① MDMAC (k, m):

1. Let $m_1, \dots, m_\tau = \text{MDPad}_\ell(m)$ where $\ell = |m_i|$
2. Set $y_0 := k$
3. For $i = 1, \dots, \tau$:
   $y_i = h(m_i | y_{i-1})$
4. Output y_τ

Assume we are given $(m, t) = (m, \text{MDMAC}(k, m))$ with $\text{MDPad}_\ell(m) = m_1, \dots, m_\tau$ where $|m_i| = \ell$. Set $m' = m_1 | \cdots | m_\tau$. Then $|m'| = \tau \cdot \ell$, and e' is the ℓ-bit string representing $|m'| = \tau \cdot \ell$ in binary form. So, $\text{MDPad}_\ell(m') = m_1, \dots, m_\tau, e'$ and $\text{MDMAC}(k, m') = h(e' | t)$.

In conclusion, $(m', t') = (m', h(e'|t))$. (m' is necessarily distinct from m because padding introduces length of m, i.e., $m_\tau = e$ where e is binary represantion of $|m|$.)

② Let m be any message with $\text{SMDPad}_\ell(m) = m_1, \dots, m_\tau$ where $|m_1| = \lambda$ and $|m_i| = \ell$ for $i \geq 2$ and $\text{SMDHash}(m) = h$. Set $m' = h(m_2 | m_1) | m_3, \dots, m_\tau$. Then $\text{SMDPad}_\ell(m') = h(m_2 | m_1), m_3, \dots, m_\tau$ and $\text{SMDHash}(m') = h$.

③ Recall:

$\mathcal{L}^H_{\text{CR-real}}$

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

Getsalt():
Return s

Test(m_1, m_2):
If $H(s, m_1) = H(s, m_2)$ & $m_1 \neq m_2$:
  output 1
Else:
  output 0

$\mathcal{L}^H_{\text{CR-fake}}$

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

Get salt():
Return s

Test(m_1, m_2):
Output 0

Observe that H being homomorphic implies that $0^\lambda \overset{\text{property of XOR}}{=} H(1^n) \oplus H(1^n) \overset{H\text{ is homomorphic}}{=} H(1^n \oplus 1^n) \overset{\text{property of XOR}}{=} H(0^n)$

for any n. Then construct adversary $\mathcal{A}$ as follows: $\mathcal{A} \diamond \mathcal{L}$:

If Test$(0, 0^2) = 1$:
  output "real"
Else:
  output "fake"

$$\Pr[\mathcal{A} \text{ succeeds}] = \Pr[\mathcal{A} \circ L \Rightarrow \text{real} \cap L = L^{H}_{\text{CR-real}}] + \Pr[\mathcal{A} \circ L \Rightarrow \text{fake} \cap L = L^{H}_{\text{CR-fake}}]$$

$$= \underbrace{\Pr[\mathcal{A} \circ L \Rightarrow \text{real} \mid L = L^{H}_{\text{CR-real}}]}_{1} \cdot \underbrace{\Pr[L = L^{H}_{\text{CR-real}}]}_{\frac{1}{2}} + \underbrace{\Pr[\mathcal{A} \circ L \Rightarrow \text{fake} \mid L = L^{H}_{\text{CR-fake}}]}_{1} \cdot \underbrace{\Pr[L = L^{H}_{\text{CR-fake}}]}_{\frac{1}{2}}$$

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

4) Think of $F(x,y)$ as $F_x(y)$ where x is a key and F_x is a permutation from $\{0,1\}^B$ to $\{0,1\}^B$. In particular, F_x is surjective. For a given output value $z \in \{0,1\}^B$ for each key $x \in \{0,1\}^\lambda$, there exists only one value $y \in \{0,1\}^B$ s.t. $F_x(y) = z$.

$\mathcal{A} \circ L$:

$x_1 \leftarrow \{0,1\}^\lambda$ — This defines a perm. F_{x_1}

$y_1 \leftarrow \{0,1\}^B$ — Input for F_{x_1}

$z := F(x_1, y_1)$ — i.e. $F_{x_1}(y_1)$

$x_2 \leftarrow \{0,1\}^\lambda \setminus \{x_1\}$ — Creates a key different than x_1

$y_2 := F_{x_2}^{-1}(z)$ — Finds the input y_2 for F_{x_2} s.t. $F_{x_2}(y_2) = F_{x_1}(y_1) = z$

If Test$(x_1|y_1, x_2|y_2) = 1$: — We know $H(x_1|y_1) = H(x_2|y_2)$

  output "real"

Else:

  output "fake"

$\Pr[\mathcal{A} \text{ succeeds}] = 1$ as in Ex. 3.