Pseudo-one-time pad security:

pOTP[G]:

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

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

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

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

Claim:

If G is a secure PRG then pOTP[G] satisfies one-time secrecy. That is, $\mathcal{L}^{\text{pOTP}[G]}_{\text{ots-L}} \equiv \mathcal{L}^{\text{pOTP}[G]}_{\text{ots-R}}$.

Overview:

Want to show:

$\mathcal{L}^{\text{pOTP}[G]}_{\text{ots-L}}$		$\mathcal{L}^{\text{pOTP}[G]}_{\text{ots-R}}$
$\textsc{query}(m_L, m_R \in \text{pOTP}.\mathcal{M})$: $k \leftarrow \text{pOTP.KeyGen}$ $c := \text{pOTP.Enc}(k, m_L)$ return c	$\approx$	$\textsc{query}(m_L, m_R \in \text{pOTP}.\mathcal{M})$: $k \leftarrow \text{pOTP.KeyGen}$ $c := \text{pOTP.Enc}(k, m_R)$ return c

Standard hybrid technique:

- Starting with $\mathcal{L}^{\text{pOTP}[G]}_{\text{ots-L}}$, make a sequence of small modifications
- Each modification has *negligible* effect on calling program
- Sequence of modifications ends with $\mathcal{L}^{\text{pOTP}[G]}_{\text{ots-R}}$

Overview:

Want to show:

$\mathcal{L}^{\text{pOTP}[G]}_{\text{ots-L}}$		$\mathcal{L}^{\text{pOTP}[G]}_{\text{ots-R}}$
$\underline{\text{QUERY}(m_L, m_R \in \text{pOTP}.\mathcal{M}):}$ $k \leftarrow \text{pOTP.KeyGen}$ $c := \text{pOTP.Enc}(k, m_L)$ return c	$\approx$	$\underline{\text{QUERY}(m_L, m_R \in \text{pOTP}.\mathcal{M}):}$ $k \leftarrow \text{pOTP.KeyGen}$ $c := \text{pOTP.Enc}(k, m_R)$ return c

The proof will **use** the fact G is a secure PRG. In other words,

$\mathcal{L}^{G}_{\text{prg-real}}$		$\mathcal{L}^{G}_{\text{prg-rand}}$
$\underline{\text{QUERY}():}$ $s \leftarrow \{0,1\}^{\lambda}$ return $G(s)$	$\approx$	$\underline{\text{QUERY}():}$ $z \leftarrow \{0,1\}^{\lambda+\ell}$ return z

Security proof

$\mathcal{L}_{\text{ots-L}}^{\text{pOTP}[G]}$

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

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

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

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

$\mathcal{L}_{\text{ots-L}}^{\text{pOTP}[G]}$

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

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

$c := G(k) \oplus m_L$

return c

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

$\mathcal{L}_{\text{ots-L}}^{\text{pOTP}[G]}$
$\text{QUERY}(m_L, m_R \in \{0,1\}^{\lambda+\ell})$:
$k \leftarrow \{0,1\}^\lambda$
$c := G(k) \oplus m_L$
return c

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

$\mathcal{L}_{\text{ots-L}}^{\text{pOTP}[G]}$

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

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

$c := G(k) \oplus m_L$

return c

These statements appear in $\mathcal{L}_{\text{prg-real}}^{G}$.

Security proof

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

$\diamond$

$\mathcal{L}^G_{\text{prg-real}}$
QUERY$'()$:
$s \leftarrow \{0,1\}^\lambda$
return $G(s)$

Factor out in terms of $\mathcal{L}^G_{\text{prg-real}}$.

$$\begin{array}{|l|}\hline \underline{\textsc{query}(m_L, m_R \in \{0,1\}^{\lambda+\ell})\text{:}} \\ \quad z \leftarrow \textsc{query}'() \\ \quad c := z \oplus m_L \\ \quad \text{return } c \\ \hline \end{array} \diamond \begin{array}{|l|}\hline \mathcal{L}^{G}_{\text{prg-real}} \\ \hline \underline{\textsc{query}'()\text{:}} \\ \quad s \leftarrow \{0,1\}^{\lambda} \\ \quad \text{return } G(s) \\ \hline \end{array}$$

Factor out in terms of $\mathcal{L}^{G}_{\text{prg-real}}$.

Security proof

$$\begin{array}{|l|}\hline \underline{\textsc{query}(m_L, m_R \in \{0,1\}^{\lambda+\ell}):} \\ \quad z \leftarrow \textsc{query}'() \\ \quad c := z \oplus m_L \\ \quad \text{return } c \\ \hline \end{array} \diamond \begin{array}{|l|}\hline \quad \mathcal{L}^G_{\text{prg-rand}} \\ \hline \underline{\textsc{query}'():} \\ \quad z \leftarrow \{0,1\}^{\lambda+\ell} \\ \quad \text{return } z \\ \hline \end{array}$$

Security of G allows us to swap $\mathcal{L}^G_{\text{prg-real}}$ with $\mathcal{L}^G_{\text{prg-rand}}$.

$$\begin{array}{|l|}\hline \underline{\text{QUERY}(m_L, m_R \in \{0,1\}^{\lambda+\ell}):} \\ \quad z \leftarrow \text{QUERY}'() \\ \quad c := z \oplus m_L \\ \quad \text{return } c \\ \hline \end{array} \diamond \begin{array}{|l|}\hline \mathcal{L}^G_{\text{prg-rand}} \\ \hline \underline{\text{QUERY}'():} \\ \quad z \leftarrow \{0,1\}^{\lambda+\ell} \\ \quad \text{return } z \\ \hline \end{array}$$

Security of G allows us to swap $\mathcal{L}^G_{\text{prg-real}}$ with $\mathcal{L}^G_{\text{prg-rand}}$.

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

$\diamond$

$\mathcal{L}^{G}_{\text{prg-rand}}$
$\textsc{query}'()$:
$z \leftarrow \{0,1\}^{\lambda+\ell}$
return z

Inline call to $\textsc{query}'$.

Security proof

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

$z \leftarrow \{0,1\}^{\lambda+\ell}$

$c := z \oplus m_L$

return c

Inline call to $\textsc{query}'$.

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

$z \leftarrow \{0,1\}^{\lambda+\ell}$

$c := z \oplus m_L$

return c

Inline call to $\textsc{query}'$.

Security proof

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

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

This is exactly $\mathcal{L}^{\text{OTP}}_{\text{ots-L}}$ — one time pad!

Security proof

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

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

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

$c := k \oplus m_L$

return c

This is exactly $\mathcal{L}_{\text{ots-L}}^{\text{OTP}}$ — one time pad!

Security proof

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

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

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

$c := k \oplus m_R$

return c

Security of one-time pad is that we can replace $\mathcal{L}^{\text{OTP}}_{\text{ots-L}}$ with $\mathcal{L}^{\text{OTP}}_{\text{ots-R}}$.

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

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

Security of one-time pad is that we can replace $\mathcal{L}^{\text{OTP}}_{\text{ots-L}}$ with $\mathcal{L}^{\text{OTP}}_{\text{ots-R}}$.

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

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

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

Same steps in reverse order. Factor out in terms of $\mathcal{L}_{\text{prg-rand}}^{G}$.

Security proof

$\textsc{query}(m_L, m_R \in \{0,1\}^{\lambda+\ell})$:
  $z := \textsc{query}'()$
  $c := z \oplus m_R$
  return c

$\diamond$

$\mathcal{L}^G_{\text{prg-rand}}$

$\textsc{query}'()$:
  $z \leftarrow \{0,1\}^{\lambda+\ell}$
  return z

Same steps in reverse order. Factor out in terms of $\mathcal{L}^G_{\text{prg-rand}}$.

QUERY$(m_L, m_R \in \{0,1\}^{\lambda+\ell})$:
$z :=$ QUERY$'()$
$c := z \oplus m_R$
return c

$\diamond$

$\mathcal{L}^G_{\text{prg-rand}}$
QUERY$'()$:
$z \leftarrow \{0,1\}^{\lambda+\ell}$
return z

Same steps in reverse order. Factor out in terms of $\mathcal{L}^G_{\text{prg-rand}}$.

Security proof

$\textsc{query}(m_L, m_R \in \{0,1\}^{\lambda+\ell})$:
  $z := \textsc{query}'()$
  $c := z \oplus m_R$
  return c

$\diamond$

$\mathcal{L}^G_{\text{prg-real}}$

$\textsc{query}'()$:
  $s \leftarrow \{0,1\}^\lambda$
  return $G(s)$

Replace $\mathcal{L}^G_{\text{prg-rand}}$ with $\mathcal{L}^G_{\text{prg-real}}$.

$\text{QUERY}(m_L, m_R \in \{0,1\}^{\lambda+\ell})$:
$z := \text{QUERY}'()$
$c := z \oplus m_R$
return c

$\diamond$

$\mathcal{L}^G_{\text{prg-real}}$
$\text{QUERY}'()$:
$s \leftarrow \{0,1\}^\lambda$
return $G(s)$

Replace $\mathcal{L}^G_{\text{prg-rand}}$ with $\mathcal{L}^G_{\text{prg-real}}$.

QUERY$(m_L, m_R \in \{0,1\}^{\lambda+\ell})$:
$z :=$ QUERY$'()$
$c := z \oplus m_R$
return c

$\diamond$

$\mathcal{L}^G_{\text{prg-real}}$
QUERY$'()$:
$s \leftarrow \{0,1\}^\lambda$
return $G(s)$

Inline call to QUERY$'$.

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

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

$c := G(k) \oplus m_R$

return c

Inline call to $\textsc{query}'$.

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

Inline call to QUERY′.

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

This happens to be $\mathcal{L}^{\text{pOTP}[G]}_{\text{ots-R}}$.

$$\mathcal{L}_{\text{ots-R}}^{\text{pOTP}[G]}$$

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

This happens to be $\mathcal{L}_{\text{ots-R}}^{\text{pOTP}[G]}$.

$$\mathcal{L}_{\text{ots-R}}^{\text{pOTP}[G]}$$

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

This happens to be $\mathcal{L}_{\text{ots-R}}^{\text{pOTP}[G]}$.

Summary

We showed:

$$\boxed{\begin{array}{l} \mathcal{L}^{\text{pOTP}[G]}_{\text{ots-L}} \\ \hline \textsc{query}(m_L, m_R \in \text{pOTP}.\mathcal{M}): \\ \quad k \leftarrow \text{pOTP.KeyGen} \\ \quad c := \text{pOTP.Enc}(k, m_L) \\ \quad \text{return } c \end{array}} \approx \cdots \approx \boxed{\begin{array}{l} \mathcal{L}^{\text{pOTP}[G]}_{\text{ots-R}} \\ \hline \textsc{query}(m_L, m_R \in \text{pOTP}.\mathcal{M}): \\ \quad k \leftarrow \text{pOTP.KeyGen} \\ \quad c := \text{pOTP.Enc}(k, m_R) \\ \quad \text{return } c \end{array}}$$

So pOTP$[G]$ satisfies one-time secrecy when G is a secure PRG.