① 1. $t_1 = \theta.MAC(k, 0^\lambda)$ and $t_2 = \theta.MAC(k, 1\|0^{\lambda-1})$

$t_1' = \theta.MAC(k, 0\|1^{\lambda-1})$ and $t_2' = \theta.MAC(k, 1^\lambda)$

Then for $m = 0^{\lambda-1}\|1^{\lambda-1}$, $ECB\text{-}MAC'(k,m) = (t_1, t_2')$. (malleable)

2. $\underline{A \circ L}$ where L is either $L_{MAC\text{-}real}$ or $L_{MAC\text{-}fake}$ for ECB-MAC'.

$(t_1, t_2) \leftarrow Gettag(0^{2\lambda-2})$

$(t_1', t_2') \leftarrow Gettag(1^{2\lambda-2})$

if $Checktag(0^{\lambda-1}\|1^{\lambda-1}, (t_1, t_2')) == True$:

  output "real"

else:

  output "fake"

$$\Pr[A \text{ succeeds}] = \Pr[A \circ L \Rightarrow \text{"real"} \wedge L = L_{MAC\text{-}real}] + \Pr[A \circ L \Rightarrow \text{"fake"} \wedge L = L_{MAC\text{-}fake}]$$

$$= \Pr[A \circ L \Rightarrow \text{"real"} \mid L = L_{MAC\text{-}real}] \Pr[L = L_{MAC\text{-}real}]$$

$$+ \Pr[A \circ L \Rightarrow \text{"fake"} \mid L = L_{MAC\text{-}fake}] \Pr[L = L_{MAC\text{-}fake}]$$

$$= 1 \cdot \frac{1}{2} + 1 \cdot \frac{1}{2} = 1$$

② 1. By assumption, we have $t = \theta.MAC(k, \theta.MAC(k, m_1) \oplus m_2)$. The MAC for $m_1\|m_2\|(m_1 \oplus t)\|m_2$ is

$$\theta.MAC(k, \theta.MAC(k, \underbrace{\underbrace{\theta.MAC(k, \theta.MAC(k, m_1) \oplus m_2)}_{t} \oplus (m_1 \oplus t)}_{m_1 \oplus \cancel{t} \oplus \cancel{t}}) \oplus m_2) = t.$$

2. $\underline{A \circ L}$ where L is either $L_{MAC\text{-}real}$ or $L_{MAC\text{-}fake}$ for CBC-MAC

$t \leftarrow Gettag(m_1\|m_2)$

if $Checktag(m_1\|m_2\|(m_1 \oplus t)\|m_2, t) == True$:

  output "real"

else:

  output "fake"

Similar to exercise ①, $\Pr[A \text{ succeeds}] = 1$.

③ 1. $\Sigma.\mathrm{Dec}\left((k_E,k_M), \Sigma.\mathrm{Enc}[(k_E,k_M),m]\right) = \Sigma.\mathrm{Dec}\left((k_E,k_M),(\Omega.\mathrm{Enc}(k_E,m), \theta.\mathrm{MAC}(k_M,c))\right)$

$= \Omega.\mathrm{Dec}(k_E, \Omega.\mathrm{Enc}(k_E,m)) = m$

by correctness of Ω

2. $L^{\Sigma}_{\text{CCA-0}}$

$k \leftarrow \Sigma.\mathrm{KeyGen}()$

$S = \emptyset$

$\mathrm{CTXT}(m_0, m_1 \in \Sigma.M)$:

1. If $|m_0| \neq |m_1|$ output $\perp$
2. $c \leftarrow \Sigma.\mathrm{Enc}(k, m_0)$
3. $S = S \cup \{c\}$
4. Output c

$\mathrm{Decrypt}(c \in \Sigma.C)$:

1. If $c \in S$ output $\perp$
2. Output $\Sigma.\mathrm{Dec}(k,c)$

$\xrightarrow{\text{Replace}}$ every call to Σ with their definitions

$L_{\text{step-1}}$

$k_E \leftarrow \Omega.\mathrm{KeyGen}()$

$k_M \leftarrow \theta.\mathrm{KeyGen}()$

$k = (k_E, k_M)$

$S = \emptyset$

$\mathrm{CTXT}(m_0, m_1 \in \Omega.M)$:

1. If $|m_0| \neq |m_1|$ output $\perp$
2. $c' \leftarrow \Omega.\mathrm{Enc}(k_E, m_0)$
3. $t' \leftarrow \theta.\mathrm{MAC}(k_M, c')$
4. $S = S \cup \{(c',t')\}$
5. output $c = (c', t')$

$\mathrm{Decrypt}(c = (c',t') \in \Omega.C \times \theta.T)$

1. If $c \in S$ output $\perp$
2. If $t' \neq \theta.\mathrm{MAC}(k_M, c')$ output $\perp$
3. output $\Omega.\mathrm{Dec}(k_E, c')$

3. Now, we make a call to $L^{\theta}_{\text{MAC-real}}$ every time we need to use $\theta.\mathrm{MAC}$.

$L^{\theta}_{\text{MAC-real}}$

$k_M \leftarrow \theta.\mathrm{KeyGen}()$

$\mathrm{Gettag}(m, \theta.M)$:

Return $\theta.\mathrm{MAC}(k_M, m)$

$\mathrm{Checktag}(m \in \theta.M, t \in \theta.T)$:

Return $\theta.\mathrm{MAC}(k_M, m) == t$

composition of libraries (meaning functions called are defined as in $L^{\theta}_{\text{MACreal}}$)

$L_{\text{step-1}} \circ L^{\theta}_{\text{MAC-real}}$

$k_E \leftarrow \Omega.\mathrm{KeyGen}()$

$k_M \leftarrow \theta.\mathrm{KeyGen}()$

$k = (k_E, k_M)$

$S = \emptyset$

$\mathrm{CTXT}(m_0, m_1 \in \Omega.M)$:

1. If $|m_0| \neq |m_1|$ output $\perp$
2. $c' \leftarrow \Omega.\mathrm{Enc}(k_E, m_0)$
3. $t' \leftarrow \mathrm{Gettag}(c')$
4. $S = S \cup \{(c',t')\}$
5. output $c = (c', t')$

$\mathrm{Decrypt}(c = (c',t') \in \Omega.C \times \theta.T)$

1. If $c \in S$ output $\perp$
2. If $\mathrm{Checktag}(c',t') = \mathit{false}$ output $\perp$
3. output $\Omega.\mathrm{Dec}(k_E, c')$

Since the library $L^{\theta}_{\text{MAC-real}}$ uses the actual functions of θ we get a perfect simulation of $L^{\Sigma}_{\text{CCA-0}}$ by $L_{\text{step-1}} \circ L^{\theta}_{\text{MAC-real}}$, then $L^{\Sigma}_{\text{CCA-0}} \equiv L_{\text{step-1}} \circ L^{\theta}_{\text{MAC-real}}$

4. By assumption Θ is a secure MAC scheme, i.e., $L^{\Theta}_{\text{MAC-real}} \approx L^{\Theta}_{\text{MAC-fake}}$.

And we know that if $L_1 \approx L_2$ and L runs in poly. time, then $L \circ L_1 \approx L \circ L_2$.

Therefore, $L_{\text{step-1}} \circ L^{\Theta}_{\text{MAC-real}} \approx L_{\text{step-1}} \circ L^{\Theta}_{\text{MAC-fake}}$.

5. We write $L_{\text{step-1}} \circ L^{\Theta}_{\text{MAC-fake}}$ into a new lib. that doesn't call $L^{\Theta}_{\text{MAC-fake}}$

$\underline{L^{\Theta}_{\text{MAC-fake}}}$
$k_M \leftarrow \Theta.\text{KeyGen}()$
$S_\Theta = \emptyset$
$\underline{\text{Gettag}}(m \in \Theta.M)$:
1. $t = \Theta.\text{MAC}(k_M, m)$
2. $S_\Theta = S_\Theta \cup \{(m,t)\}$
3. output t

$\underline{\text{Checktag}}(m \in \Theta.M, t \in \Theta.T)$
return $(m,t) \in S_\Theta$

$\underline{L_{\text{step-2}}}$
$k_E \leftarrow \Omega.\text{KeyGen}()$
$k_M \leftarrow \Theta.\text{KeyGen}()$
$k = (k_E, k_M)$
$S = \emptyset$
$\underline{\text{CTXT}}(m_0, m_1 \in \Omega.M)$:
1. If $|m_0| \neq |m_1|$ output $\perp$
2. $c' \leftarrow \Omega.\text{Enc}(k_E, m_0)$
3. $t' \leftarrow \Theta.\text{MAC}(k_M, c')$
4. $S = S \cup \{(c', t')\}$
5. output $c = (c', t')$

$\underline{\text{Decrypt}}(c = (c', t') \in \Omega.C \times \Theta.T)$
1. If $c \in S$ output $\perp$
2. If $c \notin S$ output $\perp$
3. output $\Omega.\text{Dec}(k_E, c')$

Notice that we didn't introduce the set S_Θ in $L_{\text{step-2}}$. There is no need of to do this, since S and S_Θ contain the same elements. We just rewrite the lib., their functions are the same. So,

$L_{\text{step-2}} \equiv L_{\text{step-1}} \circ L^{\Theta}_{\text{MAC-fake}}$.

6. Under which conditions will $\Omega.\text{Dec}(k_E, c')$ be reached? Since $c \in S$ and $c \notin S$ are complementary events, line 3 of "Decrypt" is never reached. Therefore, $L_{\text{step-3}} \equiv L_{\text{step-2}}$.

7. Recall: $\underline{L^{\Omega}_{\text{CPA-0}}}$
$k_E \leftarrow \Omega.\text{KeyGen}()$
$\underline{\text{CTXT}}(m_0, m_1 \in \Omega.M)$:
1. If $|m_0| \neq |m_1|$ output $\perp$
2. $c \leftarrow \Omega.\text{Enc}(k_E, m_0)$
3. output c

$L_{step\text{-}4} \circ L^{\Omega}_{CPA\text{-}0}$

$k_E \leftarrow \Omega.KeyGen()$

$k_M \leftarrow \theta.KeyGen()$

$k = (k_E, k_M)$

$S = \emptyset$

CTXT($m_0, m_1 \in \Omega.M$):

1. If $|m_0| \neq |m_1|$ output $\perp$
2. $c' \leftarrow$ CTXT (m_0, m_1)
3. $t' \leftarrow \theta.MAC(k_M, c')$
4. $S = S \cup \{(c', t')\}$
5. output $c = (c', t')$

Decrypt($c = (c', t') \in \Omega.C \times \theta.T$)

1. output $\perp$

Again, $L_{step\text{-}3} \equiv L_{step\text{-}4} \circ L^{\Omega}_{CPA\text{-}0}$ since they are using the same function to encrypt the message.

8. By assumption Ω is CPA-secure enc. scheme (for the left-right def.), i.e., $L^{\Omega}_{CPA\text{-}0} \approx L^{\Omega}_{CPA\text{-}1}$.

Similar to 4., we have $L_{step\text{-}4} \circ L^{\Omega}_{CPA\text{-}0} \approx L_{step\text{-}4} \circ L^{\Omega}_{CPA\text{-}1}$. By 2. to 7. we showed that $L^{\Sigma}_{CCA\text{-}0} \approx L_{step4} \circ L^{\Omega}_{CPA}$. In the same way, we prove $L^{\Sigma}_{CCA\text{-}1} \approx L_{step4} \circ L^{\Omega}_{CPA\text{-}1}$.

Combining all together we get $L^{\Sigma}_{CCA\text{-}0} \approx L_{step\text{-}4} \circ L^{\Omega}_{CPA\text{-}0} \approx L_{step\text{-}4} \circ L^{\Omega}_{CPA\text{-}1} \approx L^{\Sigma}_{CCA\text{-}1}$.