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

Exercise (NM-CPA security for inequality relation). *Explain why IND-CPA adversary $\mathcal{A}$ can be converted to the adversary $\mathcal{B}$ against non-malleability game for inequality relation*

```
$\mathcal{Q}_0$
    $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
    $\mathcal{M}_0 \leftarrow \mathcal{B}(\mathsf{pk})$
    $m \leftarrow \mathcal{M}_0$
    $c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m)$
    $\hat{c} \leftarrow \mathcal{B}(c)$
    if $c = \hat{c}$ then return $0$
    return $m \neq \mathsf{Dec}_{\mathsf{sk}}(\hat{c})$
```

```
$\mathcal{Q}_1$
    $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
    $\mathcal{M}_0 \leftarrow \mathcal{B}(\mathsf{pk})$
    $m, \overline{m} \leftarrow \mathcal{M}_0$
    $\overline{c} \leftarrow \mathsf{Enc}_{\mathsf{pk}}(\overline{m})$
    $\hat{c} \leftarrow \mathcal{B}(\overline{c})$
    if $c = \hat{c}$ then return $0$
    return $m \neq \mathsf{Dec}_{\mathsf{sk}}(\hat{c})$
```

How does the analysis change if we consider equality relation

Solution. **Hint:** What would be the best option to win the game if $\mathcal{A}$ is a perfect adversary against IND-CPA games?