# Komunikacja i Kryptografia Kwantowa

## Seria 8

do oddania na 7.12.2010 (**100 pkt** do podziału)

**Zadanie 1 (30 pkt)** Na wykładzie rozważyliśmy jeden atak typu intercept-resend, na protokół BB84, w którym podsłuchiwacz mierzył z prawdopodobieństwem 1/2 w bazie $|\leftrightarrow\rangle$, $|\updownarrow\rangle$ lub w bazie $|\swarrow\rangle$, $|\nwarrow\rangle$. Rozważ atak podsłuchiwacza który polega na atakowaniu $r$-tej części qubitów pomiarem w bazie $|22.5°\rangle$, $|112.5°\rangle$ i odsyłaniem zmierzonego stanu. Znajdź próg QBER powyżej którego destylacja klucza nie jest możliwa.

**Zadanie 2 (30 pkt)** Przybliżone klonowanie, może być jedną z form ataku podsłuchiwacza. Rozważ transformację klonującą podaną w Zadaniu 4 w Serii 7, jako atak. Przy czym klon 1 idzie do $B$ a klon 2 zatrzymuje sobie $E$.

a) Jaki pomiar powinna wykonać $E$ na swoim klonie aby zmaksymalizować informację $I(A:E)$ ?

b) Oblicz $I(A:B)$, $I(B:E)$ i zastanów się czy destylacja klucza jest możliwa

**Zadanie 3 (40 pkt)** Na wykładzie rozważaliśmy transformację:

$$|0\rangle_A \otimes |0\rangle_E \to |0\rangle_B \otimes |0\rangle_E \tag{1}$$
$$|1\rangle_A \otimes |0\rangle_E \to |0\rangle_B \otimes |\theta\rangle_E \tag{2}$$

gdzie $|\theta\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$, która w zależności od parametru $\theta$, pozwalała $E$ zwiększać swoją informację na temat bitów zakodowanych w stanach $|0\rangle$, $|1\rangle$ ale jednocześnie wprowadzała zaburzenie w stanach $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ wysyłanych do $B$.

a) Postaraj się napisać zsymetryzowaną operację, tzn. taką w której żadna z baz nie byłaby wyróżniona, czyli $E$ dowiaduje się takiej samej ilości informacji o bitach zakodowanych obu bazach i wprowadza takie same zaburzenie w obu bazach tym większe im więcej informacji uzyskuje.

b) Jakiej transformacji sfery Blocha będzie odpowiadać zmiana stanu qubitu wysyłanego od $A$ do $B$ pod wpływem takiego ataku.

c) Znajdź wartość parametru Twojej transformacji dla której $I(A:B) = I(A:E)$. Jakiemu QBER to odpowiada?

d) Oblicz $I(B:E)$ i zastanów się co w związku z tym wynika dla bezpieczeństwa kryptografii kwantowej z analizy takiego ataku?