Komunikacja i Kryptografia Kwantowa

Seria 5

do oddania na 16.11.2010 (**100 pkt** do podziału)

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.

Zadanie 2 (30 pkt) Udowodnij, że klasa funkcji $\{T, v\}$ działających z $\mathcal{A} = \{0,1\}^n$ do $\mathcal{B} = \{0,1\}^r$ w następujący sposób (dodawanie modulo 2):

$$b = Ta + v \tag{2}$$

gdzie T jest binarną macierzą Toeplitza, a v dowolnym wektorem binarnym długości r, jest *strongly 2-universal family of hash functions*, czyli nadaje się do autentykacji. Uzasadnij, że bez dodania wektora v powyższa klasa chociaż jest *2-universal family of hash functions* to jednak nie jest *strongly 2-universal family of hash functions*, czyli nadaje się do wzmocnienia prywatności ale nie do autentykacji.

Zadanie 3 (40 pkt) Ani klasa zbudowana na wszystkich macierzach binarnych, ani klasa z zadania 2, nie spełniają podstawowego wymagania jakiego oczekujemy od procedury autentykacji, która mogłaby być praktyczna dla kwantowej kryptografii. Konieczne jest aby, klasa funkcji haszujących zawierała na tyle mało elementów, żeby ich określenie wymagało znacznie mniej niż liczba bitów klucza którą uzyskujemy w kwantowej kryptografii n. Obie powyższe klasy wymagają $> n$ bitów do procedury autentykacji co czyni je bezużytecznymi.

Istnieje jednak klasa która wymaga jedynie $\propto \log n$ bitów do określenia funkcji, i jest w związku z tym idealna dla naszych zastosowań. W celu wprowadzenia tej klasy konieczne jest jednak pewne złagodzenie wymagań odnośnie funkcji haszujących.

Definicja. Zbiór funkcji $\mathcal{H}$, działających z $\mathcal{A}$ do $\mathcal{B}$, stanowi *ϵ-strongly 2-universal class of hash functions* iff:

(i) $\forall_{a\in\mathcal{A}}\forall_{b\in\mathcal{B}}|\{h : h(a) = b\}| = \frac{|\mathcal{H}|}{|\mathcal{B}|}$

(ii) $\forall_{a_1\neq a_2\in\mathcal{A}}\forall_{b_1,b_2\in\mathcal{B}}|\{h : h(a_1) = b_1 \wedge h(a_2) = b_2\}| \leq \frac{\epsilon|\mathcal{H}|}{|\mathcal{B}|^2}$

Konstrukcja. Niech $\mathcal{A} = \{0,1\}^a$, $\mathcal{B} = \{0,1\}^b$. Rozważmy następującą konstrukcję klasy funkcji $\mathcal{H}$ z $\mathcal{A}$ do $\mathcal{B}$ służących do autentykacji.

(i) Weźmy $s = b + \log\log a$, oraz wedle gustu $\mathcal{H}_s$ która jest *strongly 2-universal class of hash functions* z $\{0,1\}^{2s}$ do $\{0,1\}^s$

(ii) Dzielimy wiadomość (a bitową), na $\lceil a/2s \rceil$ bloków $2s$ bitowych (jak się nie dzieli dopisujemy zera do wiadomości). Wybieramy przypadkową funkcję haszującą z $\mathcal{H}_s$ i stosujemy ją do każdego z bloków (do każdego bloku ta sama funkcja haszująca).

(iii) Iterujemy (ii), aż uzyskany wynikowy ciąg bitów ma długość s. Bierzemy pierwsze b bitów z wynikowego ciągu jako nasz MAC.

A teraz ty...

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.