# 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:**

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

**Enc$(k, m)$:**
$c = k \oplus m$
return $c \| 00$

c, concatenated with 00

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

ctxt

Is it still one-time secure?

Does it still have uniform ctxts?

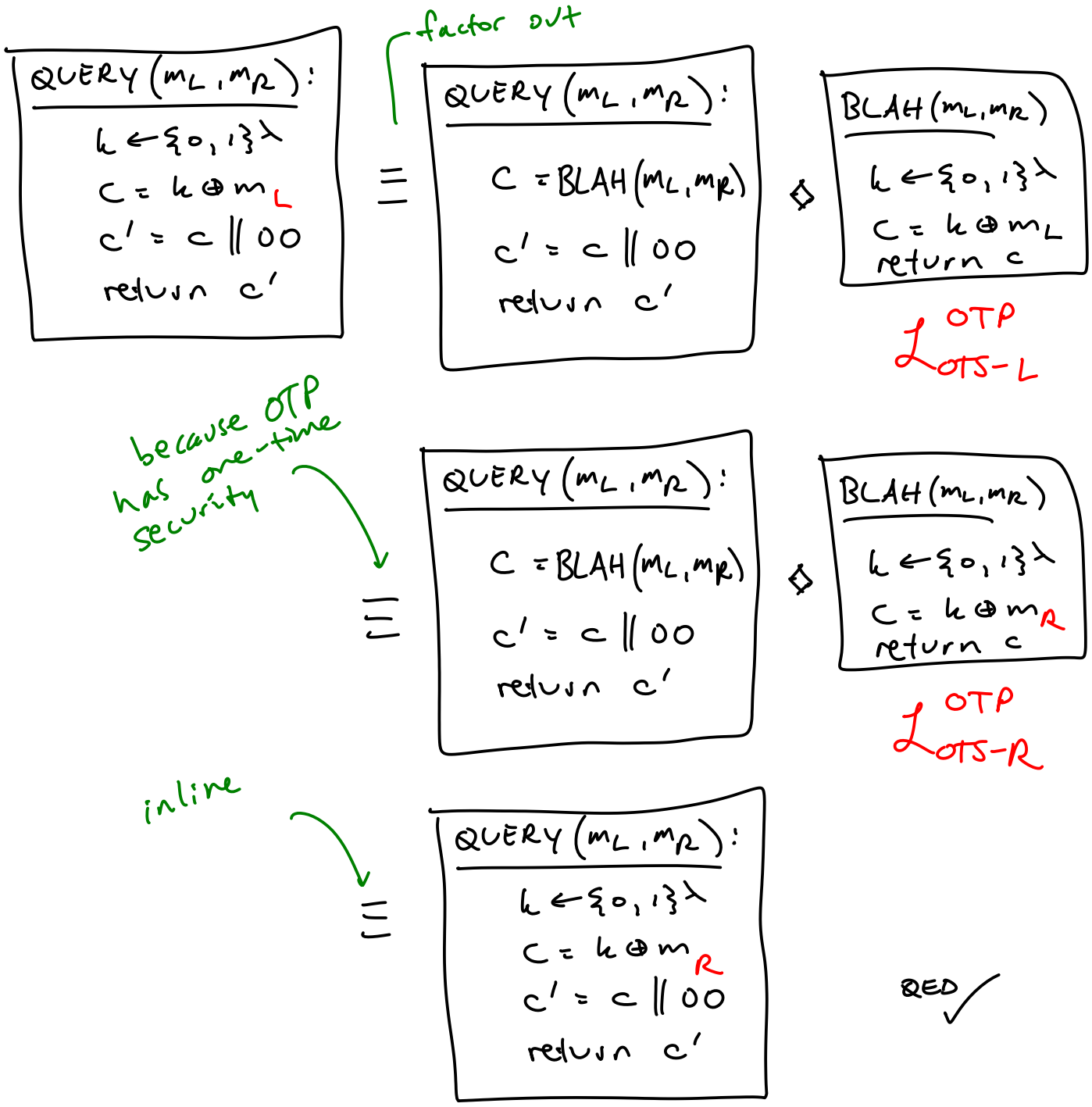
YES

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

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

## Want to show:

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




More generally:

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

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