Mechanika Kwantowa 3/2

Seria 6

do oddania na 25.05.2011

Zadanie 1 (obowiązkowe) 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 (E mierzy przypadkowo w jednej z trzech baz i odsyła stan jaki zmierzyła) i postaraj się na tej podstawie znaleźć graniczny próg QBER powyżej którego destylacja klucza nie jest możliwa. Zakładamy, że E słucha procedury uzgadniania baz przez A i B.

c) Zastosuj optymalną procedurą klonującą wszystkie stany qubitu, jako atak E. Jaki ten atak daje warunek na graniczny QBER powyżej którego destylacja klucza nie jest możliwa.

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

Zadanie 2 (obowiązkowe)

a) Rozważ jedno-bitowy kanał $X \to Y$, $\mathcal{X} = \mathcal{Y} = \{0, 1\}$, gdzie

$$p(y|x) = \begin{array}{c|c|c} y\backslash x & 0 & 1 \\ \hline 0 & 1-\epsilon & \epsilon \\ \hline 1 & \epsilon & 1-\epsilon \end{array} \tag{1}$$

czyli ϵ można traktować jako prawdopodobieństwo błędu. Oblicz informację wzajemną $I(X:Y)$, jeśli $H(X) = 1$. Narysuj wykres $I(X:Y)$ w zależności od ϵ, aby docenić jak szybko informacja wzajemna spada z wrastającym poziomem błędów.

b) Rozważ kanał, $X \to Y$, gdzie $\mathcal{X} = \{0, 1\}$, $\mathcal{Y} = \{0, 1, e\}$,

$$p(y|x) = \begin{array}{c|c|c} y\backslash x & 0 & 1 \\ \hline 0 & 1-\epsilon & 0 \\ \hline 1 & 0 & 1-\epsilon \\ \hline e & \epsilon & \epsilon \end{array} \tag{2}$$

czyli można traktować ten kanał jako kanał z prawdopodobieństwem błędu ϵ, który to błąd sygnalizowany jest symbolem e. Oblicz informację wzajemną $I(X:Y)$ przyjmując, że $H(X) = 1$. Porównaj tę informację z informację uzyskaną w poprzednim podpunkcie, zinterpretuj.

Zadanie 3 Ponieważ istotą bezpieczeństwa w kryptografii kwantowej jest nierozróżnialność nieortogonalnych stanów, ciekawe jest rozważenie protokołu, który używa jedynie dwóch nieortogonalnych stanów. Rozważmy protokół B92 (Bennet 1992) używający dwóch stanów $|0\rangle$ (wartość logiczna 0), $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ (wartość logiczna 1). Protokół przebiega następująco:

a) A wysyła przypadkowo z prawdopodobieństwem 1/2 jeden z dwóch stanów

b) B mierzy przypadkowo w bazie $\{|0\rangle, |1\rangle\}$ lub bazie $\{|+\rangle, |-\rangle\}$

c) A i B komunikują się klasycznie i B informuje A o przypadkach w których zmierzył $|1\rangle$ lub $|-\rangle$ (oczywiście nie podaje który konkretnie). Pozostałe bity zostają odrzucone.

d) B przypisuje stanowi $|1\rangle$ wartość logiczną 1, a stanowi $|-\rangle$ wartość logiczną 0.

Teraz rozwiąż następujące problemy:

a) Jaka część bitów pozostanie po procedurze uzgadniania i czy rzeczywiście w przypadku braku zakłóceń A i B uzyskają identyczny ciąg bitów.

b) Rozważ atak oparty o procedurę optymalnego rozróżniania dwóch stanów nieortogonalnych (oczywiście atak może polegać na tym, że atakowana jest jedynie część z lecących fotonów). I znajdź QBER powyżej którego protokół nie jest bezpieczny.

c) W jakiej sytuacji mogłoby być korzystne zamienić stan $|+\rangle$ używany w protokole, na stan którego iloczyn skalarny z $|0\rangle$ byłby większy? A kiedy opłacałoby się, żeby iloczyn skalarny był mniejszy?