

Homework 9

1. Libraries:

$\mathcal{L}_{\text{cca-L}}^\Sigma$	$\mathcal{L}_{\text{cca-R}}^\Sigma$
$k_1 \leftarrow \Sigma_1.\text{KeyGen}$ $k_2 \leftarrow \Sigma_2.\text{KeyGen}$ $S := \emptyset$	$k_1 \leftarrow \Sigma_1.\text{KeyGen}$ $k_2 \leftarrow \Sigma_2.\text{KeyGen}$ $S := \emptyset$
$\text{EAVESDROP}(m_L, m_R)$ <hr/> if $ m_L \neq m_R $ return err $c_1 := \Sigma_1.\text{Enc}(k_1, m_L)$ $c_2 := \Sigma_2.\text{Enc}(k_2, m_L)$ $S := S \cup \{(c_1, c_2)\}$ return (c_1, c_2)	$\text{EAVESDROP}(m_L, m_R)$ <hr/> if $ m_L \neq m_R $ return err $c_1 := \Sigma_1.\text{Enc}(k_1, m_R)$ $c_2 := \Sigma_2.\text{Enc}(k_2, m_R)$ $S := S \cup \{(c_1, c_2)\}$ return (c_1, c_2)
$\text{DEC}((c_1, c_2))$ <hr/> if $(c_1, c_2) \in S$ return err $m_1 := \Sigma_1.\text{Dec}(k_1, c_1)$ $m_2 := \Sigma_2.\text{Dec}(k_2, c_2)$ if $(m_1 == m_2)$ return m_1 else return err	$\text{DEC}((c_1, c_2))$ <hr/> if $(c_1, c_2) \in S$ return err $m_1 := \Sigma_1.\text{Dec}(k_1, c_1)$ $m_2 := \Sigma_2.\text{Dec}(k_2, c_2)$ if $(m_1 == m_2)$ return m_1 else return err

Calling Program:

A
choose $m \neq m', t \neq 0^\lambda$ $x, y := \text{EAVESDROP}(m, m')$ $\hat{m} := \text{DEC}(x \oplus t, y)$ if $(\hat{m} == x \oplus t)$: return 1 else return 0

$$\Pr[A \diamond \text{cca-L} = 1] = 1$$

$$\Pr[A \diamond \text{cca-R} = 1] = 0$$

$$\text{Advantage: } 1 - 0 = 1$$

2. Encryption:

$\begin{array}{l} \text{Enc}(k, m) : \\ r \leftarrow \{0, 1\}^\lambda \\ x := F(k, m \oplus r) \oplus r \\ \text{return } (r, x) \end{array}$

Decryption:

$\begin{array}{l} \text{Dec}(k, c) \\ x := r \oplus F^{-1}(c) \\ \text{return } x \end{array}$
--

Libraries:

$\begin{array}{c} \mathcal{L}_{\text{cca-L}}^\Sigma \\ \hline \text{EAVESDROP}(m_L, m_R) \\ r \leftarrow \{0, 1\}^\lambda \\ x := F(k, m_L \oplus r) \oplus r \\ \text{return } (r, x) \end{array}$	$\begin{array}{c} \mathcal{L}_{\text{cca-R}}^\Sigma \\ \hline \text{EAVESDROP}(m_L, m_R) \\ r \leftarrow \{0, 1\}^\lambda \\ x := F(k, m_R \oplus r) \oplus r \\ \text{return } (r, x) \end{array}$
---	---

Calling Program:

$\begin{array}{c} A \\ \text{choose } m \neq m', t \neq 0^\lambda \\ r1, x := \text{EAVESDROP}(m, m) \\ r2, x' := \text{EAVESDROP}(m, m') \\ a := \text{Dec}(r1, x \oplus t) \\ a' := \text{Dec}(r2, x' \oplus t) \\ \text{if } (a == a') \\ \quad \text{return } 1 \\ \text{return } 0 \end{array}$
--

$$\Pr[A \diamond \text{cca-L} = 1] = 1$$

$$\Pr[A \diamond \text{cca-R} = 1] = 0$$

$$\text{Advantage: } 1 - 0 = 1$$