# Informacja Kwantowa

## Seria 11

wraz z życzeniami *Wesołych i Spokojnych Świąt oraz Szczęśliwego Nowego Roku* !!!

do oddania na 10.01.2020

**Zadanie 1**

Rozważ ponownie indywidualny atak na protokół BB84 omawiany na koniec ćwiczeń, w którym podsłuchiwacz wykorzystuje maszynę klonującą zoptymalizowaną dla stanów leżących na równiku sfery Blocha (*phase-covariant cloning*, PCC) odpowiadającą przekształceniu unitarnemu:

$$U_x^{\mathrm{PCC}}\,|0\rangle_A|0\rangle_E|0\rangle_{E'} = \frac{1}{\sqrt{2}}|0\rangle_B|0\rangle_E|0\rangle_{E'} + \frac{1}{\sqrt{2}}\left(\cos x\,|0\rangle_B|1\rangle_E + \sin x\,|1\rangle_B|0\rangle_E\right)|1\rangle_{E'} \tag{1}$$

$$U_x^{\mathrm{PCC}}\,|1\rangle_A|0\rangle_E|0\rangle_{E'} = \frac{1}{\sqrt{2}}\left(\cos x\,|1\rangle_B|0\rangle_E + \sin x\,|0\rangle_B|1\rangle_E\right)|0\rangle_{E'} + \frac{1}{\sqrt{2}}|1\rangle_B|1\rangle_E|1\rangle_{E'} \tag{2}$$

a) Pokaż, że dla dowolnego stanu z równika, $|\varphi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + \mathrm{e}^{\mathrm{i}\varphi}|1\rangle\right)$, zredukowane macierze gęstości opisujące kubit wysłany przez Ewę (E) do Boba (B) po dokonaniu klonowania i kubit pozostający w rękach Ewy wynoszą, odpowiednio:

$$\varrho_B = \frac{1}{2}\begin{pmatrix} 1 & \cos x\,\mathrm{e}^{-\mathrm{i}\varphi} \\ \cos x\,\mathrm{e}^{\mathrm{i}\varphi} & 1 \end{pmatrix} \qquad \text{oraz} \qquad \varrho_E = \frac{1}{2}\begin{pmatrix} 1 & \sin x\,\mathrm{e}^{-\mathrm{i}\varphi} \\ \sin x\,\mathrm{e}^{\mathrm{i}\varphi} & 1 \end{pmatrix} \tag{3}$$

b) Rozważ protokół BB84, w którym Alicja (A) wysyła z równymi prawdopodobieństwami stany $\{|+\rangle, |-\rangle, |\mathrm{i}\rangle, |-\mathrm{i}\rangle\}$ z dwóch baz ($|\pm\rangle$, $|\pm\mathrm{i}\rangle$), które to wyznaczają wtedy pomiary wybierane losowo przez Boba. Ewa natomiast czeka do momentu ogłoszenia przez A i B użytych baz ("*sifting stage*") by móc zawsze zmierzyć swój sklonowany kubit w poprawnej bazie. Pokaż, że po dokonaniu "siftingu" ciągi bitów uzyskane przez A, B i E można efektywnie opisać za pomocą kanału $p_{\mathrm{ABE}}(y,z|x)$ przedstawionemu w Zadaniu 2 z Serii 9. Innymi słowy, odtwórz *explicite* tabele rozkładu prawdopodobieństw $p_{\mathrm{ABE}}(x=0,y,z)$ i $p_{\mathrm{ABE}}(x=1,y,z)$, gdzie zmienne losowe $X, Y, Z$ opisują bity w każdej pojedynczej rundzie, uzyskane przez, odpowiednio, A, B i E.

c) Wykorzystując swoją analizą z Serii 9, lub inaczej, wyznacz QBER w funcji $x$ odpowiadający poziomowi błędów w kanale A → B. Co więcej, określ jego wartość graniczną, $\mathrm{QBER}_{\mathrm{th}}$, powyżej której A i B nie są w stanie bezpiecznie destylować klucza kiedy dopuszczona jest dalsza komunikacja tylko w kierunku A → B.

**Zadanie 2**

Rozważmy nieco inny protokół kryptograffi kwantowej niż BB84, zwany protokołem sześciostanowym (6S). Zamiast wysyłania tylko czterech stanów $|0\rangle, |1\rangle, |+\rangle, |-\rangle$, A używa w nim także stanów $|\mathrm{i}\rangle$ i $|-\mathrm{i}\rangle$ tworzących trzecią bazę. Protokół przebiega analogicznie do BB84, z tym że A wysyła teraz 6 różnych stanów, każdy z prawdopodobieństwem 1/6, a B mierzy otrzymany 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, $\mathrm{QBER}_{\mathrm{th}}$, powyżej którego destylacja klucza nie jest możliwa.

c) Adaptując odpowiednio analizę z Zadania 1 powyżej, znajdź efektywny kanał $p_{\mathrm{ABE}}(y, z|x)$ dla indywidualnego ataku, w którym to podsłuchiwacz E podobnie klonuje kubit wysyłany przez A do B, lecz dokonuje tego za pomocą operacji opisanej w Zadaniu 1 z Serii 7 (zoptymalizowanej dla wszystkich stanów, a nie tylko tych leżących na równiku sfery Blocha).

d) Dla powyższego 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) Na bazie uzyskanych wyników, zastanów się nad korzyściami i wadami protokołu 6S nad BB84. Kiedy warto jest używać 6S zamiast BB84, a kiedy odwrotnie?