malickc@oregonstate.edu

CS 427, Assignment 3

Cody Malick

February 2, 2017

1

1.1

1.2

1.3

2

$A \diamond$

```
CHALLENGE($m_1 \cdots m_\ell$):
    $r :=$ SAMP()
    $c_0 := r$
    for $i = 1$ to $\ell$:
        $r :=$ QUERY($r$)
        $c_i := r \oplus m_i$
    return $c_0 c_1 \cdots c_\ell$
```

$\diamond$

```
$T :=$ empty

QUERY($r$):
    if $T[r]$ undefined:
        $T[r] :=$ SAMP()
    return $T[r]$
```

$\diamond$

```
SAMP():
    $s \leftarrow \{0, 1\}^\lambda$
    return $s$
```

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

$k \leftarrow \Sigma$.KeyGen

CHALLENGE($m_L, m_R$):
    $c := \Sigma$.Enc($k$, $m_L$)
    return $c$
```

$\mathcal{L}_{\text{left}} \equiv \mathcal{L}_{\text{right}} \Leftrightarrow \forall A : \Pr[A \diamond \mathcal{L}_{\text{left}} \text{ outputs } 1] = \Pr[A \diamond \mathcal{L}_{\text{right}} \text{ outputs } 1]$

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

```
$\underline{\mathsf{KeyGen}:}$
    $k \leftarrow \{0,1\}^\lambda$
    return $k$
```

```
$\underline{\mathsf{Enc}(k,m):}$
    $r \leftarrow \{0,1\}^\lambda$
    $x := F(k,r) \oplus m$
    return $(r,x)$
```

```
$\underline{\mathsf{Dec}(k,(r,x)):}$
    $m := F(k,r) \oplus x$
    return $m$
```

```
$\underline{H(s):}$
    $x := G(s)$
    $y := G(x_{\mathsf{right}})$
    return $x_{\mathsf{left}} \| y$
```