Homework 3

1. (10 + 10 + 10 points) Consider the following two-party functionalities.

> OT-channel:
>
> - Input: Sender has inputs $(x_0, x_1) \in \{0,1\}^2$ and Receiver has no input.
> - Output: Let $b \xleftarrow{\$} \{0,1\}$ and define $z := x_b$. Output (b, z) to the Receiver and nothing to the Sender.

> OT:
>
> - Input: Sender has inputs $(x_0, x_1) \in \{0,1\}^2$ and Receiver has input $b \in \{0,1\}$.
> - Output: Let $z := x_b$ and output z to the Receiver and nothing to the Sender.

Using one copy of OT-channel, construct one copy of OT against semi-honest adversaries. Give the protocol and the two simulation strategies to exhibit the protocol's semi-honest security.

2. (20 points) Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be multiplicative groups. Let g be a generator of the group $\mathbb{G}_1$ and $q = |\mathbb{G}_1|$. Suppose their exists a bilinear map $e\colon \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ with the following property: $e(g^a, g^b) = e(g, g)^{ab}$, where $a, b \in \{0, \ldots, q-1\}$ and $e(g, g)$ is a generator of the group $\mathbb{G}_2$.

Consider the following two computational assumptions:

> Assumption 1:
>
> - $\mathcal{D}_0 = (g, g^a, g^b, g^c, g^{abc})$, where $a, b, c \xleftarrow{\$} \{0, \ldots, q-1\}$.
> - $\mathcal{D}_1 = (g, g^a, g^b, g^c, g^d)$, where $a, b, c, d \xleftarrow{\$} \{0, \ldots, q-1\}$.
>
> Assumption: $\mathcal{D}_0 \approx_c \mathcal{D}_1$.

> Assumption 2:
>
> - $\mathcal{C}_0 = (g, g^a, g^b, g^c, e(g, g)^{abc})$, where $a, b, c \xleftarrow{\$} \{0, \ldots, q-1\}$.
> - $\mathcal{C}_1 = (g, g^a, g^b, g^c, e(g, g)^d)$, where $a, b, c, d \xleftarrow{\$} \{0, \ldots, q-1\}$.
>
> Assumption: $\mathcal{C}_0 \approx_c \mathcal{C}_1$.

Show that: Assumption 1 implies Assumption 2.