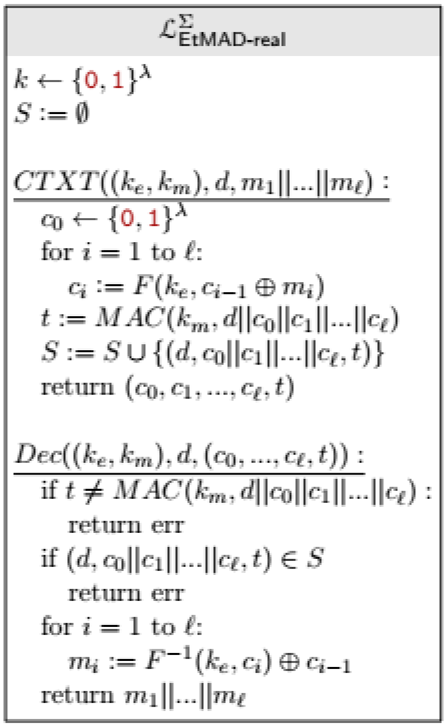
Gauge Hartwell

20 February, 2021

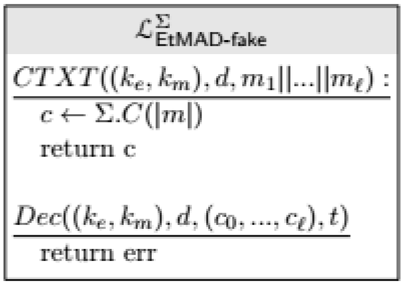
CS427

Homework 12

1. Libraries

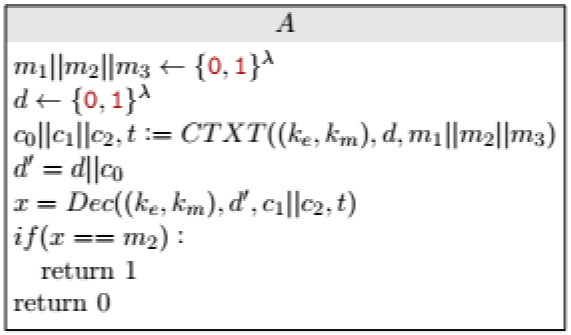


```
$\mathcal{L}^{\Sigma}_{\text{EtMAD-real}}$
$k \leftarrow \{0,1\}^\lambda$
$S := \emptyset$

$CTXT((k_e, k_m), d, m_1||...||m_\ell):$
    $c_0 \leftarrow \{0,1\}^\lambda$
    for $i = 1$ to $\ell$:
        $c_i := F(k_e, c_{i-1} \oplus m_i)$
    $t := MAC(k_m, d||c_0||c_1||...||c_\ell)$
    $S := S \cup \{(d, c_0||c_1||...||c_\ell, t)\}$
    return $(c_0, c_1, ..., c_\ell, t)$

$Dec((k_e, k_m), d, (c_0, ..., c_\ell, t)):$
    if $t \neq MAC(k_m, d||c_0||c_1||...||c_\ell)$ :
        return err
    if $(d, c_0||c_1||...||c_\ell, t) \in S$
        return err
    for $i = 1$ to $\ell$:
        $m_i := F^{-1}(k_e, c_i) \oplus c_{i-1}$
    return $m_1||...||m_\ell$
```



```
$\mathcal{L}^{\Sigma}_{\text{EtMAD-fake}}$
$CTXT((k_e, k_m), d, m_1||...||m_\ell):$
    $c \leftarrow \Sigma.C(|m|)$
    return c

$Dec((k_e, k_m), d, (c_0, ..., c_\ell), t)$
    return err
```

Calling Program:



```
$A$
$m_1||m_2||m_3 \leftarrow \{0,1\}^\lambda$
$d \leftarrow \{0,1\}^\lambda$
$c_0||c_1||c_2, t := CTXT((k_e, k_m), d, m_1||m_2||m_3)$
$d' = d||c_0$
$x = Dec((k_e, k_m), d', c_1||c_2, t)$
$if(x == m_2):$
    return 1
return 0
```

Pr[A ◊ EtMAD-real = 1] = 1

Pr[A ◊ EtMAD-fake = 1] = 0

Advantage: 1 – 0 = 1, non-negligible

2. $m_0 = m_1 = 1$
   $H(s, m_0||m_1) = s^2 + s + 1$
   $H(s, c_0||0) = s^2 + c_0$
   $s^2 + c_0 = s^2 + s + 1$
   $c_0 = s + 1$
   $s^2 + s + 1 = s^2 + s + 1$

3. $M_0 = 0$, $m_1 = 1$
   $H(s, m_0||m_1) = s^2 + 1$
   $s^2 + 1 = 17$
   $s^2 = 16$
   $s = 4$