malickc@oregonstate.edu

## CS 427, Assignment 3

## Cody Malick

February 2, 2017

```
1
1.1
1.2
1.3
```

 $A \diamond \begin{bmatrix} \frac{\text{CHALLENGE}(m_1 \cdots m_{\ell}):}{r := \text{SAMP}()} \\ c_0 := r \\ \text{for } i = 1 \text{ to } \ell: \\ r := \text{QUERY}(r) \\ c_i := r \oplus m_i \\ \text{return } c_0 c_1 \cdots c_{\ell} \end{bmatrix} \diamond \begin{bmatrix} T := \text{empty} \\ \frac{\text{QUERY}(r):}{\text{if } T[r] \text{ undefined:}} \\ T[r] := \text{SAMP}() \\ \text{return } T[r] \end{bmatrix} \diamond \begin{bmatrix} \frac{\text{SAMP}():}{s \leftarrow \{0, 1\}^{\lambda}} \\ \text{return } s \end{bmatrix}$ 

 $\mathcal{L}_{\mathsf{cpa-L}}^{\Sigma}$   $k \leftarrow \Sigma.\mathsf{KeyGen}$   $\frac{\mathsf{CHALLENGE}(m_L, m_R):}{c := \Sigma.\mathsf{Enc}(k, \textcolor{red}{m_L})}$  return c

 $\mathcal{L}_{\mathsf{left}} \equiv \mathcal{L}_{\mathsf{right}} \Leftrightarrow \forall A : \Pr[A \diamond \mathcal{L}_{\mathsf{left}} \text{ outputs } 1] = \Pr[A \diamond \mathcal{L}_{\mathsf{right}} \text{ outputs } 1]$   $\mathcal{L}_{\mathsf{left}} \approxeq \mathcal{L}_{\mathsf{right}} \Leftrightarrow \forall \text{ poly-time } A : \Pr[A \diamond \mathcal{L}_{\mathsf{left}} \text{ outputs } 1] \approx \Pr[A \diamond \mathcal{L}_{\mathsf{right}} \text{ outputs } 1]$ 

```
 \begin{array}{ll} \underline{ \text{KeyGen:} } & \underline{ \frac{ \text{Enc}(k,m):}{r \leftarrow \{\textbf{0},\textbf{1}\}^{\lambda} } \\ \text{return } k \end{array} } \begin{array}{ll} \underline{ \frac{ \text{Enc}(k,m):}{r \leftarrow \{\textbf{0},\textbf{1}\}^{\lambda} } \\ x := F(k,r) \oplus m \\ \text{return } (r,x) \end{array} } \begin{array}{ll} \underline{ \frac{ \text{Dec}(k,(r,x)):}{m := F(k,r) \oplus x} } \\ \text{return } m \end{array}
```

 $\begin{aligned} \frac{H(s):}{x := G(s)} \\ y := G(x_{\mathsf{right}}) \\ \text{return } x_{\mathsf{left}} \| y \end{aligned}$