

Informacja Kwantowa 1/2

Seria 8 (trochę obszerna)

do oddania na 26.04.2013

Zadanie 1 Stany Bella dla dwóch qubitów zdefiniowane są następująco:

$$|\Psi^\pm\rangle_{AB} = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle), \quad |\Phi^\pm\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \quad (1)$$

Na wykładzie zostało wyprowadzone, że w sytuacji gdy A i B wykonują pomiary lokalne operator pomiarowy ma postać $M_k^A \otimes M_l^B$, gdzie k, l odpowiednio wyniki pomiarowe uzyskane przez A i B . Podobnie można zastanowić się jak opisalibyśmy operator ewolucji układu, który polega na tym, że A i B wykonują lokalnie pewne operacje (unitarne) na swoich cząstkach. Nie powinno czytelnika zdziwić, że jeśli U_A jest unitarną operacją wykonaną na cząstce A , a U_B operacją wykonaną na cząstce B , to transformację stanu dwóch qubitów opisuje operacja $U_A \otimes U_B$.

- Znajdź zredukowaną macierz gęstości dla podukładu A dla każdego z czterech stanów Bella
- Wyobraź sobie, że A i B dysponują jednym ze stanów Bella. Czy są w stanie każdy ze stanów Bella przekształcić do stanu $|\Psi^-\rangle$ za pomocą lokalnych operacji unitarnych. Jeśli nie uzasadnij, jeśli tak podaj te operacje.
- Sformułuj protokół kwantowej teleportacji (podaj wszystkie kroki) w sytuacji gdy A i B na początku nie dysponują stanem splątanym $|\Psi^-\rangle$ tylko $|\Phi^+\rangle$.

Zadanie 2 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:

$$U|0\rangle_A \otimes |0\rangle_E \otimes |0\rangle_{E'} = \frac{1}{\sqrt{2}}|0\rangle_B \otimes |0\rangle_E \otimes |0\rangle_{E'} + \frac{1}{\sqrt{2}}|\Psi_+\rangle_{BE} \otimes |1\rangle_{E'} \quad (2)$$

$$U|1\rangle_A \otimes |0\rangle_E \otimes |0\rangle_{E'} = \frac{1}{\sqrt{2}}|1\rangle_B \otimes |1\rangle_E \otimes |1\rangle_{E'} + \frac{1}{\sqrt{2}}|\Psi_+\rangle_{AE} \otimes |0\rangle_{E'} \quad (3)$$

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 $\gamma \in [0, 1]$:

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

$$U|1\rangle_A \otimes |0\rangle_E \otimes |0\rangle_{E'} = \sqrt{\gamma}|1\rangle_A \otimes |1\rangle_E \otimes |1\rangle_{E'} + \sqrt{1-\gamma}|\Psi_+\rangle_{AE} \otimes |0\rangle_{E'} \quad (5)$$

- 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 który 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 zmiernic-odeślij?