Chapter 10

Mingjia Huo

Problem 10.4. Show a concrete attack:

For adversary $\mathcal{A}$, he is given trans $= (s, u, w)$, then he can compute $t = u \oplus s$. In key-exchange experiment, if $\hat{k} = w \oplus u \oplus s$, then $\mathcal{A}$ outputs $b' = 0$; otherwise, $\mathcal{A}$ outputs $b' = 1$.

So if $b = 0$, then $\mathcal{A}$ always has $b' = b$; and if $b = 1$, $\mathcal{A}$ guesses right with probability $1 - 2^{-n}$.

$$\begin{aligned}\Pr[\mathrm{KE}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n) = 1] &= \frac{1}{2}\Pr[\mathrm{KE}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n) = 1 \mid b = 0] + \frac{1}{2}\Pr[\mathrm{KE}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n) = 1 \mid b = 1]\\ &= \frac{1}{2} + \frac{1}{2}(1 - 2^{-n})\\ &= 1 - \mathrm{negl}(n),\end{aligned}$$

which is significantly larger than $\frac{1}{2}$.