Komunikacja i Kryptografia Kwantowa

Seria 12

do oddania na 11.01.2011 (**100 pkt** do podziału)

Zadanie 1 (20 pkt) Na wykładzie wyprowadziliśmy warunki bezpieczeństwa dla protokołu BB84 wobec ataków kolektywnych korzystając z wariantu kryptografii kwantowej zwanej *entanglement based*. Jak w tym obrazie wyglądałby dowód bezpieczeństwa wobec ataków indywidualnych. Zmodyfikuj rozumowanie przedstawione na wykładzie tak aby odtworzyć, wyprowadzony kiedyś warunek bezpieczeństwa dla ataków indywidualnych QBER$< 14.6\%$.

Zadanie 2 (30 pkt) Postępując analogicznie do wyprowadzenia z wykładu dla protokołu BB84, wyprowadź warunek na QBER gwarantujący bezpieczeństwo dla protokołu 6S wobec ataków kolektywnych (sformułowanie protokołu 6S znajdziesz w serii 10).

Zadanie 3 (50 pkt) Istnieje ciekawy i dość nieintuicyjny trik, który praktycznie za darmo pozwala nieco podnieść graniczny QBER poniżej którego można uznać protokół za bezpieczny. Po fazie uzgodnienia baz, ale przez procedurą korekcji błędów i wzmocnienia prywatności, A dodatkowo zaszumia swój ciąg bitów — tzn. A dla każdego ze swoich bitów niezależnie z prawdopodobieństwem p zmienia jego wartość na przeciwną, ale oczywiście nikogo nie informuje o tym ani B ani E. Dla protokołu BB84 i ataków kolektywnych zbadaj skuteczność tej strategii, tzn:

a) O ile podnosi się graniczny QBER poniżej którego można destylować klucz.

b) Narysuj wykres długości bezpiecznego klucza w zależności od QBER dla strategi z optymalnym zaszumianiem i porównaj ze standardową procedurą

c) Narysuj wykres optymalnej wartości prawdopodobieństwa zaszumiania p w funkcji QBER

Uwaga: możliwe, że konieczne będzie wsparcie się obliczeniami numerycznymi i nie wszystko da się wyprowadzić analitycznie.