Komunikacja i Kryptografia Kwantowa

Seria 10

do oddania na 21.12.2010 (**100 pkt** do podziału)

Zadanie 1 (30 pkt) Rozważ pomiar rzutowy, rzutujący na stany pewnej bazy ortonormalnej $|i\rangle$, wykonany na stanie mieszanym ρ. Wiemy, że jeśli baza $|i\rangle$ byłaby bazą wektorów własnych ρ 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 ρ. Najlepiej jeśli uda Ci się poprzeć swoją odpowiedź ścisłymi dowodami. Jeśli nie dasz rady, poprzyj swoje argumenty przykładami

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

Zadanie 3 (50 pkt) - pasuje bardziej do poprzedniej serii ale się nie zmieściło Rozważny nieco inny protokół kryptografii kwantowej niż BB84, zwany protokołem sześcio 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.

a) Jaką średnio część pomiarów A i B muszą odrzucić w procedurze uzgadniania baz

b) Przeanalizuj ataki typu intercept-resend i postaraj się na tej podstawie znaleźć graniczny próg QBER powyżej którego destylacja klucza nie jest możliwa

c) Adaptując odpowiednio wyprowadzenie z wykładu, znajdź optymalny indywidualny atak na protokół 6S

d) Dla optymalnego indywidualnego ataku narysuj zależność $I(A:B)$ i $I(A:E)$ w funkcji QBER i wyznacz $\mathrm{QBER}_{\mathrm{th}}$ powyżej którego destylacja klucza nie jest możliwa.

e) Zastanów się nad korzyściami i wadami protokołu 6S nad BB84. Kiedy używałbyś jednego a kiedy drugiego?