

PKE for $M = \{0,1\}$ from TDP $\Pi = (\text{Gen}^{\text{td}}, f, \text{Inv})$ with hc

$\text{Gen}(1^n)$: $\text{Gen}^{\text{td}}(1^n) \rightarrow \mathbb{I}, \text{td}$

output $\text{pk} = \mathbb{I}, \text{sk} = \text{td}$

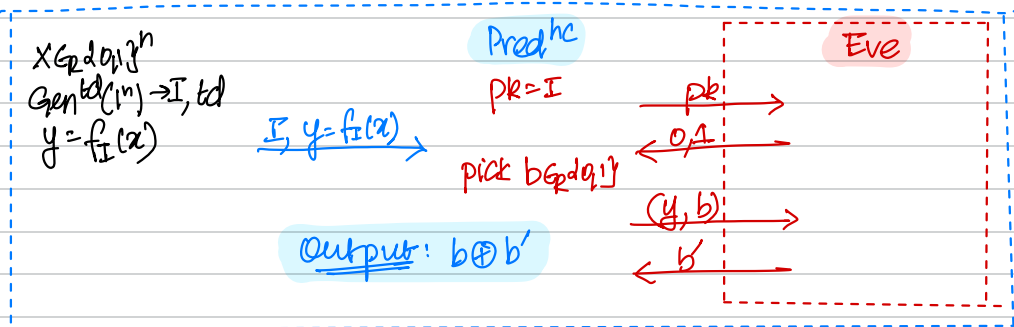
$\text{Enc}(\text{pk}, m)$: For bit $m \in \{0,1\}$, choose $r \in \{0,1\}^n$ and output
 $c = (f_{\mathbb{I}}(r), \text{hc}_{\mathbb{I}}(r) \oplus m)$

$\text{Dec}(\text{sk}, c = (r, s))$: $\because \text{sk} = \text{td}$ compute $b = \text{Inv}_{\text{td}}(r)$
 output $m = b \oplus s$.

Theorem 1 (Lecture 15): If Π is a TDP family with hc h_c then $(\text{Gen}, \text{Enc}, \text{Dec})$ is an IND-CPA PKE.

Proof:

Assume to the contrary that $\exists$ Eve against the bit-encryption we will build a Pred^{h_c} against the hc to show a contradiction.



Eq ① Now, $\Pr[\text{Pred}^{h_c}(I, y = f_I(x)) = 0 \mid \text{hc}_I(x) = 0] = \frac{1}{2} (\Pr[\text{Eve}(\text{pk}, (y, 0)) = 0 \mid \text{hc}_I(x) = 0] + \Pr[\text{Eve}(\text{pk}, (y, 1)) = 1 \mid \text{hc}_I(x) = 0])$

$\because b \oplus 0 = 0$ $\because b \oplus 1 = 1$ $\because b \oplus b = 0$

Eq ② Similarly, $\Pr[\text{Pred}^{h_c}(I, y = f_I(x)) = 1 \mid \text{hc}_I(x) = 1] = \frac{1}{2} (\Pr[\text{Eve}(\text{pk}, (y, 0)) = 1 \mid \text{hc}_I(x) = 1] + \Pr[\text{Eve}(\text{pk}, (y, 1)) = 0 \mid \text{hc}_I(x) = 1])$

$\because b \oplus 0 = 1$ $\because b \oplus 1 = 0$

$$\begin{aligned}
 & \Pr[\text{Eve wins in IND-CPA game}] \\
 &= \frac{1}{2} \left(\Pr[\text{Eve}(pk, (y, b)) = 0 \mid (y, b) \text{ encrypts } 0] + \Pr[\text{Eve}(pk, (y, b)) = 1 \mid (y, b) \text{ encrypts } 1] \right) \quad (\text{by definition}) \\
 & \quad \quad \quad \downarrow \quad \quad \quad \downarrow \\
 & \quad \quad \quad b = h_G(x) \quad \quad \quad b = h_G(x) \oplus 1 \\
 \text{Eq ③} \quad &= \frac{1}{2} \left(\Pr[\text{Eve}(pk, (y, 0)) = 0 \mid h_{G_I}(x) = 0] + \Pr[\text{Eve}(pk, (y, 1)) = 0 \mid h_{G_I}(x) = 1] \right) \\
 \text{Eq ④} \quad &= \frac{1}{2} \left(\Pr[\text{Eve}(pk, (y, 0)) = 1 \mid h_{G_I}(x) = 1] + \Pr[\text{Eve}(pk, (y, 1)) = 1 \mid h_{G_I}(x) = 0] \right)
 \end{aligned}$$

Note that $\text{Eq ③} + \text{Eq ④} = \text{Eq ①} + \text{Eq ②}$

$$\begin{aligned}
 & \text{So } \Pr[\text{Eve wins in IND-CPA game}] \\
 &= \frac{1}{2} \left(\Pr[\text{Pred}^{h_G}(I, y = f_I(x)) = 0 \mid h_{G_I}(x) = 0] + \Pr[\text{Pred}^{h_G}(I, y) = 1 \mid h_{G_I}(x) = 1] \right) \\
 &= \Pr[\text{Pred}^{h_G}(I, f_I(x)) = h_{G_I}(x)]
 \end{aligned}$$