Komunikacja i Kryptografia Kwantowa

Seria 3

Odpowiedzi

Zadanie 1 (30 pkt) Antek, Basia i Emilia postanowili przesyłać sobie wiadomości za pomocą dwóch okrzyków: „Och" i „Ach". Basia i Emilia słuchając okrzyków Antka popełniają błąd w interpretacji okrzyku z prawdopodobieństwem odpowiednio 5% i 7%. Antek wydając okrzyki również czasem się myli i wydaje niewłaściwy okrzyk z prawdopodobieństwem 5%. Antek i Basia postanowili wymyślić taki protokół kodowania i dekodowania aby móc przesyłać sobie informację tak by Emilia nie mogła dowiedzieć się niczego na temat wiadomości. Ile bitów sekretnej informacji na jeden okrzyk mogą maksymalnie przesyłać sobie Antek i Basia?

Odpowiedź: $\mathcal{C} = 0.056$ bitów.

Zadanie 5 (35 pkt) Na twierdzenie Csiszar-Korner można patrzeć jak na sytuację w której „zawczasu" nadawca A wykonuje *korekcję błędów*, kodując wiadomość tak by uprawniony odbiorca B mógł ją odkodować bez błędów, lecz dodatkowo wprowadzamy pewną losowość w kodowaniu, które powoduje, że nieuprawniony odbiorca E nie jest w stanie dowiedzieć się nic o przesyłanej wiadomości. Ten drugi element można nazwać *wzmocnieniem prywatności* „zawczasu".

Wyobraź sobie sytuację, w której A przesłał ciąg n bitów bez wykonywania żadnej korekcji błędów ani wzmocnienia prywatności zawczasu. Rozważ, tak jak to było założone w poprzedniej serii, że istnieje dodatkowy publiczny idealny kanał, którym A może wysłać dodatkową informację. Ponieważ kanał jest publiczny, informacja będzie odczytana zarówno przez B jak i E. Mając do dyspozycji taki idealny kanał, spróbuj intuicyjnie opisać co powinni zrobić A i B aby na koniec swojego postępowania uzyskać ciąg bitów, który nie ma błędów a o którym E nic nie wie. Postaraj się gdzie tylko potrafisz podać ilościowe odpowiedzi (np. ile bitów musi przesłać A do B, ile bitów zostanie im na koniec, wyrażone przez odpowiednie wielkości charakteryzujące kanał). Ten protokół można nazwać korekcją błędów i wzmocnieniem prywatności „poniewczasie".

Odpowiedź: A musi dosłać $n[H(X) - I(X:Y)]$ bitów aby B mógł naprawić błędy i miał pełną informację równą $nH(X)$. To jednak spowoduje, że podsłuchiwacz uzyska dodatkową informację i jego informacja będzie równa $n(I(X:Z) + H(X) - I(X:Y))$. A i B muszą następnie dokonać skrócenia swoich ciągów wprowadzając „randomizację" za pomocą np. przypadkowych macierzy binarnych $k \times n$, które działając na ciąg n bitowy tworzą ciąg k bitowy. Przy czym k należy wybrać nie większe niż $n[I(X:Y) - I(X:Z)]$.