Indistinguishable Encryptions in the Presence of an Eavesdropper
Class Exercise—2/22/18

Assume $G$ is a PRG with input length $n$ and output length $n + 1$. Do the following encryption schemes $\Pi$ have indistinguishable encryptions in the presence of an eavesdropper? If yes, formally prove that if $G$ is a PRG then the scheme is secure. If not, present a ppt adversary $A$ and show that $\Pr[PrivK_{\text{eav}}_{A,\Pi}(n) = 1] \geq 1/2 + \rho(n)$ for some non-negligible $\rho()$.

1. $\Pi$ is defined as follows: $Gen$ outputs a random key $k$ of length $n$. To encrypt a message $m = m_1 || m_2$, where $m_1, m_2$ each have length $n + 1$, output $c := (c_1 || c_2) := G(k) \oplus m_1 || G(k) \oplus m_2$. To decrypt output $m_1 || m_2 = G(k) \oplus c_1 || G(k) \oplus c_2$.

   Not secure. Consider the following adversary $A$:
   A chooses $m_d = m_1^0 || m_2^0$ such that $m_1^0 \oplus m_2^0 \neq m_1^1 \oplus m_2^1$. $m = m_1^1 || m_2^1$.

   Given ciphertext $c^* = c_1^* || c_2^*$
   A checks whether $c_1^* \oplus c_2^* = m_1^0 \oplus m_2^0$
   If yes, output $b' = 0$
   o/w output $b' = 1$.

   $\Pi$ can be seen -hard $\Pr[PrivK_{\text{eav}}_{A,\Pi}(n) = 1] = 1$.

2. $\Pi$ is defined as follows: $Gen$ outputs a random key $k$ of length $n$. To encrypt a message $m$, where $m$ has length $n + 1$, output $c := G(k) \oplus m || 0^n$. To decrypt, output the first $n$ bits of $c \oplus (G(k)||0^n)$.

   Secure. We will give a proof by reduction.

   Assume the scheme is not secure. Then there exists a ppt $A \cdot c.t.$ $Pr[PrivK_{A,\Pi}(n) = 1] \geq 1/2 + \rho(n)$. We construct the following Distinguisher $D$:

   $D(w)$:
   1. Run $A(m)$ to obtain $m_0, m_1$
   2. Choose $b \in \{0,1\}^n$
   Output $c^* = \omega \oplus m_b || 0^n$ to $A$
   3. Run $A(c^*)$ to obtain $b'$
   4. If $b' = b$ output $1$ o/w output $0$.

   $\Pr[D(r) = 1] = \frac{1}{2}$ (by perfect secrecy)

   $\Pr[D(G(k) = 1] = \Pr[PrivK_{A,\Pi}(n) = 1] = \frac{1}{2} + \rho(n)$ (by hypothesis).

   So $\Pr[PrivK_{A,\Pi}(n) = 1] - \Pr[D(G(k) = 1] \geq 2\rho(n)$

   So $D$ is a distinguisher for $G$. \(\square\)