. Które z tych stanów są splątane, a które produktowe?

a) $\frac{1}{\sqrt{3}}|0\rangle \otimes |0\rangle + \sqrt{\frac{2}{3}}|0\rangle \otimes |1\rangle$

b) $|0\rangle \otimes |0\rangle$

c) $\frac{1}{\sqrt{3}}|0\rangle \otimes |0\rangle + \sqrt{\frac{2}{3}}|1\rangle \otimes |1\rangle$

d) $\frac{1}{2}(|0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$

Zadanie 3 Na wykładzie przedstawiony został schemat teleportacji korzystający ze stanu splątanego $|\psi_+\rangle = 1/\sqrt{2}(|01\rangle + |10\rangle)$. Co zmieniłoby się w protokole teleportacji jeśli zamiast tego stanu używalibyśmy stanu $|\psi_-\rangle = 1/\sqrt{2}(|01\rangle - |10\rangle)$.

Zadanie 4 Wiemy, że stan $|\psi_-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$ zwany singletem jest niezmienniczy względem wspólnych operacji unitarnych na obu qubitach:

$$U \otimes U|\psi_-\rangle = |\psi_-\rangle. \tag{1}$$

Udowodnij powyższy fakt podstawiając za U ogólną postać macierzy unitarnej:

$$U = \begin{bmatrix} \cos\alpha e^{-i(\beta+\gamma)} & -\sin\alpha e^{i(-\beta+\gamma)} \\ \sin\alpha e^{i(\beta-\gamma)} & \cos\alpha e^{i(\beta+\gamma)} \end{bmatrix} \tag{2}$$

Zbadaj ponadto jak pod wpływem takich operacji zachowywałby się stan $|\phi_+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$. Dla jakiej klasy operacji U on też będzie niezmienniczy?

Zadanie 5 Rozważ atak na protokół BB84, w którym podsłuchiwacz mierzy foton losowo w bazie $|\leftrightarrow\rangle, |\updownarrow\rangle$, lub w bazie $|\nearrow\rangle, |\nwarrow\rangle$. Ponadto załóż że podsłuchiwacz atakuje tylko część fotonów. Niech r oznacza stosunek fotonów atakowanych przez podsłuchiwacza do wszystkich fotonów. Po dokonaniu pomiaru podsłuchiwacz odsyła do B taki stan jaki mu wyszedł z pomiaru.

a) Oblicz dla jakiego r informacja wzajemna $I(A:B)$, będzie równa $I(A:E)$

b) Jakiemu poziomowi błędów to odpowiada (jaki jest QBER)?

Tym samym uzyskasz lepsze górne ograniczenie na dopuszczalne QBER w kryptografii kwantowej. Przyjmij, że w sytuacji, w której podsłuchiwacz nie wykonuje pomiaru zgaduje w sposób losowy wartość bitu A.

Zadanie 6 Zamiast protokółu BB84 można rozważyć protokół korzystający z sześciu stanów:

- baza 1: $|\leftrightarrow\rangle, |\updownarrow\rangle$
- baza 2: $|\nearrow\rangle, |\nwarrow\rangle$
- baza 3: $|\circlearrowleft\rangle, |\circlearrowright\rangle$

a) Zaproponuj przebieg protokołu

b) Jaką część bitów A i B muszą odrzucić w procedurze uzgadniania baz

c) Rozważ podsłuchiwacza, który atakuje każdy foton mierząc go w sposób przypadkowy w jednej z trzech baz i odsyłając do B zmierzoby stan. Oblicz jaki wprowadzi $QBER$, jaka będzie $I(A:B)$, jaka będzie $I(A:E)$.

d) Rozważ sytuację w której podsłuchiwacz atakuje tylko część fotonów r. Dla jakiego r, $I(A:B) = I(A:E)$? Jaki jest odpowiadający temu $QBER$. Czy z tego punktu widzenia protokół 6-cio stanowy jest lepszy od BB84?

Odpowiedzi

Zadanie 1 nie, z unitarności operacji, dowód analogiczny jak w zwykłym twierdzeniu o niemożliwości klonowania

Zadanie 2

a) produktowy

b) produktowy

c) splątany

d) produktowy

Zadanie 3 B musiałby każdą swoją operację korekcji stanu poprzedzić zadziałaniem operacji:

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

Zadanie 4 Stan $|\phi_+\rangle$ będzie niezmienniczy gdy $\beta = \gamma = 0$.

Zadanie 5

a) r=0.682143

b) QBER=0.170536

Zadanie 6

a)

b) 2/3

c) QBER=1/3, $I(A:B) = 0.0817042$, $I(A:E) = 1/3$

d) r=0.681277, QBER=0.227092, wydaje się bezpieczniejszy