a) Game 0:

Chal. $\xleftarrow{\text{for } i=1,\dots q:\ m_{i0}, m_{i1}}$ Adv. A

$b \in \{0,1\}$ $k \xleftarrow{R} K$ $\xrightarrow{c_{i0}, c_{i1}}$ $\downarrow b'$

$$Adv_{CPA}[A,E] = |Pr[EXP(0)=1] - Pr[EXP(1)=1]| = |Pr[W_0] - \tfrac{1}{2}|$$

Game 1:

Chal. $\xleftarrow{\text{for } i=1,\dots q\ \ m_{i0}, m_{i1}}$ Adv. B

$k \xleftarrow{R} K$ $\xrightarrow{c_{i0}, c_{i1}}$

$$Adv_{CPA}[B,E_1] = |Pr[W_0] - Pr[W_1]|$$

~~$\because |Pr[W_0] - \frac{1}{2}| = Adv_{SS}[B, E_0]$~~

~~$\therefore Adv_{CPA}[A,E] = Adv_{SS}[B,E_0] \cdot q + Adv_{CPA}[B,E_1]$~~

$$\therefore Adv_{CPA}[A,E] = \underbrace{Adv_{SS}[B,E_0]}_{\downarrow \text{negligible}} \cdot q + \underbrace{Adv_{CPA}[B,E_1]}_{\downarrow \text{negligible}}$$

$\therefore (E,D)$ is a secure CPA.

b)

$$Adv_{CPA}[A',E'] = 2\,Adv_{CPA}[B,E_1] + q \cdot Adv_{SS}[B,E_0]$$

is negligible.

b2)

Alice $x_a \leftarrow a + k_0$ ⟶ Sam ⟵ $r, x_b = r(b+k_0)+k_1$ Bob.

a. ⟵ $x \leftarrow r x_a - x_b$ b.

① Conditions: Sam cannot change any of the values, and Sam is safe enough and Sam cannot get any value.

② If k_0, k_1 are used more than once:

$r_1, x_{b1} = r(b+k_0)+k_1$

Sam ⟵ $r_2, x_{b2} = r(b+k_0')+k_1'$ Bob.

$r_3, x_{b3} = r(b+k_0'')+k_1''$

...

Obviously, Sam know these values b, k_0, k_1, so it's not secure.

③ Make a PRF: $K \times Z_B \to Z_p$.

And the PRF is secure.