Informacja Kwantowa 1/2

Seria 6

do oddania na 25.11.2015

Zadanie 1 Na ćwiczeniach rozważyliśmy optymalne klonowanie stanów używanych w protokole BB84. Na podstawie tej analizy byliśmy w stanie stwierdzić, że skoro optymalne klonowanie wprowadza poziom błędów QBER $= 14.6\%$ to z pewnością kryptografia oparta o protokół BB84 nie jest bezpieczne powyżej tej granicy. Transformacja klonująca miała postać:

$$U|0\rangle_A \otimes |0\rangle_E \otimes |0\rangle_{E'} = \frac{1}{\sqrt{2}}|0\rangle_A \otimes |0\rangle_E \otimes |0\rangle_{E'} + \frac{1}{\sqrt{2}}|\Psi_+\rangle_{AE} \otimes |1\rangle_{E'} \tag{1}$$

$$U|1\rangle_A \otimes |0\rangle_E \otimes |0\rangle_{E'} = \frac{1}{\sqrt{2}}|1\rangle_A \otimes |1\rangle_E \otimes |1\rangle_{E'} + \frac{1}{\sqrt{2}}|\Psi_+\rangle_{AE} \otimes |0\rangle_{E'} \tag{2}$$

gdzie $|\Psi_+\rangle = (|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle)/\sqrt{2}$, a podukłady pisane są w kolejności: stan wysyłany do Boba (klon 1), stan zatrzymywany przez Ewę do późniejszego pomiaru (klon 2), maszyna klonująca Ewy. Rozważ nieco inną transformację klonującą U sparametryzowaną przez $\gamma \in [0, 1]$:

$$U|0\rangle_A \otimes |0\rangle_E \otimes |0\rangle_{E'} = \sqrt{\gamma}|0\rangle_A \otimes |0\rangle_E \otimes |0\rangle_{E'} + \sqrt{1-\gamma}|\Psi_+\rangle_{AE} \otimes |1\rangle_{E'} \tag{3}$$

$$U|1\rangle_A \otimes |0\rangle_E \otimes |0\rangle_{E'} = \sqrt{\gamma}|1\rangle_A \otimes |1\rangle_E \otimes |1\rangle_{E'} + \sqrt{1-\gamma}|\Psi_+\rangle_{AE} \otimes |0\rangle_{E'} \tag{4}$$

a) Jeśli wziąć parametr tak jak na ćwiczeniach, czyli $\gamma = 1/2$ wtedy atak nie wyróżniał żadnego ze stanów leżących na równiku sfery Blocha. A czy taka transformacja działała by w analogiczny sposób na stany z biegunów sfery Blocha? Ma to znaczenie jeśli chcielibyśmy zastosować nasz atak do protokołu 6-ścio stanowego a nie tylko do BB84. Postaraj się znaleźć taką wartość parametru γ dla którego powyższa operacja nie wyróżniałaby żadnej z trzech baz używanej w protokole 6-ścio stanowym — co oznacza że prawdopodobieństwo błędu w wyniku pomiaru klonu 1 oraz klonu 2 byłoby takie samo niezależnie od tego któy stan został wysłany przez A.

b) Zastosuj tę optymalną operację klonującą aby przeanalizować bezpieczeństwo 6-ścio stanowego protokołu kryptografii kwantowej. Powyżej jakiego QBER, A i B nie mogą się czuć bezpieczni? Na ile ten wynik jest silniejszy od wyników jakie uzyskiwaliśmy używając bardziej prymitywnych ataków typu zmierz-odeślij?