Informacja Kwantowa

Seria 9

do oddania na 13.12.2019

Zadanie 1

Dla $n \geq 2$ zmiennych losowych X_i oraz zmiennej losowej Y udowodnij następujący fakt (*chain rule*):

$$I(X_1, X_2 \ldots, X_n : Y) = I(X_1 : Y) + \sum_{i=2}^{n} I(X_i : Y | X_1, X_2, \ldots, X_{i-1}). \tag{1}$$

Zadanie 2

Wyobraź sobie, że w wyniku interwencji podsłuchiwacza (Ewy), rozkład prawdopodobieństwa wartości bitów Alicji (A), Boba (B) i Ewy (E) ma postać:

$$p_{\mathrm{ABE}}(0,y,z) = \begin{array}{c|c|c} z\backslash y & 0 & 1 \\ \hline 0 & \frac{1}{2}(1-D)(1-E) & \frac{1}{2}D(1-E) \\ \hline 1 & \frac{1}{2}(1-D)E & \frac{1}{2}DE \end{array}, \quad p_{\mathrm{ABE}}(1,y,z) = \begin{array}{c|c|c} z\backslash y & 0 & 1 \\ \hline 0 & \frac{1}{2}DE & \frac{1}{2}(1-D)E \\ \hline 1 & \frac{1}{2}D(1-E) & \frac{1}{2}(1-D)(1-E) \end{array} \tag{2}$$

gdzie $D = (1-\cos x)/2$, $E = (1-\sin x)/2$, a parametr x jest wolnym parametrem odpowiadającym za siłę ingerencji podsłuchiwacza w komunikację między Alicją i Bobem.

a) Wyraź poziom błędów w kanale A → B (bit-error-rate, BER) w funkcji x.

b) Zakładając, że wszelka komunikacja będzie odbywała się w kierunku A → B znajdź graniczną wartość BER, poniżej której możliwe jest bezpieczne przesyłanie bitów, $\mathcal{C}_S^{\mathrm{A}\to\mathrm{B}} > 0$.

c) Powtórz polecenie z poprzedniego punktu dopuszczając, że komunikacja może odbywać się albo w kierunku A → B albo B → A w zależności od tego co jest lepsze z punktu widzenia Alicji i Boba, $\max\{\mathcal{C}_S^{\mathrm{A}\to\mathrm{B}}, \mathcal{C}_S^{\mathrm{B}\to\mathrm{A}}\} > 0$.

(*)[1] Zadanie 3

Udowodnij że uniwersalną rodzinę funkcji haszujących n-bitów na m-bitów, $\mathcal{H} = \{h : \{0,1\}^n \to \{0,1\}^m\}$, można stworzyć za pomocą przypadkowych binarnych macierzy Toeplitza $\mathbf{T}$ o wymiarach $m \times n$ i przypadkowych binarnych wektorów $\mathbf{b} \in \{0,1\}^m$ jako $\mathcal{H} = \{h(\mathbf{x}) | h(\mathbf{x}) = \mathbf{T}\mathbf{x} + \mathbf{b}\}$[2]. Innymi słowy, pokaż że dla dwóch dowolnych różnych ciągów bitów $\mathbf{x}_1 \neq \mathbf{x}_2 \in \{0,1\}^n$ i dowolnych $\mathbf{y}_1, \mathbf{y}_2 \in \{0,1\}^m$,

$$\Pr_{h\in\mathcal{H}}[\mathbf{y}_1 = h(\mathbf{x}_1) \wedge \mathbf{y}_2 = h(\mathbf{x}_2)] = \frac{1}{2^{2m}}, \tag{3}$$

gdzie h jest wylosowane jednorodnie z rodziny $\mathcal{H}$ (każdy element $\mathbf{T}$ i $\mathbf{b}$ może przyjmować 0 lub 1 z prawdopodobieństwem $\frac{1}{2}$). Pokaż, że w konsekwencji prawdopodobieństwo kolizji dla różnych $\mathbf{x}_1 \neq \mathbf{x}_2$ jest równomierne, tzn. $\Pr_{h\in\mathcal{H}}[h(\mathbf{x}_1) = h(\mathbf{x}_2)] = \frac{1}{2^m}$.

Podpowiedź: Dla macierzy Toeplitza i $\mathbf{x}' = \mathbf{T}\mathbf{x}$ zauważ relację x'_{i+1} z x'_i "rząd po rzędzie".

[1] Zadanie dodatkowe, punkty z którego zostaną doliczone w przypadku "nieidealnych" odpowiedzi na Zad. 1 i 2.

[2] W działaniu macierzy na wektor stosujemy dodawanie modulo 2, czyli operacje XOR dla której $1 \oplus 1 = 0$