One-time pad security:

OTP:

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

KeyGen:	Enc(k,m):	Dec(k,c):
$k \leftarrow \mathcal{K}$ return k	return $k \oplus m$	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:

$\textsc{ctxt}(m \in \{0,1\}^\lambda)$:		$\textsc{ctxt}(m \in \{0,1\}^\lambda)$:
$k \leftarrow \{0,1\}^\lambda$ return $k \oplus m$	$\equiv$	$c \leftarrow \{0,1\}^\lambda$ return c

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

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

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

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

return c

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

Security proof

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

```
QUERY(m_L, m_R ∈ OTP.M):
  k ← OTP.KeyGen
  c := OTP.Enc(k, m_L)
  return c
```

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

Security proof

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

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

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

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

```
QUERY(m_L, m_R ∈ {0,1}^λ):
  k ← {0,1}^λ
  c := k ⊕ m_L
  return c
```

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

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

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

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

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

Security proof

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

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

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

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

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

$\diamond$

$\mathcal{L}_{\text{otp-rand}}$

$\textsc{ctxt}\ m \in \{0,1\}^\lambda)$:
$\quad c \leftarrow \{0,1\}^\lambda$
$\quad$return c

Argument to CTXT is never used!

Security proof

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

Unused argument can be changed to m_R.

Security proof

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

Unused argument can be changed to m_R.

Security proof

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

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

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

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

Security proof

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

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.

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

Inline the subroutine call.

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

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

Security proof

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

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

Security proof

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

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

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

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

return c

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

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

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

Summary

We showed:

$\mathcal{L}^{\text{OTP}}_{\text{ots-L}}$		$\mathcal{L}^{\text{OTP}}_{\text{ots-R}}$
$\underline{\textsc{query}(m_L, m_R \in \text{OTP}.\mathcal{M})\text{:}}$ $k \leftarrow \text{OTP.KeyGen}$ $c := \text{OTP.Enc}(k, m_L)$ return c	$\equiv \cdots \equiv$	$\underline{\textsc{query}(m_L, m_R \in \text{OTP}.\mathcal{M})\text{:}}$ $k \leftarrow \text{OTP.KeyGen}$ $c := \text{OTP.Enc}(k, m_R)$ return c

So OTP satisfies one-time secrecy.