Gauge Hartwell

4 February, 2021

CS427

Homework 8

1. a)

$$\underline{Dec(k, c_1||...||m_\ell)}$$
$$c_0 \leftarrow \{0,1\}^\lambda$$
$$\text{for } i = 1 \text{ to } \ell:$$
$$\quad m_i := F'(k, c_i \oplus c_{i-1})$$
$$\text{return } m'_0||m_1||...||m_\ell$$

b)

Libraries:

$\mathcal{L}^{\Sigma}_{\text{cpa-real}}$

$$k \leftarrow \Sigma.KeyGen$$
$$\underline{CHALLENGE(m \in \Sigma.\mathcal{M}):}$$
$$\quad c := \Sigma.Enc(k, m)$$
$$\text{return } c$$

$\mathcal{L}^{\Sigma}_{\text{cpa-rand}}$

$$c \leftarrow \Sigma.C(|m|)$$
$$\text{return } c$$

Calling Program:

$$\underline{Call}$$
$$m \leftarrow \{0,1\}^\lambda$$
$$a||b := CHALLENGE(m)$$
$$x||y := CHALLENGE(m)$$
$$\text{if } a \oplus b == x \oplus y$$
$$\quad \text{return } 1$$
$$\text{return } 0$$

Pr[Call ◊ cpa-real = 1] = 1

Pr[Call ◊ cpa-rand = 1] = $1/2^{\lambda}$

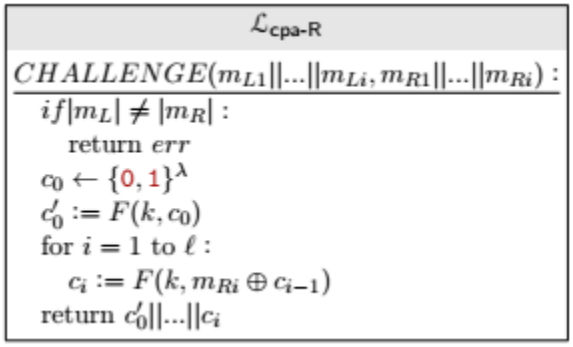
Advantage: $1 - 1/1^{\lambda}$, non-negligible

2.

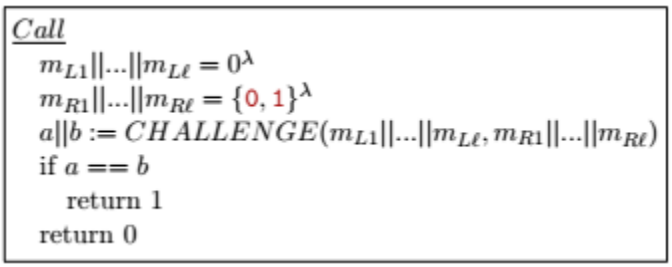
Libraries:

$\mathcal{L}_{\text{cpa-L}}$

$$\underline{CHALLENGE(m_{L1}||...||m_{Li}, m_{R1}||...||m_{Ri}):}$$
$$if |m_L| \neq |m_R|:$$
$$\quad \text{return } err$$
$$c_0 \leftarrow \{0,1\}^\lambda$$
$$c'_0 := F(k, c_0)$$
$$\text{for } i = 1 \text{ to } \ell:$$
$$\quad c_i := F(k, m_{Li} \oplus c_{i-1})$$
$$\text{return } c'_0||...||c_i$$



Calling program:



Pr[Call ◊ cpa-real = 1] = 1

Pr[Call ◊ cpa-rand = 1] = 0

Advantage: 1-0 = 1, non-negligible