

# Uniform ciphertexts implies one-time secrecy:

Want to show:

If  $\Sigma$  has uniform ciphertexts then it has one-time secrecy, too.

# Uniform ciphertexts implies one-time secrecy:

Want to show:

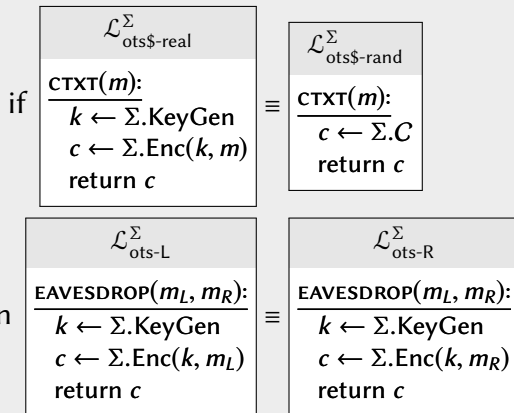
If  $\Sigma$  has **uniform ciphertexts** then it has one-time secrecy, too.

$$\text{if } \frac{\mathcal{L}_{\text{ots\$-real}}^{\Sigma}}{\text{CTXT}(m):} \begin{array}{l} k \leftarrow \Sigma.\text{KeyGen} \\ c \leftarrow \Sigma.\text{Enc}(k, m) \\ \text{return } c \end{array} \equiv \frac{\mathcal{L}_{\text{ots\$-rand}}^{\Sigma}}{\text{CTXT}(m):} \begin{array}{l} c \leftarrow \Sigma.C \\ \text{return } c \end{array}$$

# Uniform ciphertexts implies one-time secrecy:

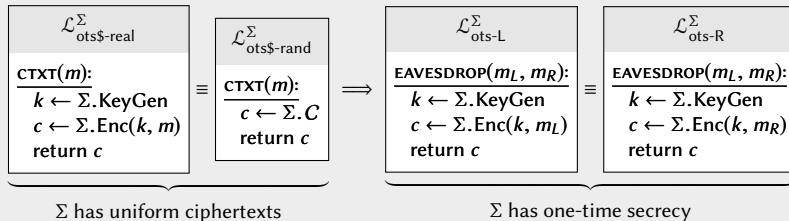
## Want to show:

If  $\Sigma$  has uniform ciphertexts then **it has one-time secrecy**, too.



# Overview:

## Want to show:



## Standard hybrid technique:

- ▶ Starting with  $\mathcal{L}_{\text{ots-L}}^\Sigma$ , make a sequence of small modifications
- ▶ Each modification has no effect on calling program
  - ▶ **Modifications can include swapping  $\mathcal{L}_{\text{ots-real}}^\Sigma$  &  $\mathcal{L}_{\text{ots-rand}}^\Sigma$ !**
- ▶ Sequence of modifications ends with  $\mathcal{L}_{\text{ots-R}}^\Sigma$

# Security proof

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

EAVESDROP( $m_L, m_R$ ):

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

$c \leftarrow \Sigma.\text{Enc}(k, m_L)$

return  $c$

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

# Security proof



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

**EAVESDROP( $m_L, m_R$ ):**

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

$c \leftarrow \Sigma.\text{Enc}(k, m_L)$

return  $c$

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

# Security proof



$\text{EAVESDROP}(m_L, m_R):$   
 $c := \text{CTXT}(m_L)$   
return  $c$



$\mathcal{L}_{\text{ots\$-real}}^\Sigma$   
 $\text{CTXT}(m):$   
 $k \leftarrow \Sigma.\text{KeyGen}$   
 $c \leftarrow \Sigma.\text{Enc}(k, m)$   
return  $c$

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

# Security proof



$\text{EAVESDROP}(m_L, m_R):$
$c := \text{CTXT}(m_L)$
return $c$

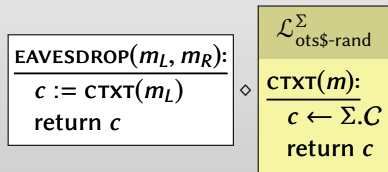


$\mathcal{L}_{\text{ots\$-real}}^{\Sigma}$
$\text{CTXT}(m):$
$k \leftarrow \Sigma.\text{KeyGen}$
$c \leftarrow \Sigma.\text{Enc}(k, m)$
return $c$

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

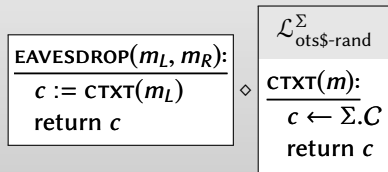


# Security proof



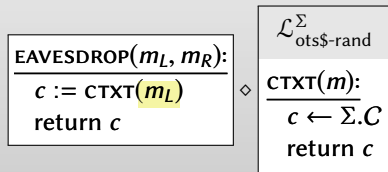
$\mathcal{L}_{\text{ots\$-real}}$  can be replaced with  $\mathcal{L}_{\text{ots\$-rand}}$ .

# Security proof



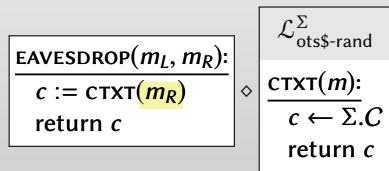
$\mathcal{L}_{\text{ots\$-real}}$  can be replaced with  $\mathcal{L}_{\text{ots\$-rand}}$ .

# Security proof



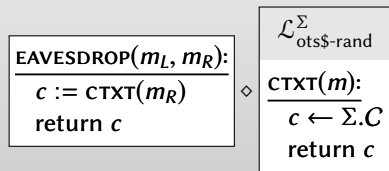
Argument to CTXT is never used!

# Security proof



Unused argument can be changed to  $m_R$ .

# Security proof



Unused argument can be changed to  $m_R$ .

# Security proof



$\text{EAVESDROP}(m_L, m_R):$
$c := \text{CTXT}(m_R)$
return $c$



$\mathcal{L}_{\text{ots\$-real}}^{\Sigma}$
$\text{CTXT}(m):$
$k \leftarrow \Sigma.\text{KeyGen}$
$c \leftarrow \Sigma.\text{Enc}(k, m)$
return $c$

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

# Security proof



$\text{EAVESDROP}(m_L, m_R):$
$c := \text{CTXT}(m_R)$
return $c$



$\mathcal{L}_{\text{ots\$-real}}^{\Sigma}$
$\text{CTXT}(m):$
$k \leftarrow \Sigma.\text{KeyGen}$
$c \leftarrow \Sigma.\text{Enc}(k, m)$
return $c$

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

# Security proof



EAVESDROP( $m_L, m_R$ ):  
 $c := \text{CTXT}(m_R)$   
return  $c$



$\mathcal{L}_{\text{ots\$-real}}^\Sigma$

CTXT( $m$ ):  
 $k \leftarrow \Sigma.\text{KeyGen}$   
 $c \leftarrow \Sigma.\text{Enc}(k, m)$   
return  $c$

Inline the subroutine call.



# Security proof ● ● ● ● ● ●

EAVESDROP( $m_L, m_R$ ):

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

$c \leftarrow \Sigma.\text{Enc}(k, m_R)$

return  $c$

Inline the subroutine call.

## Security proof ● ● ● ● ● ●

EAVESDROP( $m_L, m_R$ ):

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

$c \leftarrow \Sigma.\text{Enc}(k, m_R)$

return  $c$

Inline the subroutine call.

# Security proof ●●●●●●

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

EAVESDROP( $m_L, m_R$ ):

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

$c \leftarrow \Sigma.\text{Enc}(k, m_R)$

return  $c$

This happens to be  $\mathcal{L}_{\text{ots-R}}^{\Sigma}$ . We're done! ■