

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 podsłuchiacza na protokół BB84. Oznaczmy jako \mathcal{E}_{AB} odwzorowanie obcięte do wyjściowej podprzestrzeni \mathcal{H}_B , czyli $\mathcal{E}_{AB}(\rho) = \text{Tr}_E \mathcal{E}(\rho_A)$. 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:

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

- Udowodnij, że średni QBER dla operacji $\mathcal{E}_{AB}^{\text{cov}}$ jest taki sam jak dla operacji \mathcal{E}_{AB} .
- Udowodnij, że operacja $\mathcal{E}_{AB}^{\text{cov}}$ jest operacją kowariantną, ze względu na grupę $\{U_i\}$
- Na wykładzie było powiedziane, że możemy ograniczyć się w poszukiwaniach optymalnych ataków zawsze do operacji które na kanale $A \rightarrow B$ 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 odwzorowanie tzn, uwzględniające również E , takie które byłoby kowariantne na kanale $A \rightarrow B$, nie zmieniało QBER a co więcej nie zmieniało średniej informacji E o atakowanym qubicie. Postaraj się podać taką konstrukcję

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 $I_2(A : E)$. Jeśli by za kryterium bezpieczeństwa przyjąć $I(A : B) \geq I_2(A : E)$ ile wynosi QBER threshold.