Komunikacja i Kryptografia Kwantowa

Seria 4

do oddania na 09.11.2010 (**100 pkt** do podziału)

Zadanie 1 (20 pkt) Wyobraź sobie, że w wyniku interwencji podsłuchiwacza (Ewa), rozkład prawdopodobieństwa wartości bitów Alicji, Boba i Ewy ma postać [1]:

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

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

a) Wyraź poziom błędów w kanale $A \to B$ (QBER) w funkcji x

b) Zakładając, że wszelka komunikacja będzie odbywała się w kierunku $A \to B$, znajdź graniczną wartość QBER, poniżej której jest możliwa destylacja bezpiecznego klucza

c) Powtórz polecenie z poprzedniego punktu dopuszczając, że komunikacją może odbywać się albo w kierunku $A \to B$ albo $B \to A$, w zależności od tego co jest lepsze z punktu widzenia A i B.

Odpowiedź:

a) QBER $= D$

b) QBER $< (2-\sqrt{2})/4 \approx 14.6\%$

c) QBER $< 50\%$

Zadanie 4 (20 pkt) Niech X, Z będą jednobitowymi zmiennymi losowymi. Rozważ rozkład prawdopodobieństwa $p(X^n, Z^n)$ postaci:

$$p(x^n, z^n) = \frac{p}{2^n}\ \delta_{x^n,z^n} + \frac{1-p}{2^{2n}} \tag{2}$$

Gdzie δ_{x^n,z^n} przyjmuje wartość 1 gdy ciąg x^n jest równy ciągowi z^n, a 0 w pozostałych przypadkach.

a) Oblicz warunkową entropię Shanonna $H(X^n|Z^n)$ dla tego rozkładu

b) Oblicz warunkową entropię Renyi'ego $H_2(X^n|Z^n)$ dla tego rozkładu

c) Na podstawie tego przykładu, zastanów się, dlaczego to entropia Renyi'ego a nie entropia Shannona ma większe szanse na bycie odpowiednią wielkością, charakteryzującą liczbę bitów jakie można bezpiecznie wydestylować za pomocą procedur wzmocnienia prywatności.

[1] Taki rozkład prawdopodobieństwa powstaje po wykonaniu przez podsłuchiwacza tzw. optymalnego asymetrycznego klonowania qubitu

Odpowiedź:

a) $H(X^n|Z^n) = -\left(p + \frac{1-p}{2^n}\right)\log\left(p + \frac{1-p}{2^n}\right) - (2^n - 1)\frac{1-p}{2^n}\log\frac{1-p}{2^n} \xrightarrow{n\to\infty} n(1-\epsilon)$

b) $H_2(X^n|Z^n) = -\log\left[\left(p + \frac{1-p}{2^n}\right)^2 + (2^n - 1)\frac{(1-p)^2}{2^{2n}}\right] \xrightarrow{n\to\infty} -\log p^2$

c) Entropia Renyiego nigdy nie będzie duża, nawet jak $n \to \infty$. Co dobrze oddaje fakt, że z prawdopodobieństwem p podsłuchiwacz zna bezbłędnie ciąg x^n a w związku z tym żadne wzmocnienie prywatności nie jest możliwe

Zadanie 5 (20 pkt) Entropia Renyiego (s=2) zmiennej losowej X jest w ogólności mniejsza niż odpowiednia entropia Shannona. Wyjątkiem jest sytuacja gdy rozkład zmiennej losowej jest płaski. Wtedy obie entropie są sobie równe. Wiemy, że dla bardzo wielu realizacji pewnej zmiennej losowej, możemy spodziewać się praktycznie tylko ciągów typowych, których rozkład jest bliski płaskiemu (Asymptotic Equipartition Property). Niech X będzie binarną zmienną losową o rozkładzie prawdopodobieństwa $p(x = 0) = p$, $p(x = 1) = 1 - p$.

a) Oblicz entropię Renyiego $H_2(X^n)$ $(s = 2)$ oraz entropię Shannona $H(X^n)$ zmiennej losowej X^n (n niezależnych realizacji zmiennej losowej X) i wyraź ją przez entropię pojedynczej zmiennej losowej [odpowiednio przez $H_2(X)$ lub $H(X)$].

b) Postaraj się oszacować jak najlepiej potrafisz powyższe entropie, ale przy założeniu, że ograniczamy się jedynie do ciągów ϵ-typowych. Tzn. patrzymy na warunkowy rozkład prawdopodobieństwa X^n wiedząc że ciąg jest ϵ-typowy. Skomentuj uzyskany wynik i porównaj go z wynikiem z poprzedniego podpunktu.

Odpowiedź:

a) $H_2(X^n) = nH_2(X) = -n\log(p^2 + (1-p)^2), H(X^n) = nH(X) = -n[p\log p + (1-p)\log(1-p)]$