

Informacja Kwantowa 1/2

Seria 6

do oddania na 04.04.2014

Zadanie 1 Rozważ jedno-bitowy kanał $X \rightarrow Y$, $\mathcal{X} = \mathcal{Y} = \{0, 1\}$, gdzie

$$p(y|x) = \begin{array}{c|cc} y \backslash x & 0 & 1 \\ \hline 0 & 1 - \epsilon & \epsilon \\ \hline 1 & \epsilon & 1 - \epsilon \end{array} \quad (1)$$

Znajdź pojemność \mathcal{C} tego kanału. Zwróć uwagę, że ten kanał nie jest symetryczny ze względu na zamianę wartości bitów wejściowych. Porównaj z pojemnością kanału w którym błąd występowałby w sposób symetryczny: z prawdopodobieństwem ϵ niezależnie od wartości bitu wejściowego.

Zadanie 2 Alicja koduje informację klasyczną przy użyciu dwóch nieortogonalnych stanów qubitów

$$|\psi\rangle = \begin{pmatrix} \sin \frac{\theta}{2} \\ \cos \frac{\theta}{2} \end{pmatrix}, \quad |\chi\rangle = \begin{pmatrix} -\sin \frac{\theta}{2} \\ \cos \frac{\theta}{2} \end{pmatrix},$$

wysyłanych z jednakowym prawdopodobieństwem równym $\frac{1}{2}$, gdzie $0 \leq \theta \leq \pi/2$.

- Podać informację wzajemną $\mathcal{I}_{\text{minerr}}$ gdy Bob wykonuje pomiar minimalizujący błąd.
- Znaleźć informację wzajemną $\mathcal{I}_{\text{unamb}}$ dla pomiaru jednoznacznego.
- Posiłkując się klasyczną technologią komputerową narysować na wspólnym wykresie, $\mathcal{I}_{\text{minerr}}$ oraz $\mathcal{I}_{\text{unamb}}$ w funkcji $0 \leq \theta \leq \pi/2$.

Zadanie 3 (dodatkowe nie punktowane, ale dla przecznych warto zrobić...) Postępując analogicznie jak na ćwiczeniach, przeanalizuj bezpieczeństwo protokołu sześćo-stanowego kwantowej dystrybucji klucza wobec dwóch rodzajów ataków rozważanych w serii 4, ale tym razem używając informacji Shannona jako miary informacji pozyskanej przez podsłuchiawca. Dla jakich wartości QBER protokół sześćo-stanowy na pewno nie jest bezpieczny?