CSE 539 Fall 2018
Quiz 2 9 – 27– 2018

Consider the following Encryption scheme on message space $\{0,1\}^n$, the set bit strings of length n where n is an even number

- Gen:
  $k_0 \leftarrow \{0,1\}^n$ choose k_1 uniformly at random from amongst all n-bit strings
  $k_1 \leftarrow \{0,1\}^{n/2}$ choose k_2 uniformly at random from amongst all n/2-bit strings
  $k \leftarrow \{ k_0 , k_1 || k_1\}$ one of k_0 or $k_1 || k_1$ is chosen at random and returned by Gen

- $Enc_k(m) = k \oplus m$

Show that this scheme is not perfectly secret by giving an adversary that can succeed in the perfect indistinguishability experiment with probability other than 1/2. You should specify the two messages that the adversary will send in the experiment and how the adversary decides the value of b' based on the cipher text it receives from the challenger and the probability of success for the adversary.

Solution

Here is an adversary that can succeed in the perfect indistinguishability experiment with probability other than ½

Adversary A:
send $m_0 = 0^n$ and $m_1 = 0^{n-1}1$
if the received cipher text c is of the form c'||c'
output b' = 0
else
outputs b' $\leftarrow \{0,1\}$

Pr[success] = Pr[b' =0 and b = 0] + Pr[b' = 1 and b = 1]

Pr[b' =0 and b = 0] =
1/2 x Pr[b' =0 | b = 0] =
1/2 x (Pr[b' = 0 and k_0 is chosen | b = 0] + Pr[b' = 0 and k_1 is chosen | b = 0]) =
1/2 x (1/2 x Pr[b' = 0 | k_0 is chosen and b = 0] + 1/2 x Pr[b' = 0 | k_1 is chosen and b = 0]) =
1/4 x (Pr[b' = 0 | k_0 is chosen and b = 0] + Pr[b' = 0 | k_1 is chosen and b = 0]) ≥
1/4 x (1/2 + 1) = 3/8

Note. Pr[b' = 0 | k_0 is chosen and b = 0] is no less than 1/2 because in the worst case b' is chosen randomly. In the best case, it is set to 0.

Pr[b' =1 and b = 1] =
1/2 x Pr[b' =1 | b = 1] =
1/2 x (Pr[b' = 1 and k_0 is chosen | b = 1] + Pr[b' = 1 and k_1 is chosen | b = 1]) =
1/2 x (1/2 x Pr[b' = 1 | k_0 is chosen and b = 1] + 1/2 x Pr[b' = 1 | k_1 is chosen and b = 1]) =
1/4 x (Pr[b' = 1 | k_0 is chosen and b = 1] + Pr[b' = 1 | k_1 is chosen and b = 1]) ≥
1/4 x ($(1-1/2^{n/2})$ x ½ + 1/2) = 1/4 x (1 - $1/2^{1+n/2}$)

Pr[success] ≥ 3/8 + 1/4 x (1 - $1/2^{1+n/2}$) ≥ 1/2