

# Komunikacja i Kryptografia Kwantowa

Seria 10

Odpowiedzi

**Zadanie 1 (30 pkt)** Rozważ pomiar rzutowy, rzutujący na stany pewnej bazy ortonormalnej  $|i\rangle$ , wykonany na stanie mieszanym  $\rho$ . Wiemy, że jeśli baza  $|i\rangle$  byłaby bazą wektorów własnych  $\rho$  to entropia Shannona rozkładu prawdopodobieństwa uzyskanych wyników byłaby równa entropii von Neumanna. Zbadaj jak się zachowuje entropia Shannona jeśli baza  $|i\rangle$  nie będzie bazą wektorów własnych  $\rho$ . Najlepiej jeśli uda Ci się poprzeć swoją odpowiedź ścisłymi dowodami. Jeśli nie dasz rady, poprzyj swoje argumenty przykładami

**Odpowiedź:** W ogólności  $H(X) \geq S(\rho)$ . Skorzystaj z wklęsłości funkcji  $-x \log x$ .

**Zadanie 2 (20 pkt)** Rozważ zbiór zawierający wszystkie stany czyste leżące na sferze Blocha na równoleżniku a szerokości geograficznej  $\theta$ . Jaki jest asymptotycznie maksymalny możliwy współczynnik kompresji stanu produktowego  $n$  qubitów, gdzie stan pojedynczego qubit jest niezależnie losowany przypadkowo z powyższego zbioru.

**Odpowiedź:**  $R = -\cos^2 \frac{\theta}{2} \log \cos^2 \frac{\theta}{2} - \sin^2 \frac{\theta}{2} \log \sin^2 \frac{\theta}{2}$

**Zadanie 3 (50 pkt) - pasuje bardziej do poprzedniej serii ale się nie zmieściło** Rozważmy nieco inny protokół kryptografii kwantowej niż BB84, zwany protokołem sześć stanowym (6S). Zamiast czterech stanów  $|0\rangle, |1\rangle, |+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}, |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ , dodajmy jeszcze stany  $|+i\rangle = (|0\rangle + i|1\rangle)/\sqrt{2}, |-i\rangle = (|0\rangle - i|1\rangle)/\sqrt{2}$ , tworzące trzecią bazę. Protokół przebiega analogicznie z tym że teraz  $A$  wysyła 6 różnych stanów każdy z prawdopodobieństwem  $1/6$  a  $B$  mierzy qubit przypadkowo w jednej z trzech baz.

- Jaką średnio część pomiarów  $A$  i  $B$  muszą odrzucić w procedurze uzgadniania baz
- Przeanalizuj ataki typu intercept-resend i postaraj się na tej podstawie znaleźć graniczny próg QBER powyżej którego destylacja klucza nie jest możliwa
- Adaptując odpowiednio wyprowadzenie z wykładu, znajdź optymalny indywidualny atak na protokół 6S
- Dla optymalnego indywidualnego ataku narysuj zależność  $I(A : B)$  i  $I(A : E)$  w funkcji QBER i wyznacz  $\text{QBER}_{\text{th}}$  powyżej którego destylacja klucza nie jest możliwa.
- Zastanów się nad korzyściami i wadami protokołu 6S nad BB84. Kiedy używałbyś jednego a kiedy drugiego?

**Odpowiedź:**

a) Trzeba odrzucić 2/3 pomiarów

b)  $QBER_{th} = 22,7\%$

c) Dodatkowo w porównaniu z wyprowadzeniem dla BB84 iloczyn skalarny  $\langle e_{01}|e_{10}\rangle = 0$ , co powoduje, że  $\langle e_{00}|e_{11}\rangle = 2 - \frac{1}{1-QBER}$ .

d)  $QBER_{th} = 15,6\%$

e) Ponieważ tracimy, aż 2/3 zdarzeń w protokole 6S opłaca się go używać gdy jesteśmy blisko  $QBER_{th}$  i dla protokołu BB84 praktycznie nie byłibyśmy w stanie nic uzyskać albo bardzo mało.