

Informacja Kwantowa 1/2

Seria 11

do oddania na 18.05.2012

Na ćwiczeniach rozważyliśmy optymalny atak na protokół BB84, który był równocześnie procedurą optymalnego klonowania stanów qubitu leżących na równiku sfery Blocha. W sytuacji gdy oba klony były tej samej jakości transformacja miała postać:

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

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

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

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

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

- 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.
- 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?
- Wiemy, że stan mieszany qubitu możemy przestawić za pomocą wektora \vec{s} w kuli Blocha

$$\rho = \frac{1}{2} (\mathbb{1} + \vec{s} \cdot \vec{\sigma})$$

(jeśli $|\vec{s}| = 1$, czyli jesteśmy na sferze Blocha to mamy stany czyste, a im bardziej do środka tym bardziej mamy stany mieszane). Jeśli by patrzeć na dowolny czysty stan wejściowy $|\psi\rangle_A$ a następnie na któryś z klonów tego stanu, który oczywiście będzie stanem mieszanym, to jak to by wyglądało w języku wektora Blocha. — podaj geometryczny opis co się dzieje z wektorem Blocha w wyniku klonowania qubitu, które znalazł(a)ś w podpunkcie a).