MTAT.07.003 Cryptology II
Spring 2012 / Exercise session ?? / Example Solution

Exercise (Trivial inclusions). *Prove the following claims about public key cryptosystems*

1. *A homomorphic cryptosystem cannot be non-malleable.*
2. *NM-CPA security implies IND-CPA security.*
3. *NM-CCA1 security implies IND-CCA1 security.*
4. *NM-CCA2 security implies IND-CCA2 security.*

Solution. To prove the first claim about non-malleability, we have recall the definition of homomorphic encryption. There are many types of homomorphic encryption. Here we consider only multiplicatively and additively homomorphic encryption. A cryptosystem is additively homomorphic if

$$\forall \mathsf{pk}, \mathsf{sk} \leftarrow \mathsf{Gen},\ \forall m_1, m_2 \in \mathcal{M}_{\mathsf{pk}} : \quad \mathsf{Enc}_{\mathsf{pk}}(m_1) \cdot \mathsf{Enc}_{\mathsf{pk}}(m_2) \equiv \mathsf{Enc}_{\mathsf{pk}}(m_1 + m_2)\ .$$

A cryptosystem is multiplicatively homomorphic if

$$\forall \mathsf{pk}, \mathsf{sk} \leftarrow \mathsf{Gen},\ \forall m_1, m_2 \in \mathcal{M}_{\mathsf{pk}} : \quad \mathsf{Enc}_{\mathsf{pk}}(m_1) \cdot \mathsf{Enc}_{\mathsf{pk}}(m_2) \equiv \mathsf{Enc}_{\mathsf{pk}}(m_1 \cdot m_2)\ .$$

One of the best properties of homomorphic encryption schemes is re-randomisation. Let c be a valid ciphertext of a message m. For additively homomorphic encryption scheme, we can re-randomise a ciphertext c by multiplying it by a freshly generated encryption $\mathsf{Enc}_{\mathsf{pk}}(0)$. As a result, we get a ciphertext $\hat{c}_1$ such that if is a random ciphertext of m:

$$\hat{c}_1 \equiv c \cdot \mathsf{Enc}_{\mathsf{pk}}(0) \equiv \mathsf{Enc}_{\mathsf{pk}}(m + 0) \equiv \mathsf{Enc}_{\mathsf{pk}}(m)\ .$$

For multiplicatively homomorphic encryption scheme, we can re-randomise a ciphertext c by multiplying it by a freshly generated encryption $\mathsf{Enc}_{\mathsf{pk}}(1)$. Again, we get a ciphertext $\hat{c}_1$ such that

$$\hat{c}_1 \equiv c \cdot \mathsf{Enc}_{\mathsf{pk}}(1) \equiv \mathsf{Enc}_{\mathsf{pk}}(m \cdot 1) \equiv \mathsf{Enc}_{\mathsf{pk}}(m)\ .$$

In other words, a malicious attacker can always alter the ciphertext without altering the messages underneath. As result, it is easy to show malleability of such encryption schemes. In the following, the left adversary is constructed for an additively and the right one is for multiplicatively homomorphic encryption:

$\mathcal{B}(\mathsf{pk})$
$\lfloor$ **return** $\mathcal{M}_{\mathsf{pk}}$

$\mathcal{B}(c)$
$\lceil\ \pi(m, \hat{m}_1) = [m \stackrel{?}{=} \hat{m}_1]$
$\lfloor$ **return** $(\pi, \hat{c}_1)$

$\mathcal{B}(\mathsf{pk})$
$\lfloor$ **return** $\mathcal{M}_{\mathsf{pk}}$

$\mathcal{B}(c)$
$\lceil\ \pi(m, \hat{m}_1) = [m \stackrel{?}{=} \hat{m}_1]$
$\hat{c}_1 \leftarrow c \cdot \mathsf{Enc}_{\mathsf{pk}}(1)$
$\lfloor$ **return** $(\pi, \hat{c}_1)$.

If we inline the definition of the adversary into the games defining non-malleability

$\mathcal{Q}_0^{\mathcal{B}}$
$\lceil\ (\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$\mathcal{M}_0 \leftarrow \mathcal{B}(\mathsf{pk})$
$m \leftarrow \mathcal{M}_0$
$c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m)$
$\pi(\cdot), \hat{c}_1, \ldots \hat{c}_n \leftarrow \mathcal{B}(c)$
if $c \in \{\hat{c}_1, \ldots \hat{c}_n\}$ then **return** 0
$\lfloor$ **return** $\pi(m, \mathsf{Dec}_{\mathsf{sk}}(\hat{c}_1), \ldots)$

$\mathcal{Q}_1^{\mathcal{B}}$
$\lceil\ (\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$\mathcal{M}_0 \leftarrow \mathcal{B}(\mathsf{pk})$
$m \leftarrow \mathcal{M}_0, \overline{m} \leftarrow \mathcal{M}_0$
$\overline{c} \leftarrow \mathsf{Enc}_{\mathsf{pk}}(\overline{m})$
$\pi(\cdot), \hat{c}_1, \ldots \hat{c}_n \leftarrow \mathcal{B}(\overline{c})$
if $\overline{c} \in \{\hat{c}_1, \ldots \hat{c}_n\}$ then **return** 0
$\lfloor$ **return** $\pi(m, \mathsf{Dec}_{\mathsf{sk}}(\hat{c}_1), \ldots)$

we get

$\mathcal{Q}_0^{\mathcal{B}}$
$\lceil (\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$\quad m \leftarrow \mathcal{M}$
$\quad c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m)$
$\quad \hat{c}_1 \leftarrow c \cdot \mathsf{Enc}_{\mathsf{pk}}(0)$
$\quad$ if $c = \hat{c}_1$ then **return** 0
$\lfloor$ **return** $[m \stackrel{?}{=} \mathsf{Dec}_{\mathsf{sk}}(\hat{c}_1)]$

$\mathcal{Q}_1^{\mathcal{B}}$
$\lceil (\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$\quad m \leftarrow \mathcal{M}, \overline{m} \leftarrow \mathcal{M}$
$\quad \overline{c} \leftarrow \mathsf{Enc}_{\mathsf{pk}}(\overline{m})$
$\quad \hat{c}_1 \leftarrow \overline{c} \cdot \mathsf{Enc}_{\mathsf{pk}}(0)$
$\quad$ if $c = \hat{c}_1$ then **return** 0
$\lfloor$ **return** $[m \stackrel{?}{=} \mathsf{Dec}_{\mathsf{sk}}(\hat{c}_1)]$

which further simplifies due to the properties of re-randomisation:

$\mathcal{Q}_0^{\mathcal{B}}$
$\lceil (\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$\quad m \leftarrow \mathcal{M}$
$\quad c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m)$
$\quad \hat{c}_1 \leftarrow c \cdot \mathsf{Enc}_{\mathsf{pk}}(0)$
$\quad$ if $c = \hat{c}_1$ then **return** 0
$\lfloor$ **return** $[m \stackrel{?}{=} m]$

$\mathcal{Q}_1^{\mathcal{B}}$
$\lceil (\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$\quad m \leftarrow \mathcal{M}, \overline{m} \leftarrow \mathcal{M}$
$\quad \overline{c} \leftarrow \mathsf{Enc}_{\mathsf{pk}}(\overline{m})$
$\quad \hat{c}_1 \leftarrow \overline{c} \cdot \mathsf{Enc}_{\mathsf{pk}}(0)$
$\quad$ if $c = \hat{c}_1$ then **return** 0
$\lfloor$ **return** $[m \stackrel{?}{=} \overline{m}]$.

From this simplified form it is evident that $\mathcal{Q}^{\mathcal{B}}$ can return zero only if $c = \hat{c}_1$. Let δ denote the corresponding probability that re-randomisation produces the same ciphertext:

$$\delta = \Pr[c = \hat{c}_1] = \frac{1}{|\mathsf{Enc}_{\mathsf{pk}}(m)|} \ .$$

It is relatively straightforward to prove that the number of potential ciphertexts must be the same for all messages. Usually, the number of potential ciphertexts is directly related to the size of randomness space $\mathcal{R}$ used during encryption operation. The game $\mathcal{Q}^{\mathcal{B}}$ can return one only if $m = \overline{m}$. Hence, the advantage

$$\mathsf{Adv}^{\mathsf{nm\text{-}cpa}}(\mathcal{B}) \geq 1 - \delta - \frac{1}{|\mathcal{M}_{\mathsf{pk}}|} \gg 0$$

is really noticeable. Since $\mathcal{B}$ is also efficient algorithm, the homomorphic encryption cannot be non-malleable for reasonable time bounds and success bounds.

Non-malleability implies indistinguishability. All three reductions that tie non-malleability with indistinguishability are very similar. The only difference is when the adversary can use decryption oracle. Therefore, we provide the construction for the most restricted case where the adversary has no access to decryption oracle. Let $\mathcal{A}$ be an adversary against IND-CPA games:

$\mathcal{G}_0^{\mathcal{A}}$
$\lceil (\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$\quad (m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk})$
$\quad c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_0)$
$\lfloor$ **return** $\mathcal{A}(c)$

$\mathcal{G}_1^{\mathcal{A}}$
$\lceil (\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$\quad (m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk})$
$\quad c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_1)$
$\lfloor$ **return** $\mathcal{A}(c)$.

Then we can construct an adversary $\mathcal{B}$ that encrypts the guess b of $\mathcal{A}$ as an encryption $\hat{c}_1$. By default the message space $\mathcal{M}_{\mathsf{pk}}$ does not have to contain elements 0 and 1. However, this is an easy problem to solve. W.l.o.g. we can assume that $\mathcal{A}$ outputs more probably 0 in the game $\mathcal{G}_0$ and 1 in the game $\mathcal{G}_1$. Then we can just encrypt $\mathsf{Enc}_{\mathsf{pk}}(m_b)$ as related ciphertext and check for equality as a relation. However, this can lead to

situations where the adversary with the correct guess is disqualified as $c = \hat{c}_1$. To avoid this problem, we can encrypt $\mathsf{Enc}_{\mathsf{pk}}(m_{1-b})$ as related ciphertext and check for inequality as a relation:

$$\begin{array}{l}\mathcal{B}(\mathsf{pk}) \\ \left[\begin{array}{l}(m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk}) \\ \textbf{return } \{m_0, m_1\}\end{array}\right.\end{array}$$

$$\begin{array}{l}\mathcal{B}(c) \\ \left[\begin{array}{l}\pi(m, \hat{m}_1) = [m \neq \hat{m}_1] \\ b \leftarrow \mathcal{A}(c) \\ \hat{c}_1 \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_{1-b}) \\ \textbf{return } (\pi, \hat{c}_1)\end{array}\right.\end{array}$$

If we inline the definition of the adversary into the games defining non-malleability we get simplified games:

$$\begin{array}{l}\mathcal{Q}_0^{\mathcal{B}} \\ \left[\begin{array}{l}(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen} \\ (m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk}) \\ m \xleftarrow{u} \{m_0, m_1\} \\ c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m) \\ b \leftarrow \mathcal{A}(c) \\ \hat{c}_1 \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_{1-b}) \\ \mathsf{if}\ c = \hat{c}_1\ \mathsf{then}\ \textbf{return } 0 \\ \textbf{return } [m \neq \mathsf{Dec}_{\mathsf{sk}}(\hat{c}_1)]\end{array}\right.\end{array} \qquad \begin{array}{l}\mathcal{Q}_1^{\mathcal{B}} \\ \left[\begin{array}{l}(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen} \\ (m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk}) \\ m \xleftarrow{u} \{m_0, m_1\}, \overline{m} \xleftarrow{u} \{m_0, m_1\} \\ \overline{c} \leftarrow \mathsf{Enc}_{\mathsf{pk}}(\overline{m}) \\ b \leftarrow \mathcal{A}(\overline{c}) \\ \hat{c}_1 \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_{1-b}) \\ \mathsf{if}\ c = \hat{c}_1\ \mathsf{then}\ \textbf{return } 0 \\ \textbf{return } [m \neq \mathsf{Dec}_{\mathsf{sk}}(\hat{c}_1)]\end{array}\right.\end{array}$$

which can be further simplified:

$$\begin{array}{l}\mathcal{Q}_0^{\mathcal{B}} \\ \left[\begin{array}{l}(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen} \\ (m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk}) \\ m \xleftarrow{u} \{m_0, m_1\} \\ c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m) \\ b \leftarrow \mathcal{A}(c) \\ \hat{c}_1 \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_{1-b}) \\ \mathsf{if}\ c = \hat{c}_1\ \mathsf{then}\ \textbf{return } 0 \\ \textbf{return } [m \neq m_{1-b}]\end{array}\right.\end{array} \qquad \begin{array}{l}\mathcal{Q}_1^{\mathcal{B}} \\ \left[\begin{array}{l}(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen} \\ (m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk}) \\ m \xleftarrow{u} \{m_0, m_1\}, \overline{m} \xleftarrow{u} \{m_0, m_1\} \\ \overline{c} \leftarrow \mathsf{Enc}_{\mathsf{pk}}(\overline{m}) \\ b \leftarrow \mathcal{A}(\overline{c}) \\ \hat{c}_1 \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_{1-b}) \\ \mathsf{if}\ c = \hat{c}_1\ \mathsf{then}\ \textbf{return } 0 \\ \textbf{return } [m \neq m_{1-b}]\ .\end{array}\right.\end{array}$$

The game $\mathcal{Q}_1^{\mathcal{B}}$ can end with one only if $m \neq m_{1-b}$. Since b is independent from m and there are at most two options for value of m, we can easily derive

$$\Pr\left[\mathcal{Q}_1^{\mathcal{B}} = 1\right] \leq \Pr\left[m \stackrel{?}{=} m_b\right] \leq \frac{1}{2}\ .$$

The analysis of $\mathcal{Q}_0^{\mathcal{B}}$ requires decomposition:

$$\Pr\left[\mathcal{Q}_0^{\mathcal{B}} = 1\right] = \Pr\left[\mathcal{Q}_0^{\mathcal{B}} = 1 \wedge m_0 = m_1\right] + \Pr\left[\mathcal{Q}_0^{\mathcal{B}} = 1 \wedge m_0 \neq m_1\right] = \Pr\left[\mathcal{Q}_0^{\mathcal{B}} = 1 \wedge m_0 \neq m_1\right]\ .$$

Note that the last equality follows form the fact that if $m_0 = m_1$ then m cannot be different from m_{1-b}. Further decomposition according to the value of m yields to two probabilities

$$\Pr\left[\mathcal{Q}_0^{\mathcal{B}} = 1 \wedge m_0 \neq m_1\right] = \Pr\left[\mathcal{Q}_0^{\mathcal{B}} = 1 \wedge m_0 \neq m_1 \wedge m = m_0\right] + \Pr\left[\mathcal{Q}_0^{\mathcal{B}} = 1 \wedge m_0 \neq m_1 \wedge m = m_1\right]\ ,$$

which can be modelled with the following games:

$\mathcal{Q}_2^{\mathcal{B}}$

$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$(m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk})$
if $m_0 = m_1$ then **return** 0
$m \xleftarrow{u} \{m_0, m_1\}$
if $m \neq m_0$ then **return** 0
$c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_0)$
$b \leftarrow \mathcal{A}(c)$
$\hat{c}_1 \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_{1-b})$
if $c = \hat{c}_1$ then **return** 0
return $[b \stackrel{?}{=} 0]$

$\mathcal{Q}_3^{\mathcal{B}}$

$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$(m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk})$
if $m_0 = m_1$ then **return** 0
$m \xleftarrow{u} \{m_0, m_1\}$
if $m \neq m_1$ then **return** 0
$c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_1)$
$b \leftarrow \mathcal{A}(c)$
$\hat{c}_1 \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_{1-b})$
if $c = \hat{c}_1$ then **return** 0
return $[b \stackrel{?}{=} 1]$.

As the second check in both games succeeds with probability $\frac{1}{2}$ we can express

$$\Pr\left[\mathcal{Q}_0^{\mathcal{B}} = 1\right] = \tfrac{1}{2} \cdot \Pr\left[\mathcal{Q}_4^{\mathcal{B}} = 1\right] + \tfrac{1}{2} \cdot \Pr\left[\mathcal{Q}_5^{\mathcal{B}} = 1\right]$$

where the games $\mathcal{Q}_4$ and $\mathcal{Q}_5$ are very close to IND-CPA games:

$\mathcal{Q}_4^{\mathcal{B}}$

$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$(m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk})$
if $m_0 = m_1$ then **return** 0
$c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_0)$
$b \leftarrow \mathcal{A}(c)$
$\hat{c}_1 \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_b)$
if $c = \hat{c}_1$ then **return** 0
return $[b \stackrel{?}{=} 0]$

$\mathcal{Q}_5^{\mathcal{B}}$

$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$(m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk})$
if $m_0 = m_1$ then **return** 0
$c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_1)$
$b \leftarrow \mathcal{A}(c)$
$\hat{c}_1 \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_b)$
if $c = \hat{c}_1$ then **return** 0
return $[b \stackrel{?}{=} 1]$.

In particular, note that the last condition holds in the games then the check $c = \hat{c}_1$ can never hold as we encrypt a different message m_{1-b}. Thus, we can further simplify games without changing the output distributions:

$\mathcal{Q}_4^{\mathcal{B}}$

$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$(m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk})$
if $m_0 = m_1$ then **return** 0
$c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_0)$
$b \leftarrow \mathcal{A}(c)$
return $[b \stackrel{?}{=} 0]$

$\mathcal{Q}_5^{\mathcal{B}}$

$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$(m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk})$
if $m_0 = m_1$ then **return** 0
$c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_1)$
$b \leftarrow \mathcal{A}(c)$
return $[b \stackrel{?}{=} 1]$.

Now it is straightforward to see that

$$\begin{aligned}\Pr\left[\mathcal{Q}_4^{\mathcal{B}} = 1\right] + \Pr\left[\mathcal{Q}_5^{\mathcal{B}} = 1\right] &= 1 - \Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1 \wedge m_0 \neq m_1\right] + \Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1 \wedge m_0 \neq m_1\right] \\ &= 1 + \mathsf{Adv}^{\mathsf{ind\text{-}cpa}}(\mathcal{A}) \ ,\end{aligned}$$

since the choice $m_0 = m_1$ does not contribute to IND-CPA advantage and we assumed that the adversary $\mathcal{A}$ predicts the bit correctly. As a result, we have proven

$$\Pr\left[\mathcal{Q}_0^{\mathcal{B}} = 1\right] = \frac{1}{2} + \frac{1}{2} \cdot \mathsf{Adv}^{\mathsf{ind\text{-}cpa}}(\mathcal{A})$$

which implies that

$$\mathsf{Adv}^{\mathsf{nm\text{-}cpa}}(\mathcal{B}) = \frac{1}{2} + \frac{1}{2} \cdot \mathsf{Adv}^{\mathsf{ind\text{-}cpa}}(\mathcal{A}) - \frac{1}{2} = \frac{1}{2} \cdot \mathsf{Adv}^{\mathsf{ind\text{-}cpa}}(\mathcal{A})$$

Since the running times of $\mathcal{A}$ and $\mathcal{B}$ are comparable and $\mathcal{B}$ is well defined, we have established that (t, ε)-secure NM-CPA encryption scheme is also $(t, 2\varepsilon)$-secure IND-CPA encryption scheme.

The same construction is applicable for the reductions NM-CCA1 $\Rightarrow$ IND-CCA1 and NM-CCA2 $\Rightarrow$ IND-CCA2, as the adversary $\mathcal{B}$ makes oracle calls in right phases.

Limits of non-malleability definition. Note that the target relation π is defined only after the adversary has seen the ciphertext c. Hence, we can stretch the limits of the non-malleability games and allow attacks where no related ciphertexts are defined:

$\mathcal{Q}_0^{\mathcal{B}}$
$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$\mathcal{M}_0 \leftarrow \mathcal{B}(\mathsf{pk})$
$m \leftarrow \mathcal{M}_0$
$c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m)$
$\pi(\cdot) \leftarrow \mathcal{B}(c)$
return $\pi(m)$

$\mathcal{Q}_1^{\mathcal{B}}$
$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$\mathcal{M}_0 \leftarrow \mathcal{B}(\mathsf{pk})$
$m \leftarrow \mathcal{M}_0, \overline{m} \leftarrow \mathcal{M}_0$
$\overline{c} \leftarrow \mathsf{Enc}_{\mathsf{pk}}(\overline{m})$
$\pi(\cdot) \leftarrow \mathcal{B}(\overline{c})$
return $\pi(m)$.

In this attack is a legitimate attack against non-malleability, then $\mathcal{B}$ can directly define $\pi(m) = [m \stackrel{?}{=} m_b]$ and output no additional ciphertexts:

$\mathcal{B}(\mathsf{pk})$
$(m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk})$
return $\{m_0, m_1\}$

$\mathcal{B}(c)$
$b \leftarrow \mathcal{A}(c)$
$\pi(m) = [m \stackrel{?}{=} m_b]$
return π .

The success analysis of this adversary is analogous and slightly simpler as we do not have to worry that related ciphertexts coincide with the challenge ciphertext c.

Even if such a natural extension to non-malleability definition is not allowed, we can still use the same relation by ignoring all messages corresponding to related ciphertexts $\hat{c}_1, \ldots, \hat{c}_n$. The analysis would be analogous again. However, we should then estimate the probability that $c \in \{\hat{c}_1, \ldots, \hat{c}_n\}$ which is negligible if we generate $\hat{c}_1, \ldots, \hat{c}_n$ as valid encryptions of random message space elements.