# Hybrid Security Proofs

HW1 due Friday ★

security of OTP (using fact that ctxt distribution is uniform)

## Another Example Hybrid Proof: [Ex 2.4]

Dumb OTP:

c, concatenated with 00

```
KeyGen:
    $k \leftarrow \{0,1\}^\lambda$
    ret $k$

Enc(k, m):
    $c = k \oplus m$
    return $\underbrace{c \| 00}_{\text{ctxt}}$

Dec(k, c):
    remove last 2 chars of c
    ret $k \oplus c$
```

Is it still one-time secure? YES

Does it still have uniform ctxts?

NO, if $C = \{0,1\}^{\lambda+2}$

YES, if $C = \{\text{strings ending in } 00\}$

## Want to show:

```
QUERY($m_L$, $m_R$):
    $k \leftarrow \{0,1\}^\lambda$
    $c = k \oplus m_L$
    $c' = c \| 00$
    return $c'$
```

$\equiv$

```
QUERY($m_L$, $m_R$):
    $k \leftarrow \{0,1\}^\lambda$
    $c = k \oplus m_R$
    $c' = c \| 00$
    return $c'$
```

```
QUERY($m_L, m_R$):
    $k \leftarrow \{0,1\}^\lambda$
    $c = k \oplus m_L$
    $c' = c \| 00$
    return $c'$
```

$\equiv$

factor out

```
QUERY($m_L, m_R$):
    $c = \text{BLAH}(m_L, m_R)$
    $c' = c \| 00$
    return $c'$
```

$\diamond$

```
BLAH($m_L, m_R$)
    $k \leftarrow \{0,1\}^\lambda$
    $c = k \oplus m_L$
    return $c$
```

$\mathcal{L}^{\text{OTP}}_{\text{OTS-L}}$

because OTP has one-time security

$\equiv$

```
QUERY($m_L, m_R$):
    $c = \text{BLAH}(m_L, m_R)$
    $c' = c \| 00$
    return $c'$
```

$\diamond$

```
BLAH($m_L, m_R$)
    $k \leftarrow \{0,1\}^\lambda$
    $c = k \oplus m_R$
    return $c$
```

$\mathcal{L}^{\text{OTP}}_{\text{OTS-R}}$

inline

$\equiv$

```
QUERY($m_L, m_R$):
    $k \leftarrow \{0,1\}^\lambda$
    $c = k \oplus m_R$
    $c' = c \| 00$
    return $c'$
```

QED ✓

More generally:

If $\text{Enc}(k,m)$ is a "good encryption scheme" (one-time sec)

then $\text{Enc}(k,m) \| 00$ is too