Eavesdropper

Wednesday, 22 February 2023 8:33 PM

Let Π be our construction. and A be a PPTM Adv. and define $\varepsilon(n)$

$$\varepsilon(n) = Pr\left[Priv k^{eav}_{A,\Pi}(n) = 1 \right] - \frac{1}{2}$$

Let D be a distinguisher

1.) Run $A(1^n)$ to obtain pair of messages $m_0, m_1 \in \{0,1\}^{l(n)}$

2.) Choose a random bit $b \leftarrow \{0,1\}$ Set $c := w \oplus m_b$

3.) Give c to A and obtain b'. Output 1 if $b' = b$, and output 0 otherwise

Let $\tilde{\Pi}$ be one-time pad.

$$Pr\left[Priv k^{eav}_{A,\tilde{\Pi}}(n) = 1 \right] = \frac{1}{2} \quad (1)$$

1.) If w is chosen uniformly at random from $\{0,1\}^{l(n)}$ then the view of A run as subroutine of D is distributed identically to the view of A in $Priv k^{eav}_{A,\tilde{\Pi}}(n)$

2.) If w is equal to $G(k)$ for $k \leftarrow \{0,1\}^n$ chosen uniformly then the view of A when run as a subroutine of D is distributed identically to the view of A in exp. $Priv k^{eav}_{A,\tilde{\Pi}}(n)$

$\therefore w \in \{0,1\}^{l(n)}$ chosen uniformly

$$Pr\left[D(w) = 1 \right] = Pr\left[Priv k^{eav}_{A,\tilde{\Pi}}(n) = 1 \right] = \frac{1}{2}$$

from (1)

$$Pr[D(w) = 1] = Pr[D(G(k)) = 1] = Pr\left[Priv k^{eav}_{A,\Pi}(n) = 1 \right] = \frac{1}{2} + \varepsilon(n)$$

Hence

$$\left| Pr[D(w) = 1] - Pr[D(G(s)) = 1] \right| = \varepsilon(n)$$

ε is negl. hence proved.