Komunikacja i Kryptografia Kwantowa

Seria 5

Odpowiedzi

Zadanie 1 (30 pkt) Podobnie jak w poprzedniej serii, wyobraź sobie, że w wyniku interwencji podsłuchiwacza (Ewa), rozkład prawdopodobieństwa wartości bitów Alicji, Boba i Ewy ma postać:

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

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) Oblicz entropię Renyiego $H_2(A|E)$.

b) Przyjmując, że destylacja klucza jest możliwa pod warunkiem, że $H_2(A|E)$ jest większa od liczby bitów jakie muszą przesłać sobie A i B w celu korekcji błędów, znajdź graniczną wartość QBER poniżej której destylacja jest możliwa. Porównaj i skomentuj uzyskany wynik z wynikiem uzyskanym w zadaniu 1 w poprzedniej serii gdzie korzystaliśmy jedynie z entropii Shannona. Zastanów się, który z tych wyników i kiedy właściwie powinniśmy używać w praktyce.

Odpowiedzi

a) $-\log(1-2E+2E^2)$

b) $QBER < 11.38\%$, bardziej restrykcyjny warunek użyteczny gdy mamy krótkie dane (małe n), jeśli $n \to \infty$ to jest zbyt pesymistyczne ograniczenie i należy raczej używać warunków wynikających z entropii Shannona bo wiadomo, że w granicy $n \to \infty$, na ciągach typowych entropia Renyiego jest równa Shannona

Zadanie 3 (40 pkt)

a) Jeśli za $\mathcal{H}_s$ wziąć klasę funkcji haszujących z zadania 2, ile bitów wystarcza do identyfikacji funkcji w $\mathcal{H}$. Zapisz w sposób z którego wyraźnie widać, że jest to to o co chodzi

b) Udowodnij, że powyższa klasa $\mathcal{H}$ jest rzeczywiście ϵ-*strongly 2-universal* i znajdź wartość ϵ.

c) Jak wpływa złagodzenie definicji *strongly 2-universal class of hash functions* przez dodanie ϵ na bezpieczeństwo autentykacji? Podaj prawdopodobieństwa udanego *impersonation* i *substitution* attack.

Odpowiedzi

a) $(4s-1)\log(a/s) \approx 4\log a(b+\log\log a)$, czyli skaluje się logarytmicznie z a więc ok.

b)

c) $p_i \leq \frac{1}{|\mathcal{B}|}$, $p_s \leq \frac{\epsilon}{|\mathcal{B}|}$