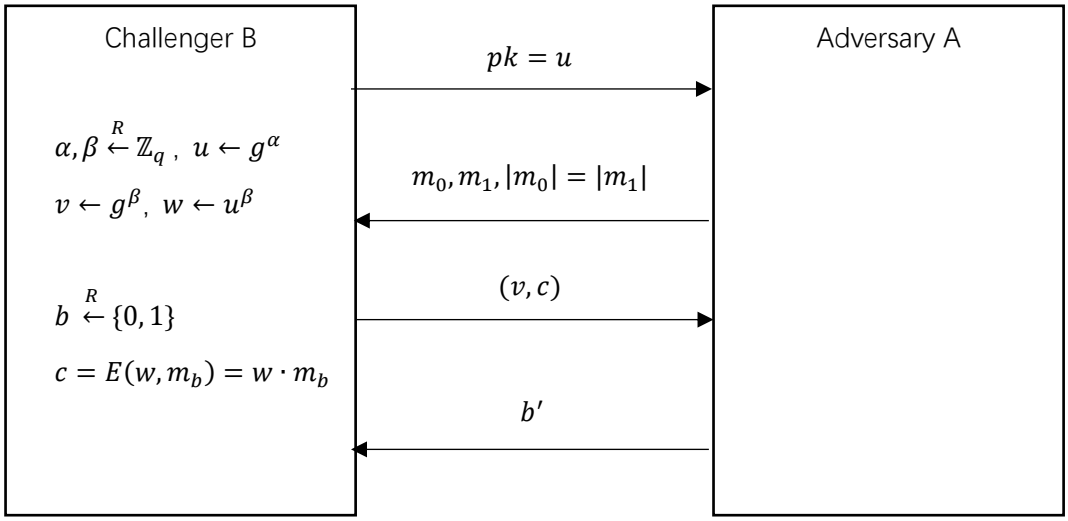
1. Protocol: First Alice send $\hat{m} = H(m) \cdot g^{\rho}$ to Bob. Then Bob calculates $(\hat{m})^k$ and send $(\hat{m})^k$ and g^k to Alice.
   Alice can obtain $F(k, m)$ by following way:

$$\frac{(\hat{m})^k}{(g^k)^{\rho}} = \frac{(H(m) \cdot g^{\rho})^k}{(g^k)^{\rho}} = \frac{H(m)^k \cdot g^{\rho k}}{g^{\rho k}} = H(m)^k = F(k, m)$$

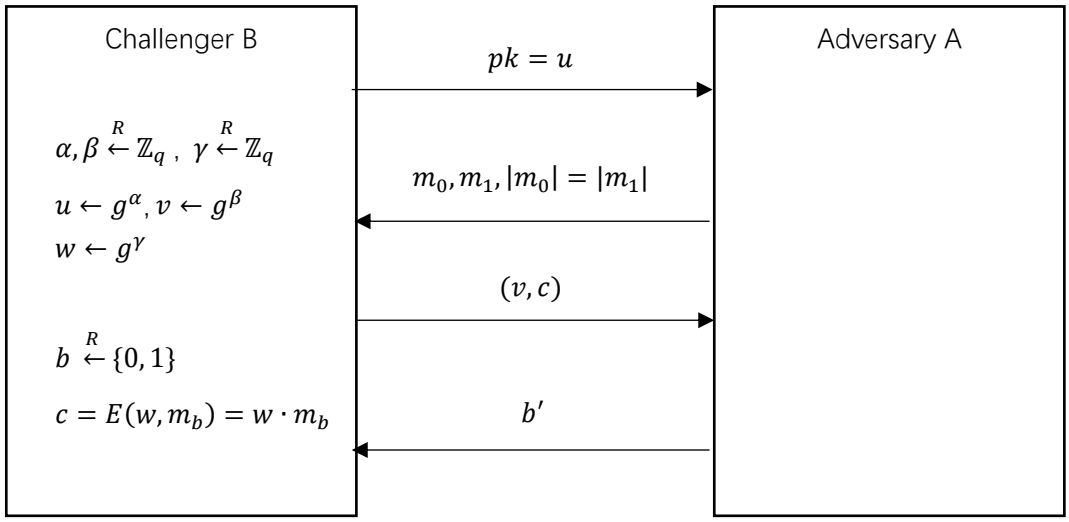
2. **Theorem:** If a public-key encryption scheme ε is semantically secure, then it is also CPA secure.
   a) Therefore, we prove that $E_{MEG} = (G, E, D)$ is CPA semantically secure is to prove that E_{MEG} is semantically secure.

Game 0

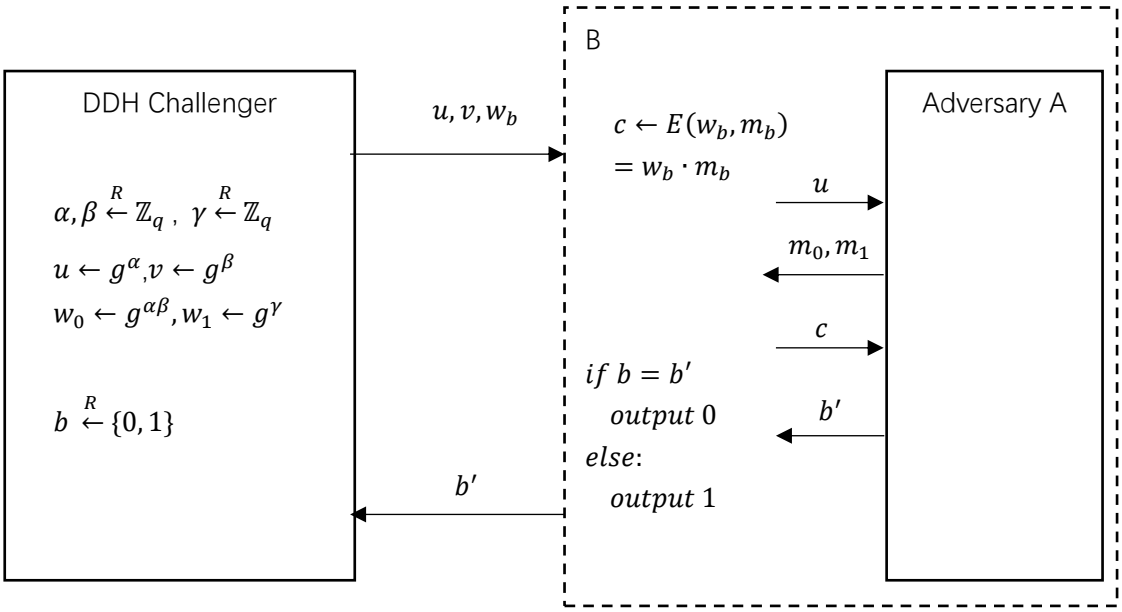


$$SS^*_{adv}[A, E_{MEG}] = \left|\Pr[W_0] - \frac{1}{2}\right|$$

Game 1



$$\left|\Pr[W_1] - \frac{1}{2}\right| = 0$$



$$|\Pr[W_0] - \Pr[W_1]| = DDHadv[B_{ddh}, \mathbb{G}].$$

Then we can get

$$SS^*_{adv}[A, E_{MEG}] = \left|\Pr[W_0] - \frac{1}{2}\right|$$

$$|\Pr[W_0] - \Pr[W_1]| = DDHadv[B_{ddh}, \mathbb{G}].$$

$$\left|\Pr[W_1] - \frac{1}{2}\right| = 0$$

Therefore,

$$SS^*_{adv}[A, E_{MEG}] \leq DDHadv[B_{ddh}, \mathbb{G}]$$

E_{MEG} is CPA semantically secure assuming the DDH assumption holds in G.

b) if the DDH assumption does not hold in G. Then we can find $\gamma \overset{R}{\leftarrow} \mathbb{Z}_q$ to make the following two probability distributions **computationally distinguishable:**

$$(g^{\alpha}, g^{\beta}, g^{\alpha\beta}) \ and \ (g^{\alpha}, g^{\beta}, g^{\gamma})$$

Therefore, $DDHadv[B_{ddh}, \mathbb{G}]$ is **not negligible**. E_{MEG} is not semantically secure.

c) Prove: E_{MEG} has a multiplicative homomorphism.

$$c_1 = E(pk, m_1) = g^{\alpha\beta} \cdot m_1$$

$$c_2 = E(pk, m_2) = g^{\alpha\beta} \cdot m_2$$

$$c = \frac{c_1 \cdot c_2}{g^{\alpha\beta}} = \frac{g^{\alpha\beta} \cdot m_1 \cdot g^{\alpha\beta} \cdot m_2}{g^{\alpha\beta}} = g^{\alpha\beta} \cdot (m_1 \cdot m_2) = E(pk, m_1 \cdot m_2)$$

d) Solution:

We can construct the message m into the following form:

$$m' = g^m$$

Then we can make the Elgamal encryption additive homomorphic:

$$c_1 = E(pk, m_1') = g^{\alpha\beta} \cdot g^{m_1}$$

$$c_2 = E(pk, m_2') = g^{\alpha\beta} \cdot g^{m_2}$$

$$c = \frac{c_1 \cdot c_2}{g^{\alpha\beta}} = \frac{g^{\alpha\beta} \cdot g^{m_1} \cdot g^{\alpha\beta} \cdot g^{m_2}}{g^{\alpha\beta}} = g^{\alpha\beta} \cdot g^{m_1+m_2} = E(pk, g^{m_1+m_2})$$

Drawbacks:

When we decrypt, we can only get $g^{m_1+m_2}$, and it is difficult to calculate $m_1 + m_2$ from $g^{m_1+m_2}$.