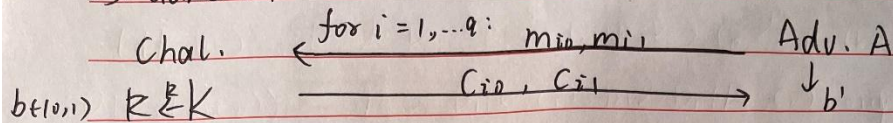
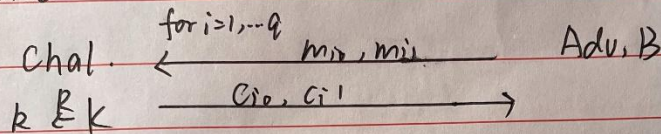


a) Game 0:



$$\text{Adv}_{\text{CPA}}[A, E] = |\Pr[\text{Exp}(1_0)=1] - \Pr[\text{Exp}(1_1)=1]| = |\Pr[w_0] - \frac{1}{2}|$$

Game 1:



$$\text{Adv}_{\text{CPA}}[A, E] = |\Pr[w_0] - \Pr[w_1]|$$

$$\therefore |\Pr[w_0] - \frac{1}{2}| = \text{Adv}_{\text{CPA}}[B, E_0]$$

$$\therefore \text{Adv}_{\text{CPA}}[A, E] = \text{Adv}_{\text{CPA}}[B, E_0]$$

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

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

b)

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

is negligible.



12)

Alice:  $x_a \leftarrow a + k_0$ , Sam:  $\leftarrow r, x_b = r(b + k_0) + k_1$  Bob:  
 $\xleftarrow{a} x \leftarrow rx_a - x_b$  b.

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

②.  $r$  are used  
 If  $k_0, k_1$  more than once:

Sam:  $\leftarrow r_1, x_{b1} = r(b + k_0) + k_1$   
 $\leftarrow r_2, x_{b2} = r(b + k_0') + k_1'$  Bob:  
 $\leftarrow r_3, x_{b3} = r(b + k_0'') + k_1''$   
 ...

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

③ Make a PRF:  $K \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ .

And the PRF is secure.