Hybrid encryption:

Hybrid Encryption (Σ_{hyb}):

$$\mathcal{M} = \Sigma_{\text{sym}}.\mathcal{M}$$
$$\mathcal{C} = \Sigma_{\text{pub}}.\mathcal{C} \times \Sigma_{\text{sym}}.\mathcal{C}$$

$\underline{\text{KeyGen:}}$
$(pk, sk) \leftarrow \Sigma_{\text{pub}}.\text{KeyGen}$
return (pk, sk)

$\underline{\text{Enc}(pk, m):}$
$tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$
$c_{\text{pub}} \leftarrow \Sigma_{\text{pub}}.\text{Enc}(pk, tk)$
$c_{\text{sym}} \leftarrow \Sigma_{\text{sym}}.\text{Enc}(tk, m)$
return $(c_{\text{pub}}, c_{\text{sym}})$

$\underline{\text{Dec}(sk, (c_{\text{pub}}, c_{\text{sym}})):}$
$tk := \Sigma_{\text{pub}}.\text{Dec}(sk, c_{\text{pub}})$
return $\Sigma_{\text{sym}}.\text{Dec}(tk, c_{\text{sym}})$

Claim:

If Σ_{sym} is a one-time-secret symmetric-key encryption scheme and Σ_{pub} is a CPA-secure public-key encryption scheme, then Σ_{hyb} is also a CPA-secure public-key encryption scheme. That is, $\mathcal{L}^{\Sigma_{\text{hyb}}}_{\text{pk-cpa-L}} \approx \mathcal{L}^{\Sigma_{\text{hyb}}}_{\text{pk-cpa-R}}$.

Overview:

Want to show:

$\mathcal{L}^{\Sigma_{\text{hyb}}}_{\text{pk-cpa-L}}$		$\mathcal{L}^{\Sigma_{\text{hyb}}}_{\text{pk-cpa-R}}$
$(pk, sk) \leftarrow \Sigma_{\text{pub}}.\text{KeyGen}$ $\underline{\text{GETPK}():}$ return pk $\underline{\text{CHALLENGE}(m_L, m_R):}$ $tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$ $c_{\text{pub}} \leftarrow \Sigma_{\text{pub}}.\text{Enc}(pk, tk)$ $c_{\text{sym}} \leftarrow \Sigma_{\text{sym}}.\text{Enc}(tk, m_L)$ return $(c_{\text{pub}}, c_{\text{sym}})$	$\approx$	$(pk, sk) \leftarrow \Sigma_{\text{pub}}.\text{KeyGen}$ $\underline{\text{GETPK}():}$ return pk $\underline{\text{CHALLENGE}(m_L, m_R):}$ $tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$ $c_{\text{pub}} \leftarrow \Sigma_{\text{pub}}.\text{Enc}(pk, tk)$ $c_{\text{sym}} \leftarrow \Sigma_{\text{sym}}.\text{Enc}(tk, m_R)$ return $(c_{\text{pub}}, c_{\text{sym}})$

The proof will **use** the fact that Σ_{sym} has one-time secrecy and Σ_{pub} has CPA security.

$$\mathcal{L}^{\Sigma_{\mathsf{hyb}}}_{\mathsf{pk\text{-}cpa\text{-}L}}$$

$(pk, sk) \leftarrow \Sigma_{\mathsf{pub}}.\mathsf{KeyGen}$

<u>$\textsc{getpk}()$:</u>
  return pk

<u>$\textsc{challenge}(m_L, m_R)$:</u>
  $tk \leftarrow \Sigma_{\mathsf{sym}}.\mathsf{KeyGen}$
  $c_{\mathsf{pub}} \leftarrow \Sigma_{\mathsf{pub}}.\mathsf{Enc}(pk, tk)$
  $c_{\mathsf{sym}} \leftarrow \Sigma_{\mathsf{sym}}.\mathsf{Enc}(tk, m_L)$
  return $(c_{\mathsf{pub}}, c_{\mathsf{sym}})$

Starting point is $\mathcal{L}^{\Sigma_{\mathsf{hyb}}}_{\mathsf{pk\text{-}cpa\text{-}L}}$.

Security proof

$$\mathcal{L}^{\Sigma_{\text{hyb}}}_{\text{pk-cpa-L}}$$

$(pk, sk) \leftarrow \Sigma_{\text{pub}}.\text{KeyGen}$

$\underline{\textsc{getpk}():}$
  return pk

$\underline{\textsc{challenge}(m_L, m_R):}$
  $tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$
  $c_{\text{pub}} \leftarrow \Sigma_{\text{pub}}.\text{Enc}(pk, tk)$
  $c_{\text{sym}} \leftarrow \Sigma_{\text{sym}}.\text{Enc}(tk, m_L)$
  return $(c_{\text{pub}}, c_{\text{sym}})$

Starting point is $\mathcal{L}^{\Sigma_{\text{hyb}}}_{\text{pk-cpa-L}}$. Can we switch m_L to m_R right away?

Security proof

$\mathcal{L}^{\Sigma_{\text{hyb}}}_{\text{pk-cpa-L}}$

$(pk, sk) \leftarrow \Sigma_{\text{pub}}.\text{KeyGen}$

$\underline{\text{GETPK}():}$
  return pk

$\underline{\text{CHALLENGE}(m_L, m_R):}$
  $tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$
  $c_{\text{pub}} \leftarrow \Sigma_{\text{pub}}.\text{Enc}(pk, tk)$
  $c_{\text{sym}} \leftarrow \Sigma_{\text{sym}}.\text{Enc}(tk, m_L)$
  return $(c_{\text{pub}}, c_{\text{sym}})$

$\diamond$

$\mathcal{L}^{\Sigma_{\text{sym}}}_{\text{ots-L}}$

$\underline{\text{CHALLENGE}'(m_L, m_R):}$
$tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$
return $\Sigma_{\text{sym}}.\text{Enc}(tk, m_L)$

Can we apply security of Σ_{sym}?

Security proof

$\mathcal{L}^{\Sigma_{\text{hyb}}}_{\text{pk-cpa-L}}$

$(pk, sk) \leftarrow \Sigma_{\text{pub}}.\text{KeyGen}$

$\underline{\text{GETPK}():}$

  return pk

$\underline{\text{CHALLENGE}(m_L, m_R):}$

  $tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$

  $c_{\text{pub}} \leftarrow \Sigma_{\text{pub}}.\text{Enc}(pk, tk)$

  $c_{\text{sym}} \leftarrow \Sigma_{\text{sym}}.\text{Enc}(tk, m_L)$

  return $(c_{\text{pub}}, c_{\text{sym}})$

$\diamond$

$\mathcal{L}^{\Sigma_{\text{sym}}}_{\text{ots-L}}$

$\underline{\text{CHALLENGE}'(m_L, m_R):}$

  $tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$

  return $\Sigma_{\text{sym}}.\text{Enc}(tk, m_L)$

Can we apply security of Σ_{sym}? **No!** Its key used elsewhere!

$$\mathcal{L}^{\Sigma_{\text{hyb}}}_{\text{pk-cpa-L}}$$

$(pk, sk) \leftarrow \Sigma_{\text{pub}}.\text{KeyGen}$

$\underline{\textsc{getpk}():}$
  return pk

$\underline{\textsc{challenge}(m_L, m_R):}$
  $tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$
  $c_{\text{pub}} \leftarrow \Sigma_{\text{pub}}.\text{Enc}(pk, tk)$
  $c_{\text{sym}} \leftarrow \Sigma_{\text{sym}}.\text{Enc}(tk, m_L)$
  return $(c_{\text{pub}}, c_{\text{sym}})$

Instead, apply security of Σ_{pub} to get rid of *tk* here

$(pk, sk) \leftarrow \Sigma_{\text{pub}}.\text{KeyGen}$

$\underline{\textsc{getpk}():}$

  return pk

$\underline{\textsc{challenge}(m_L, m_R):}$

  $tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$

  $tk' \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$

  $c_{\text{pub}} \leftarrow \Sigma_{\text{pub}}.\text{Enc}(pk, tk)$

  $c_{\text{sym}} \leftarrow \Sigma_{\text{sym}}.\text{Enc}(tk, m_L)$

  return $(c_{\text{pub}}, c_{\text{sym}})$

Add unused "dummy *tk*" value.

$(pk, sk) \leftarrow \Sigma_{\text{pub}}.\text{KeyGen}$

$\underline{\textsc{getpk}():}$
  return pk

$\underline{\textsc{challenge}(m_L, m_R):}$
  $tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$
  $tk' \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$
  $c_{\text{pub}} \leftarrow \Sigma_{\text{pub}}.\text{Enc}(pk, tk)$
  $c_{\text{sym}} \leftarrow \Sigma_{\text{sym}}.\text{Enc}(tk, m_L)$
  return $(c_{\text{pub}}, c_{\text{sym}})$

Add unused "dummy *tk*" value.

Security proof

$$\begin{array}{|l|}\hline \underline{\textsc{challenge}(m_L, m_R):} \\ \quad tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen} \\ \quad tk' \leftarrow \Sigma_{\text{sym}}.\text{KeyGen} \\ \quad c_{\text{pub}} \leftarrow \textsc{challenge}'(tk, tk') \\ \quad c_{\text{sym}} \leftarrow \Sigma_{\text{sym}}.\text{Enc}(tk, m_L) \\ \quad \text{return } (c_{\text{pub}}, c_{\text{sym}}) \\ \hline \end{array} \diamond \begin{array}{|l|}\hline \mathcal{L}^{\Sigma_{\text{pub}}}_{\text{pk-cpa-L}} \\ \hline (pk, sk) \leftarrow \Sigma_{\text{pub}}.\text{KeyGen} \\ \\ \underline{\textsc{getpk}():} \\ \quad \text{return } pk \\ \\ \underline{\textsc{challenge}'(tk_L, tk_R):} \\ \quad \text{return } \Sigma_{\text{pub}}.\text{Enc}(pk, tk_L) \\ \hline \end{array}$$

Factor out Σ_{pub} operations in terms of $\mathcal{L}_{\text{pk-cpa-L}}$.

Security proof

$\textsc{challenge}(m_L, m_R)$:
$tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$
$tk' \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$
$c_{\text{pub}} \leftarrow \textsc{challenge}'(tk, tk')$
$c_{\text{sym}} \leftarrow \Sigma_{\text{sym}}.\text{Enc}(tk, m_L)$
return $(c_{\text{pub}}, c_{\text{sym}})$

$\diamond$

$\mathcal{L}^{\Sigma_{\text{pub}}}_{\text{pk-cpa-L}}$
$(pk, sk) \leftarrow \Sigma_{\text{pub}}.\text{KeyGen}$
$\textsc{getpk}()$:
return pk
$\textsc{challenge}'(tk_L, tk_R)$:
return $\Sigma_{\text{pub}}.\text{Enc}(pk, tk_L)$

Factor out Σ_{pub} operations in terms of $\mathcal{L}_{\text{pk-cpa-L}}$.

Security proof

$\textsc{challenge}(m_L, m_R)$:
$\quad tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$
$\quad tk' \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$
$\quad c_{\text{pub}} \leftarrow \textsc{challenge}'(tk, tk')$
$\quad c_{\text{sym}} \leftarrow \Sigma_{\text{sym}}.\text{Enc}(tk, m_L)$
$\quad$ return $(c_{\text{pub}}, c_{\text{sym}})$

$\diamond$

$\mathcal{L}^{\Sigma_{\text{pub}}}_{\text{pk-cpa-R}}$
$(pk, sk) \leftarrow \Sigma_{\text{pub}}.\text{KeyGen}$
$\textsc{getpk}()$:
$\quad$ return pk
$\textsc{challenge}'(tk_L, tk_R)$:
$\quad$ return $\Sigma_{\text{pub}}.\text{Enc}(pk\ tk_R)$

Replace $\mathcal{L}_{\text{pk-cpa-L}}$ with $\mathcal{L}_{\text{pk-cpa-R}}$.

Security proof

$$\begin{array}{|l|}\hline \underline{\textsc{challenge}(m_L, m_R):} \\ \quad tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen} \\ \quad tk' \leftarrow \Sigma_{\text{sym}}.\text{KeyGen} \\ \quad c_{\text{pub}} \leftarrow \textsc{challenge}'(tk, tk') \\ \quad c_{\text{sym}} \leftarrow \Sigma_{\text{sym}}.\text{Enc}(tk, m_L) \\ \quad \text{return } (c_{\text{pub}}, c_{\text{sym}}) \\ \hline \end{array} \diamond \begin{array}{|l|}\hline \qquad\qquad \mathcal{L}^{\Sigma_{\text{pub}}}_{\text{pk-cpa-R}} \\ \hline (pk, sk) \leftarrow \Sigma_{\text{pub}}.\text{KeyGen} \\ \\ \underline{\textsc{getpk}():} \\ \quad \text{return } pk \\ \\ \underline{\textsc{challenge}'(tk_L, tk_R):} \\ \quad \text{return } \Sigma_{\text{pub}}.\text{Enc}(pk, tk_R) \\ \hline \end{array}$$

Replace $\mathcal{L}_{\text{pk-cpa-L}}$ with $\mathcal{L}_{\text{pk-cpa-R}}$.

$(pk, sk) \leftarrow \Sigma_{\text{pub}}.\text{KeyGen}$

$\underline{\textsc{getpk}():}$
  return pk

$\underline{\textsc{challenge}(m_L, m_R):}$
  $tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$
  $tk' \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$
  $c_{\text{pub}} \leftarrow \Sigma_{\text{pub}}.\text{Enc}(pk, tk')$
  $c_{\text{sym}} \leftarrow \Sigma_{\text{sym}}.\text{Enc}(tk, m_L)$
  return $(c_{\text{pub}}, c_{\text{sym}})$

Inline $\mathcal{L}_{\text{pk-cpa-R}}$.

$(pk, sk) \leftarrow \Sigma_{\text{pub}}.\text{KeyGen}$

$\underline{\textsc{getpk}():}$
  return pk

$\underline{\textsc{challenge}(m_L, m_R):}$
  $tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$
  $tk' \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$
  $c_{\text{pub}} \leftarrow \Sigma_{\text{pub}}.\text{Enc}(pk, tk')$
  $c_{\text{sym}} \leftarrow \Sigma_{\text{sym}}.\text{Enc}(tk, m_L)$
  return $(c_{\text{pub}}, c_{\text{sym}})$

Inline $\mathcal{L}_{\text{pk-cpa-R}}$.

$(pk, sk) \leftarrow \Sigma_{\text{pub}}.\text{KeyGen}$

$\underline{\textsc{getpk}():}$
  return pk

$\underline{\textsc{challenge}(m_L, m_R):}$
  $tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$
  $tk' \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$
  $c_{\text{pub}} \leftarrow \Sigma_{\text{pub}}.\text{Enc}(pk, tk')$
  $c_{\text{sym}} \leftarrow \Sigma_{\text{sym}}.\text{Enc}(tk, m_L)$
  return $(c_{\text{pub}}, c_{\text{sym}})$

Now tk is used only in these lines.

Security proof

$$
\begin{array}{|l|}
\hline
(pk, sk) \leftarrow \Sigma_{\text{pub}}.\text{KeyGen} \\
\\
\underline{\text{GETPK}():} \\
\quad \text{return } pk \\
\\
\underline{\text{CHALLENGE}(m_L, m_R):} \\
\quad tk' \leftarrow \Sigma_{\text{sym}}.\text{KeyGen} \\
\quad c_{\text{pub}} \leftarrow \Sigma_{\text{pub}}.\text{Enc}(pk, tk') \\
\quad c_{\text{sym}} \leftarrow \text{CHALLENGE}'(m_L, m_R) \\
\quad \text{return } (c_{\text{pub}}, c_{\text{sym}}) \\
\hline
\end{array}
\diamond
\begin{array}{|l|}
\hline
\mathcal{L}^{\Sigma_{\text{sym}}}_{\text{ots-L}} \\
\hline
\underline{\text{CHALLENGE}'(m_L, m_R):} \\
\quad tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen} \\
\quad \text{return } \Sigma_{\text{sym}}.\text{Enc}(tk, m_L) \\
\hline
\end{array}
$$

Can factor out Σ_{sym} operations in terms of $\mathcal{L}_{\text{ots-L}}$.

$$
\begin{array}{|l|}
\hline
(pk, sk) \leftarrow \Sigma_{\text{pub}}.\text{KeyGen} \\
\\
\underline{\textsc{getpk}():} \\
\quad \text{return } pk \\
\\
\underline{\textsc{challenge}(m_L, m_R):} \\
\quad tk' \leftarrow \Sigma_{\text{sym}}.\text{KeyGen} \\
\quad c_{\text{pub}} \leftarrow \Sigma_{\text{pub}}.\text{Enc}(pk, tk') \\
\quad c_{\text{sym}} \leftarrow \textsc{challenge}'(m_L, m_R) \\
\quad \text{return } (c_{\text{pub}}, c_{\text{sym}}) \\
\hline
\end{array}
\diamond
\begin{array}{|l|}
\hline
\qquad \mathcal{L}_{\text{ots-L}}^{\Sigma_{\text{sym}}} \\
\hline
\underline{\textsc{challenge}'(m_L, m_R):} \\
\quad tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen} \\
\quad \text{return } \Sigma_{\text{sym}}.\text{Enc}(tk, m_L) \\
\hline
\end{array}
$$

Can factor out Σ_{sym} operations in terms of $\mathcal{L}_{\text{ots-L}}$.

Security proof

$(pk, sk) \leftarrow \Sigma_{\text{pub}}.\text{KeyGen}$

$\underline{\text{GETPK}():}$
  return pk

$\underline{\text{CHALLENGE}(m_L, m_R):}$
  $tk' \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$
  $c_{\text{pub}} \leftarrow \Sigma_{\text{pub}}.\text{Enc}(pk, tk')$
  $c_{\text{sym}} \leftarrow \text{CHALLENGE}'(m_L, m_R)$
  return $(c_{\text{pub}}, c_{\text{sym}})$

$\diamond$

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

$\underline{\text{CHALLENGE}'(m_L, m_R):}$
  $tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$
  return $\Sigma_{\text{sym}}.\text{Enc}(tk\ m_R)$

Replace $\mathcal{L}_{\text{ots-L}}$ with $\mathcal{L}_{\text{ots-R}}$.

$$
\begin{array}{|l|}
\hline
(pk, sk) \leftarrow \Sigma_{\text{pub}}.\text{KeyGen} \\
\\
\underline{\textsc{getpk}():} \\
\quad \text{return } pk \\
\\
\underline{\textsc{challenge}(m_L, m_R):} \\
\quad tk' \leftarrow \Sigma_{\text{sym}}.\text{KeyGen} \\
\quad c_{\text{pub}} \leftarrow \Sigma_{\text{pub}}.\text{Enc}(pk, tk') \\
\quad c_{\text{sym}} \leftarrow \textsc{challenge}'(m_L, m_R) \\
\quad \text{return } (c_{\text{pub}}, c_{\text{sym}}) \\
\hline
\end{array}
\diamond
\begin{array}{|l|}
\hline
\qquad\qquad \mathcal{L}_{\text{ots-R}}^{\Sigma_{\text{sym}}} \\
\hline
\underline{\textsc{challenge}'(m_L, m_R):} \\
\quad tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen} \\
\quad \text{return } \Sigma_{\text{sym}}.\text{Enc}(tk, m_R) \\
\hline
\end{array}
$$

Replace $\mathcal{L}_{\text{ots-L}}$ with $\mathcal{L}_{\text{ots-R}}$.

$(pk, sk) \leftarrow \Sigma_{\text{pub}}.\text{KeyGen}$

$\underline{\textsc{getpk}():}$
  return pk

$\underline{\textsc{challenge}(m_L, m_R):}$
  $tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$
  $tk' \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$
  $c_{\text{pub}} \leftarrow \Sigma_{\text{pub}}.\text{Enc}(pk, tk')$
  $c_{\text{sym}} \leftarrow \Sigma_{\text{sym}}.\text{Enc}(tk, m_R)$
  return $(c_{\text{pub}}, c_{\text{sym}})$

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

$(pk, sk) \leftarrow \Sigma_{\text{pub}}.\text{KeyGen}$

$\underline{\textsc{getpk}():}$

  return pk

$\underline{\textsc{challenge}(m_L, m_R):}$

  $tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$
  $tk' \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$
  $c_{\text{pub}} \leftarrow \Sigma_{\text{pub}}.\text{Enc}(pk, tk')$
  $c_{\text{sym}} \leftarrow \Sigma_{\text{sym}}.\text{Enc}(tk, m_R)$
  return $(c_{\text{pub}}, c_{\text{sym}})$

Inline $\mathcal{L}_{\text{ots-R}}$. Similar steps as before, now in reverse...

$$
\begin{array}{|l|}
\hline
\underline{\textsc{challenge}(m_L, m_R):} \\
\quad tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen} \\
\quad tk' \leftarrow \Sigma_{\text{sym}}.\text{KeyGen} \\
\quad c_{\text{pub}} \leftarrow \textsc{challenge}'(tk, tk') \\
\quad c_{\text{sym}} \leftarrow \Sigma_{\text{sym}}.\text{Enc}(tk, m_R) \\
\quad \text{return } (c_{\text{pub}}, c_{\text{sym}}) \\
\hline
\end{array}
\diamond
\begin{array}{|l|}
\hline
\qquad \mathcal{L}^{\Sigma_{\text{pub}}}_{\text{pk-cpa-R}} \\
\hline
(pk, sk) \leftarrow \Sigma_{\text{pub}}.\text{KeyGen} \\
\\
\underline{\textsc{getpk}():} \\
\quad \text{return } pk \\
\\
\underline{\textsc{challenge}'(tk_L, tk_R):} \\
\quad \text{return } \Sigma_{\text{pub}}.\text{Enc}(pk, tk_R) \\
\hline
\end{array}
$$

Factor out Σ_{pub} operations in terms of $\mathcal{L}_{\text{pk-cpa-R}}$.

Security proof

$$
\begin{array}{|l|}
\hline
\underline{\textsc{challenge}(m_L, m_R):} \\
\quad tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen} \\
\quad tk' \leftarrow \Sigma_{\text{sym}}.\text{KeyGen} \\
\quad c_{\text{pub}} \leftarrow \textsc{challenge}'(tk, tk') \\
\quad c_{\text{sym}} \leftarrow \Sigma_{\text{sym}}.\text{Enc}(tk, m_R) \\
\quad \text{return } (c_{\text{pub}}, c_{\text{sym}}) \\
\hline
\end{array}
\diamond
\begin{array}{|l|}
\hline
\qquad\qquad \mathcal{L}^{\Sigma_{\text{pub}}}_{\text{pk-cpa-R}} \\
\hline
(pk, sk) \leftarrow \Sigma_{\text{pub}}.\text{KeyGen} \\
\\
\underline{\textsc{getpk}():} \\
\quad \text{return } pk \\
\\
\underline{\textsc{challenge}'(tk_L, tk_R):} \\
\quad \text{return } \Sigma_{\text{pub}}.\text{Enc}(pk, tk_R) \\
\hline
\end{array}
$$

Factor out Σ_{pub} operations in terms of $\mathcal{L}_{\text{pk-cpa-R}}$.

$$
\begin{array}{|l|}
\hline
\underline{\textsc{challenge}(m_L, m_R):} \\
\quad tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen} \\
\quad tk' \leftarrow \Sigma_{\text{sym}}.\text{KeyGen} \\
\quad c_{\text{pub}} \leftarrow \textsc{challenge}'(tk, tk') \\
\quad c_{\text{sym}} \leftarrow \Sigma_{\text{sym}}.\text{Enc}(tk, m_R) \\
\quad \text{return } (c_{\text{pub}}, c_{\text{sym}}) \\
\hline
\end{array}
\diamond
\begin{array}{|l|}
\hline
\qquad\qquad \mathcal{L}_{\text{pk-cpa-L}}^{\Sigma_{\text{pub}}} \\
\hline
(pk, sk) \leftarrow \Sigma_{\text{pub}}.\text{KeyGen} \\
\\
\underline{\textsc{getpk}():} \\
\quad \text{return } pk \\
\\
\underline{\textsc{challenge}'(tk_L, tk_R):} \\
\quad \text{return } \Sigma_{\text{pub}}.\text{Enc}(pk, \boxed{tk_L}) \\
\hline
\end{array}
$$

Replace $\mathcal{L}_{\text{pk-cpa-R}}$ with $\mathcal{L}_{\text{pk-cpa-L}}$.

$$
\begin{array}{|l|}
\hline
\underline{\textsc{challenge}(m_L, m_R):} \\
\quad tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen} \\
\quad tk' \leftarrow \Sigma_{\text{sym}}.\text{KeyGen} \\
\quad c_{\text{pub}} \leftarrow \textsc{challenge}'(tk, tk') \\
\quad c_{\text{sym}} \leftarrow \Sigma_{\text{sym}}.\text{Enc}(tk, m_R) \\
\quad \text{return } (c_{\text{pub}}, c_{\text{sym}}) \\
\hline
\end{array}
\diamond
\begin{array}{|l|}
\hline
\mathcal{L}^{\Sigma_{\text{pub}}}_{\text{pk-cpa-L}} \\
\hline
(pk, sk) \leftarrow \Sigma_{\text{pub}}.\text{KeyGen} \\
\\
\underline{\textsc{getpk}():} \\
\quad \text{return } pk \\
\\
\underline{\textsc{challenge}'(tk_L, tk_R):} \\
\quad \text{return } \Sigma_{\text{pub}}.\text{Enc}(pk, tk_L) \\
\hline
\end{array}
$$

Replace $\mathcal{L}_{\text{pk-cpa-R}}$ with $\mathcal{L}_{\text{pk-cpa-L}}$.

Security proof

$(pk, sk) \leftarrow \Sigma_{\text{pub}}.\text{KeyGen}$

$\underline{\text{GETPK}():}$

  return pk

$\underline{\text{CHALLENGE}(m_L, m_R):}$

  $tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$
  $tk' \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$
  $c_{\text{pub}} \leftarrow \Sigma_{\text{pub}}.\text{Enc}(pk, tk)$
  $c_{\text{sym}} \leftarrow \Sigma_{\text{sym}}.\text{Enc}(tk, m_R)$
  return $(c_{\text{pub}}, c_{\text{sym}})$

Inline $\mathcal{L}_{\text{pk-cpa-L}}$.

$(pk, sk) \leftarrow \Sigma_{\text{pub}}.\text{KeyGen}$

$\underline{\textsc{getpk}():}$

  return pk

$\underline{\textsc{challenge}(m_L, m_R):}$

  $tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$
  $tk' \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$
  $c_{\text{pub}} \leftarrow \Sigma_{\text{pub}}.\text{Enc}(pk, tk)$
  $c_{\text{sym}} \leftarrow \Sigma_{\text{sym}}.\text{Enc}(tk, m_R)$
  return $(c_{\text{pub}}, c_{\text{sym}})$

Inline $\mathcal{L}_{\text{pk-cpa-L}}$.

$(pk, sk) \leftarrow \Sigma_{\text{pub}}.\text{KeyGen}$

$\underline{\textsc{getpk}():}$

  return pk

$\underline{\textsc{challenge}(m_L, m_R):}$

  $tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$
  $tk' \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$
  $c_{\text{pub}} \leftarrow \Sigma_{\text{pub}}.\text{Enc}(pk, tk)$
  $c_{\text{sym}} \leftarrow \Sigma_{\text{sym}}.\text{Enc}(tk, m_R)$
  return $(c_{\text{pub}}, c_{\text{sym}})$

Unused variable tk' can be removed.

$$\mathcal{L}^{\Sigma_{\text{hyb}}}_{\text{pk-cpa-R}}$$

$(pk, sk) \leftarrow \Sigma_{\text{pub}}.\text{KeyGen}$

$\underline{\text{GETPK}():}$
  return pk

$\underline{\text{CHALLENGE}(m_L, m_R):}$
  $tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$
  $c_{\text{pub}} \leftarrow \Sigma_{\text{pub}}.\text{Enc}(pk, tk)$
  $c_{\text{sym}} \leftarrow \Sigma_{\text{sym}}.\text{Enc}(tk, m_R)$
  return $(c_{\text{pub}}, c_{\text{sym}})$

Remove tk'. Result is $\mathcal{L}^{\Sigma_{\text{hyb}}}_{\text{pk-cpa-R}}$.

Summary

We showed:

$\mathcal{L}^{\Sigma_{\text{hyb}}}_{\text{pk-cpa-L}}$		$\mathcal{L}^{\Sigma_{\text{hyb}}}_{\text{pk-cpa-R}}$

$(pk, sk) \leftarrow \Sigma_{\text{pub}}.\text{KeyGen}$
 	
$\underline{\text{GETPK}()}$:
  return pk
 	
$\underline{\text{CHALLENGE}(m_L, m_R)}$:
  $tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$
  $c_{\text{pub}} \leftarrow \Sigma_{\text{pub}}.\text{Enc}(pk, tk)$
  $c_{\text{sym}} \leftarrow \Sigma_{\text{sym}}.\text{Enc}(tk, m_L)$
  return $(c_{\text{pub}}, c_{\text{sym}})$
	$\approx$	$(pk, sk) \leftarrow \Sigma_{\text{pub}}.\text{KeyGen}$
		
		$\underline{\text{GETPK}()}$:
		  return pk
		
		$\underline{\text{CHALLENGE}(m_L, m_R)}$:
		  $tk \leftarrow \Sigma_{\text{sym}}.\text{KeyGen}$
		  $c_{\text{pub}} \leftarrow \Sigma_{\text{pub}}.\text{Enc}(pk, tk)$
		  $c_{\text{sym}} \leftarrow \Sigma_{\text{sym}}.\text{Enc}(tk, m_R)$
		  return $(c_{\text{pub}}, c_{\text{sym}})$

So our scheme is a CPA-secure public-key encryption scheme.