Uniform ciphertexts implies one-time secrecy:

Want to show:

If Σ has uniform ciphertexts then it has one-time secrecy, too.

Uniform ciphertexts implies one-time secrecy:

Want to show:

If Σ **has uniform ciphertexts** then it has one-time secrecy, too.

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

Uniform ciphertexts implies one-time secrecy:

Want to show:

If Σ has uniform ciphertexts then **it has one-time secrecy**, too.

if

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

$\equiv$

$$\mathcal{L}^{\Sigma}_{\text{ots\$-rand}}: \quad \underline{\textsc{ctxt}(m):} \quad c \leftarrow \Sigma.\mathcal{C}; \quad \text{return } c$$

then

$$\mathcal{L}^{\Sigma}_{\text{ots-L}}: \quad \underline{\textsc{eavesdrop}(m_L, m_R):} \quad k \leftarrow \Sigma.\text{KeyGen}; \quad c \leftarrow \Sigma.\text{Enc}(k, m_L); \quad \text{return } c$$

$\equiv$

$$\mathcal{L}^{\Sigma}_{\text{ots-R}}: \quad \underline{\textsc{eavesdrop}(m_L, m_R):} \quad k \leftarrow \Sigma.\text{KeyGen}; \quad c \leftarrow \Sigma.\text{Enc}(k, m_R); \quad \text{return } c$$

Overview:

Want to show:

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

$\equiv$

$\mathcal{L}^{\Sigma}_{\text{ots\$-rand}}$
$\underline{\textsc{ctxt}(m):}$
$c \leftarrow \Sigma.\mathcal{C}$
return c

Σ has uniform ciphertexts

$\Longrightarrow$

$\mathcal{L}^{\Sigma}_{\text{ots-L}}$
$\underline{\textsc{eavesdrop}(m_L, m_R):}$
$k \leftarrow \Sigma.\text{KeyGen}$
$c \leftarrow \Sigma.\text{Enc}(k, m_L)$
return c

$\equiv$

$\mathcal{L}^{\Sigma}_{\text{ots-R}}$
$\underline{\textsc{eavesdrop}(m_L, m_R):}$
$k \leftarrow \Sigma.\text{KeyGen}$
$c \leftarrow \Sigma.\text{Enc}(k, m_R)$
return c

Σ has one-time secrecy

Standard hybrid technique:

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

Security proof

$$\begin{array}{|l|}\hline \mathcal{L}^{\Sigma}_{\text{ots-L}} \\ \hline \underline{\text{EAVESDROP}(m_L, m_R):} \\ \quad k \leftarrow \Sigma.\text{KeyGen} \\ \quad c \leftarrow \Sigma.\text{Enc}(k, m_L) \\ \quad \text{return } c \\ \hline \end{array}$$

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

Security proof

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

$\textsc{eavesdrop}(m_L, m_R)$:

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

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

Security proof

$\textsc{eavesdrop}(m_L, m_R)$:
$c := \textsc{ctxt}(m_L)$
return c

$\diamond$

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

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

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

$\diamond$

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

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

Security proof

$$\begin{array}{|l|}\hline \textsc{eavesdrop}(m_L, m_R): \\ \quad c := \textsc{ctxt}(m_L) \\ \quad \text{return } c \\ \hline \end{array} \diamond \begin{array}{|l|}\hline \mathcal{L}^{\Sigma}_{\text{ots\$-rand}} \\ \hline \textsc{ctxt}(m): \\ \quad c \leftarrow \Sigma.\mathcal{C} \\ \quad \text{return } c \\ \hline \end{array}$$

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

$$\begin{array}{|l|}\hline \textsc{eavesdrop}(m_L, m_R): \\ \hline \quad c := \textsc{ctxt}(m_L) \\ \quad \text{return } c \\ \hline \end{array} \diamond \begin{array}{|l|}\hline \mathcal{L}^{\Sigma}_{\text{ots\$-rand}} \\ \hline \textsc{ctxt}(m): \\ \quad c \leftarrow \Sigma.\mathcal{C} \\ \quad \text{return } c \\ \hline \end{array}$$

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

Security proof

$\textsc{eavesdrop}(m_L, m_R)$:
$c := \textsc{ctxt}(m_L)$
return c

$\diamond$

$\mathcal{L}^{\Sigma}_{\text{ots\$-rand}}$
$\textsc{ctxt}(m)$:
$c \leftarrow \Sigma.\mathcal{C}$
return c

Argument to CTXT is never used!

Security proof

EAVESDROP(m_L, m_R):
$c :=$ CTXT(m_R)
return c

$\diamond$

$\mathcal{L}^{\Sigma}_{\text{ots\$-rand}}$
CTXT(m):
$c \leftarrow \Sigma.\mathcal{C}$
return c

Unused argument can be changed to m_R.

Security proof

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

$\diamond$

$\mathcal{L}^{\Sigma}_{\text{ots\$-rand}}$
CTXT(m):
$c \leftarrow \Sigma.\mathcal{C}$
return c

Unused argument can be changed to m_R.

Security proof

$$
\begin{array}{|l|}
\hline
\underline{\textsc{eavesdrop}(m_L, m_R):} \\
\quad c := \textsc{ctxt}(m_R) \\
\quad \text{return } c \\
\hline
\end{array}
\diamond
\begin{array}{|l|}
\hline
\qquad \mathcal{L}^{\Sigma}_{\text{ots\$-real}} \\
\hline
\underline{\textsc{ctxt}(m):} \\
\quad k \leftarrow \Sigma.\text{KeyGen} \\
\quad c \leftarrow \Sigma.\text{Enc}(k, m) \\
\quad \text{return } c \\
\hline
\end{array}
$$

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

$$\begin{array}{|l|}\hline \underline{\textsc{eavesdrop}(m_L, m_R):} \\ \quad c := \textsc{ctxt}(m_R) \\ \quad \text{return } c \\ \hline \end{array} \diamond \begin{array}{|l|}\hline \mathcal{L}^{\Sigma}_{\text{ots\$-real}} \\ \hline \underline{\textsc{ctxt}(m):} \\ \quad k \leftarrow \Sigma.\text{KeyGen} \\ \quad c \leftarrow \Sigma.\text{Enc}(k, m) \\ \quad \text{return } c \\ \hline \end{array}$$

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

Security proof

$$\begin{array}{|l|}\hline \underline{\textsc{eavesdrop}(m_L, m_R):} \\ \quad c := \textsc{ctxt}(m_R) \\ \quad \text{return } c \\ \hline \end{array} \diamond \begin{array}{|l|}\hline \mathcal{L}^{\Sigma}_{\text{ots\$-real}} \\ \hline \underline{\textsc{ctxt}(m):} \\ \quad k \leftarrow \Sigma.\text{KeyGen} \\ \quad c \leftarrow \Sigma.\text{Enc}(k, m) \\ \quad \text{return } c \\ \hline \end{array}$$

Inline the subroutine call.

Security proof

$$\underline{\textsc{eavesdrop}(m_L, m_R):}$$
$$k \leftarrow \Sigma.\text{KeyGen}$$
$$c \leftarrow \Sigma.\text{Enc}(k, m_R)$$
$$\text{return } c$$

Inline the subroutine call.

$$\begin{array}{|l|}\hline \underline{\textsc{eavesdrop}(m_L, m_R):} \\ \quad k \leftarrow \Sigma.\mathrm{KeyGen} \\ \quad c \leftarrow \Sigma.\mathrm{Enc}(k, m_R) \\ \quad \text{return } c \\ \hline \end{array}$$

Inline the subroutine call.

$\mathcal{L}^{\Sigma}_{\text{ots-R}}$
$\underline{\textsc{eavesdrop}(m_L, m_R)\text{:}}$ $k \leftarrow \Sigma.\mathsf{KeyGen}$ $c \leftarrow \Sigma.\mathsf{Enc}(k, m_R)$ return c

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