

# One-time pad security:

OTP:			
$\mathcal{K} = \{0, 1\}^\lambda$	<u>KeyGen:</u>	<u>Enc(<math>k, m</math>):</u>	<u>Dec(<math>k, c</math>):</u>
$\mathcal{M} = \{0, 1\}^\lambda$	$k \leftarrow \mathcal{K}$	return $k \oplus m$	return $k \oplus c$
$\mathcal{C} = \{0, 1\}^\lambda$	return $k$		

## Claim:

OTP satisfies one-time secrecy. That is,  $\mathcal{L}_{\text{ots-L}}^{\text{OTP}} \equiv \mathcal{L}_{\text{ots-R}}^{\text{OTP}}$ .

We will **use** the fact that OTP ciphertexts are uniformly distributed:

$$\frac{\text{CTXT}(m \in \{0, 1\}^\lambda):}{\begin{array}{l} k \leftarrow \{0, 1\}^\lambda \\ \text{return } k \oplus m \end{array}} \equiv \frac{\text{CTXT}(m \in \{0, 1\}^\lambda):}{\begin{array}{l} c \leftarrow \{0, 1\}^\lambda \\ \text{return } c \end{array}}$$

# Security proof


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

QUERY( $m_L, m_R \in \text{OTP}.\mathcal{M}$ ):

$k \leftarrow \text{OTP.KeyGen}$

$c := \text{OTP.Enc}(k, m_L)$

return  $c$

Starting point is  $\mathcal{L}_{\text{ots-L}}^{\text{OTP}}$ .

# Security proof


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

QUERY( $m_L, m_R \in \text{OTP}.\mathcal{M}$ ):

$k \leftarrow \text{OTP.KeyGen}$

$c := \text{OTP.Enc}(k, m_L)$

return  $c$

Starting point is  $\mathcal{L}_{\text{ots-L}}^{\text{OTP}}$ . Fill in details of OTP

# Security proof



$\mathcal{L}_{\text{ots-L}}^{\text{OTP}}$	
QUERY( $m_L, m_R \in \{0, 1\}^\lambda$ ):	
<hr/>	
$k \leftarrow \{0, 1\}^\lambda$	
$c := k \oplus m_L$	
return $c$	

Starting point is  $\mathcal{L}_{\text{ots-L}}^{\text{OTP}}$ . Fill in details of OTP

# Security proof

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

QUERY( $m_L, m_R \in \{0, 1\}^\lambda$ ):

 $k \leftarrow \{0, 1\}^\lambda$  $c := k \oplus m_L$ return  $c$ 

Starting point is  $\mathcal{L}_{\text{ots-L}}^{\text{OTP}}$ . Fill in details of OTP

# Security proof



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

QUERY( $m_L, m_R \in \{0, 1\}^\lambda$ ):

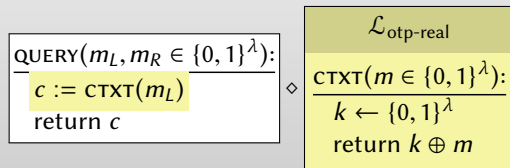
$k \leftarrow \{0, 1\}^\lambda$

$c := k \oplus m_L$

return  $c$

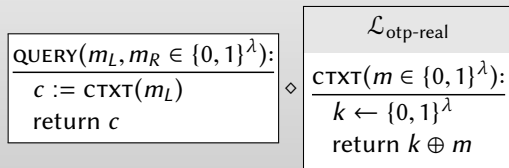
These statements appear also in  $\mathcal{L}_{\text{otp-real}}$ .

# Security proof



Factor out so that  $\mathcal{L}_{\text{otp-real}}$  appears.

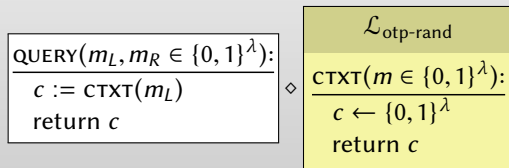
# Security proof



Factor out so that  $\mathcal{L}_{\text{otp-real}}$  appears.

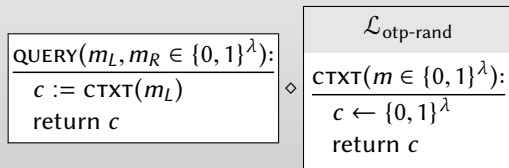


# Security proof



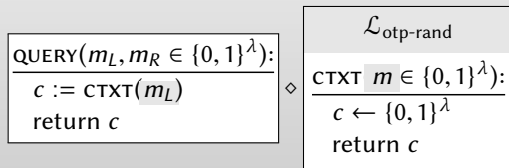
$\mathcal{L}_{\text{otp-real}}$  can be replaced with  $\mathcal{L}_{\text{otp-rand}}$ .

# Security proof



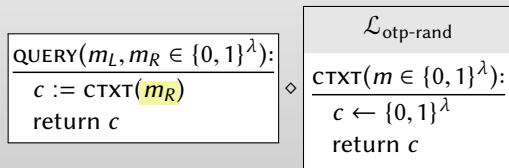
$\mathcal{L}_{\text{otp-real}}$  can be replaced with  $\mathcal{L}_{\text{otp-rand}}$ .

# Security proof



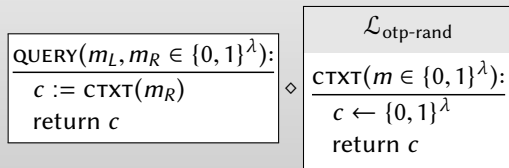
Argument to CTXT is never used!

# Security proof



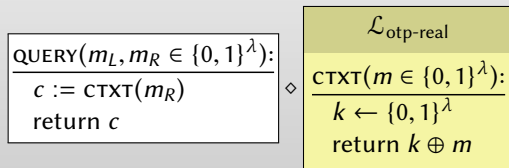
Unused argument can be changed to  $m_R$ .

# Security proof



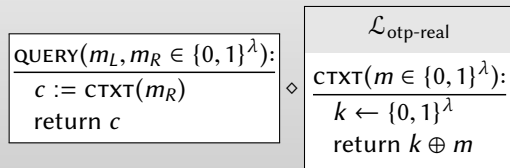
Unused argument can be changed to  $m_R$ .

# Security proof



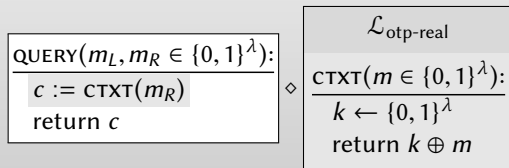
$\mathcal{L}_{\text{otp-rand}}$  can be replaced with  $\mathcal{L}_{\text{otp-real}}$ .

# Security proof



$\mathcal{L}_{\text{otp-rand}}$  can be replaced with  $\mathcal{L}_{\text{otp-real}}$ .

# Security proof



Inline the subroutine call.



# Security proof



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

Inline the subroutine call.

# Security proof



QUERY( $m_L, m_R \in \{0, 1\}^\lambda$ ):

$k \leftarrow \{0, 1\}^\lambda$

$c := k \oplus m_R$

return  $c$

Inline the subroutine call.

# Security proof



QUERY( $m_L, m_R \in \{0, 1\}^\lambda$ ):

$k \leftarrow \{0, 1\}^\lambda$

$c := k \oplus m_R$

return  $c$

This happens to be  $\mathcal{L}_{\text{ots-R}}^{\text{OTP}}$ .

# Security proof



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

This happens to be  $\mathcal{L}_{\text{ots-R}}^{\text{OTP}}$ .

# Security proof



$\mathcal{L}_{\text{ots-R}}^{\text{OTP}}$
<u>QUERY(<math>m_L, m_R \in \text{OTP}.\mathcal{M}</math>):</u>
$k \leftarrow \text{OTP.KeyGen}$
$c := \text{OTP.Enc}(k, m_R)$
return $c$

This happens to be  $\mathcal{L}_{\text{ots-R}}^{\text{OTP}}$ .

# Security proof


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

QUERY( $m_L, m_R \in \text{OTP}.\mathcal{M}$ ):

$k \leftarrow \text{OTP.KeyGen}$

$c := \text{OTP.Enc}(k, m_R)$

return  $c$

This happens to be  $\mathcal{L}_{\text{ots-R}}^{\text{OTP}}$ .

# Summary

We showed:

$\mathcal{L}_{\text{ots-L}}^{\text{OTP}}$		$\mathcal{L}_{\text{ots-R}}^{\text{OTP}}$
<div style="border-bottom: 1px solid black; margin-bottom: 5px;"><math>\text{QUERY}(m_L, m_R \in \text{OTP}.\mathcal{M}):</math></div> <div><math>k \leftarrow \text{OTP.KeyGen}</math> <math>c := \text{OTP.Enc}(k, m_L)</math> return <math>c</math></div>	$\equiv \dots \equiv$	<div style="border-bottom: 1px solid black; margin-bottom: 5px;"><math>\text{QUERY}(m_L, m_R \in \text{OTP}.\mathcal{M}):</math></div> <div><math>k \leftarrow \text{OTP.KeyGen}</math> <math>c := \text{OTP.Enc}(k, m_R)</math> return <math>c</math></div>

So OTP satisfies one-time secrecy.