One-time pad security:

OTP:

$\mathcal{K} = \{0,1\}^\lambda$
$\mathcal{M} = \{0,1\}^\lambda$
$\mathcal{C} = \{0,1\}^\lambda$

KeyGen:
$k \leftarrow \mathcal{K}$
return k

Enc(k, m):
return $k \oplus m$

Dec(k, c):
return $k \oplus c$

Claim:

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

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

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

Overview:

Want to show:

$$\begin{array}{|l|}\hline \mathcal{L}^{\text{OTP}}_{\text{ots-L}} \\ \hline \underline{\text{QUERY}(m_L, m_R \in \text{OTP}.\mathcal{M}):} \\ \quad k \leftarrow \text{OTP.KeyGen} \\ \quad c := \text{OTP.Enc}(k, m_L) \\ \quad \text{return } c \\ \hline \end{array} \equiv \begin{array}{|l|}\hline \mathcal{L}^{\text{OTP}}_{\text{ots-R}} \\ \hline \underline{\text{QUERY}(m_L, m_R \in \text{OTP}.\mathcal{M}):} \\ \quad k \leftarrow \text{OTP.KeyGen} \\ \quad c := \text{OTP.Enc}(k, m_R) \\ \quad \text{return } c \\ \hline \end{array}$$

Standard hybrid technique:

- Starting with $\mathcal{L}^{\text{OTP}}_{\text{ots-L}}$, make a sequence of small modifications
- Each modification has no effect on calling program / adversary
- Sequence of modifications ends with $\mathcal{L}^{\text{OTP}}_{\text{ots-R}}$

Security proof

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

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

Security proof

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

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

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

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

$\quad$ return c

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

Security proof

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

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

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

$c := k \oplus m_L$

return c

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

Security proof

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

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

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

Security proof

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

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

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

$c := k \oplus m_L$

return c

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

Security proof

$$\begin{array}{|l|}\hline \underline{\textsc{query}(m_L, m_R \in \{0,1\}^\lambda):} \\ \quad c := \textsc{ctxt}(m_L) \\ \quad \text{return } c \\ \hline \end{array} \diamond \begin{array}{|l|}\hline \mathcal{L}_{\text{otp-real}} \\ \hline \underline{\textsc{ctxt}(m \in \{0,1\}^\lambda):} \\ \quad k \leftarrow \{0,1\}^\lambda \\ \quad \text{return } k \oplus m \\ \hline \end{array}$$

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

$$\boxed{\begin{array}{l}\underline{\textsc{query}(m_L, m_R \in \{0,1\}^\lambda):}\\ \quad c := \textsc{ctxt}(m_L)\\ \quad \text{return } c\end{array}} \diamond \boxed{\begin{array}{l}\qquad\mathcal{L}_{\text{otp-real}}\\ \hline \underline{\textsc{ctxt}(m \in \{0,1\}^\lambda):}\\ \quad k \leftarrow \{0,1\}^\lambda\\ \quad \text{return } k \oplus m\end{array}}$$

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

Security proof

$\textsc{query}(m_L, m_R \in \{0,1\}^\lambda)$:
$c := \textsc{ctxt}(m_L)$
return c

$\diamond$

$\mathcal{L}_{\text{otp-rand}}$
$\textsc{ctxt}(m \in \{0,1\}^\lambda)$:
$c \leftarrow \{0,1\}^\lambda$
return c

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

$$\begin{array}{|l|}\hline \underline{\textsc{query}(m_L, m_R \in \{0,1\}^\lambda):} \\ \quad c := \textsc{ctxt}(m_L) \\ \quad \text{return } c \\ \hline \end{array} \diamond \begin{array}{|l|}\hline \qquad \mathcal{L}_{\text{otp-rand}} \\ \hline \underline{\textsc{ctxt}(m \in \{0,1\}^\lambda):} \\ \quad c \leftarrow \{0,1\}^\lambda \\ \quad \text{return } c \\ \hline \end{array}$$

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

Security proof

$$\begin{array}{|l|}\hline \underline{\textsc{query}(m_L, m_R \in \{0,1\}^\lambda):} \\ \quad c := \textsc{ctxt}(m_L) \\ \quad \text{return } c \\ \hline \end{array} \diamond \begin{array}{|l|}\hline \quad\quad \mathcal{L}_{\text{otp-rand}} \\ \hline \underline{\textsc{ctxt}(m \in \{0,1\}^\lambda):} \\ \quad c \leftarrow \{0,1\}^\lambda \\ \quad \text{return } c \\ \hline \end{array}$$

Argument to CTXT is never used!

$$\begin{array}{|l|}\hline \underline{\textsc{query}(m_L, m_R \in \{0,1\}^\lambda):} \\ \quad c := \textsc{ctxt}(m_R) \\ \quad \text{return } c \\ \hline \end{array} \diamond \begin{array}{|l|}\hline \qquad \mathcal{L}_{\text{otp-rand}} \\ \hline \underline{\textsc{ctxt}(m \in \{0,1\}^\lambda):} \\ \quad c \leftarrow \{0,1\}^\lambda \\ \quad \text{return } c \\ \hline \end{array}$$

Unused argument can be changed to m_R.

$$\begin{array}{|l|}\hline \underline{\textsc{query}(m_L, m_R \in \{0,1\}^\lambda):} \\ \quad c := \textsc{ctxt}(m_R) \\ \quad \text{return } c \\ \hline \end{array} \diamond \begin{array}{|l|}\hline \quad\quad \mathcal{L}_{\text{otp-rand}} \\ \hline \underline{\textsc{ctxt}(m \in \{0,1\}^\lambda):} \\ \quad c \leftarrow \{0,1\}^\lambda \\ \quad \text{return } c \\ \hline \end{array}$$

Unused argument can be changed to m_R.

Security proof

$\textsc{query}(m_L, m_R \in \{0,1\}^\lambda)$:
$c := \textsc{ctxt}(m_R)$
return c

$\diamond$

$\mathcal{L}_{\text{otp-real}}$
$\textsc{ctxt}(m \in \{0,1\}^\lambda)$:
$k \leftarrow \{0,1\}^\lambda$
return $k \oplus m$

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

$\textsc{query}(m_L, m_R \in \{0,1\}^\lambda)$:
$c := \textsc{ctxt}(m_R)$
return c

$\diamond$

$\mathcal{L}_{\text{otp-real}}$
$\textsc{ctxt}(m \in \{0,1\}^\lambda)$:
$k \leftarrow \{0,1\}^\lambda$
return $k \oplus m$

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

$$\begin{array}{|l|}\hline \underline{\textsc{query}(m_L, m_R \in \{0,1\}^\lambda):} \\ \quad c := \textsc{ctxt}(m_R) \\ \quad \text{return } c \\ \hline \end{array} \diamond \begin{array}{|l|}\hline \quad\quad \mathcal{L}_{\text{otp-real}} \\ \hline \underline{\textsc{ctxt}(m \in \{0,1\}^\lambda):} \\ \quad k \leftarrow \{0,1\}^\lambda \\ \quad \text{return } k \oplus m \\ \hline \end{array}$$

Inline the subroutine call.

Security proof

$$\begin{array}{l}
\underline{\textsc{query}(m_L, m_R \in \{0,1\}^\lambda):} \\
\quad k \leftarrow \{0,1\}^\lambda \\
\quad c := k \oplus m_R \\
\quad \text{return } c
\end{array}$$

Inline the subroutine call.

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

Inline the subroutine call.

$$\boxed{\begin{array}{l} \underline{\textsc{query}(m_L, m_R \in \{0,1\}^\lambda):} \\ \quad k \leftarrow \{0,1\}^\lambda \\ \quad c := k \oplus m_R \\ \quad \text{return } c \end{array}}$$

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

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

$\textsc{query}(m_L, m_R \in \text{OTP}.\mathcal{M})$:
 $k \leftarrow \text{OTP.KeyGen}$
 $c := \text{OTP.Enc}(k, m_R)$
 return c

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

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

$\textsc{query}(m_L, m_R \in \text{OTP}.\mathcal{M})$:
  $k \leftarrow \text{OTP.KeyGen}$
  $c := \text{OTP.Enc}(k, m_R)$
  return c

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