Komunikacja i Kryptografia Kwantowa

Seria 9 - trudna

do oddania na 14.12.2010 (**100 pkt** do podziału)

Zadanie 1 (40 pkt) Niech $\mathcal{E} : \mathcal{L}(\mathcal{H}_A) \mapsto \mathcal{L}(\mathcal{H}_B \otimes \mathcal{H}_E)$ będzie odwzorowaniem całkowicie dodatnim opisującym pewien atak podsłuchiwacza na protokół BB84. Oznaczmy jako $\mathcal{E}_{AB}$ odwzorowanie obcięte do wyjściowej podprzestrzeni $\mathcal{H}_B$, czyli $\mathcal{E}_{AB}(\rho) = \mathrm{Tr}_E \mathcal{E}(\rho_A)$. Niech U_i, $i \in \{0,1,2,3\}$, będą operacjami unitarnymi generującymi stany używane w BB84: $|\psi_i\rangle = U_i|0\rangle$. Zdefiniujmy operację:

$$\mathcal{E}^{\mathrm{cov}}_{AB}(\rho) = \frac{1}{4}\sum_i U_i^\dagger \mathcal{E}_{AB}(U_i \rho U_i^\dagger) U_i \tag{1}$$

a) Udowodnij, że średni QBER dla operacji $\mathcal{E}^{\mathrm{cov}}_{AB}$ jest taki sam jak dla operacji $\mathcal{E}_{AB}$.

b) Udowodnij, że operacja $\mathcal{E}^{\mathrm{cov}}_{AB}$ jest operacją kowariantną, ze względu na grupę $\{U_i\}$

c) Na wykładzie było powiedziane, że możemy ograniczyć się w poszukiwaniach optymalnych ataków zawsze do operacji które na kanale $A \to B$ są kowariantne. Poprzednie punkty pokazały, że istotnie zawsze można przedstawić konstrukcję odwzorowania kowariantnego z niekowariantnego, które nie zmienia QBER. Żeby jednak uzasadnić założenie z wykładu, należy skonstruować pełne odzworowanie tzn, uwzględniające również E, takie które byłoby kowariantne na kanale $A \to B$, nie zmieniało QBER a co więcej nie zmieniało średniej informacji E o atakowanym qubicie. Postaraj się podać taką konstrukcję

Odpowiedzi

c) E musi zapisywać w jakimś ze swoich dodatkowych rejestrów E' jaką operację zastosowała do danego qubitu w celu ukowariantnienia kanału $A \to B$. Dzięki temu będzie zawsze w stanie odzyskać dokładnie taką informację jak dla oryginalnej transformacji. Formalnie, jeśli $\mathcal{E}_{A\to BE}$ jest operacją z przestrzeni A do BE, to operacja poszukiwana kowariantna ma postać:

$$\mathcal{E}^{\mathrm{cov}}_{A\to BEE'}(\rho_A) = \frac{1}{4}\sum_i U_i^\dagger \otimes \mathbb{1}_E \otimes V_i \; \mathcal{E}_{A\to BE}(U_i \rho_A U_i^\dagger) \otimes |0\rangle\langle 0| \; U_i \otimes \mathbb{1}_E \otimes V_i^\dagger, \tag{2}$$

gdzie $V_i|0\rangle = |i\rangle$ zapisuje w dodatkowym rejestrze E' numer operacji zastosowanej na qubicie.

Zadanie 2 (30 pkt) Na wykładzie uczyniliśmy założenie, że wszystkie iloczyny skalarne i współczynniki opisujące atak E są rzeczywiste. Spróbuj wyprowadzić optymalny atak bez tego założenia (ja nie wiem jak).

Zadanie 3 (30 pkt) Powtórz wyprowadzenie optymalnego symetrycznego ataku, przy założeniu rzeczywistych współczynników, ale tym razem postaraj się zmaksymalizować informację Renyiego $I_2(A:E) = H_2(A) - H_2(A|E)$, zamiast maksymalizować informację Shannona $I(A:E)$ Narysuj wykres w funkcji QBER, $I(A:B)$ oraz $I_2(A:E)$. Jeśliby za kryterium bezpieczeństwa przyjąć $I(A:B) \geq I_2(A:E)$ ile wynosi QBER threshold.

Odpowiedzi Atak jest dokładnie taki sam jak dla maksymalizacji informacji Shannona,

$$I_2(A:E) = 1 + \log\left[\frac{1}{2} + 2\mathrm{QBER}(1-\mathrm{QBER})\right] \tag{3}$$

$I(A:B) = I_2(A:E)$ dla $\mathrm{QBER}_{\mathrm{th}} = 11.38\%$.