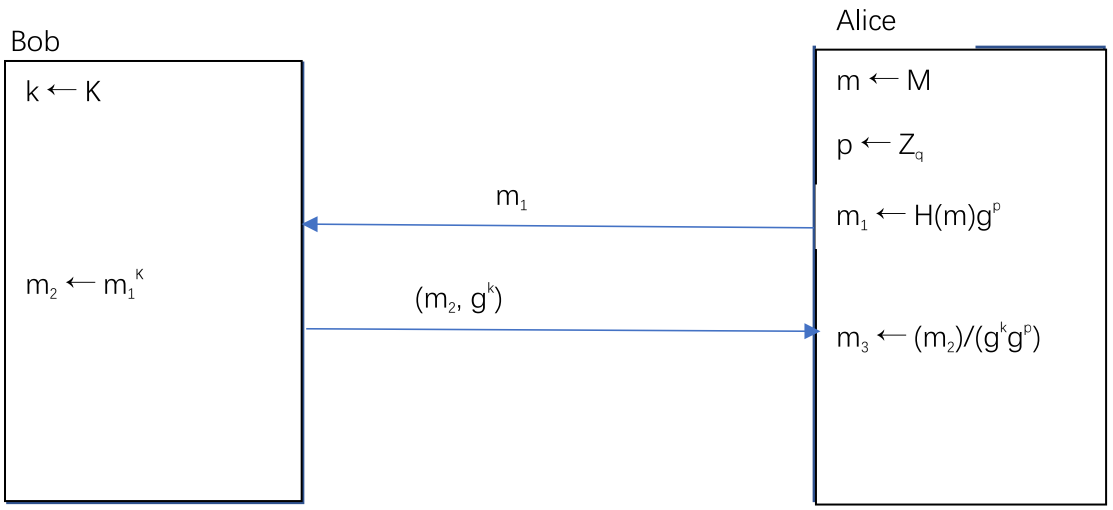
CSCI971 Modern Cryptography Assignment 8

Author: Weijian Ye

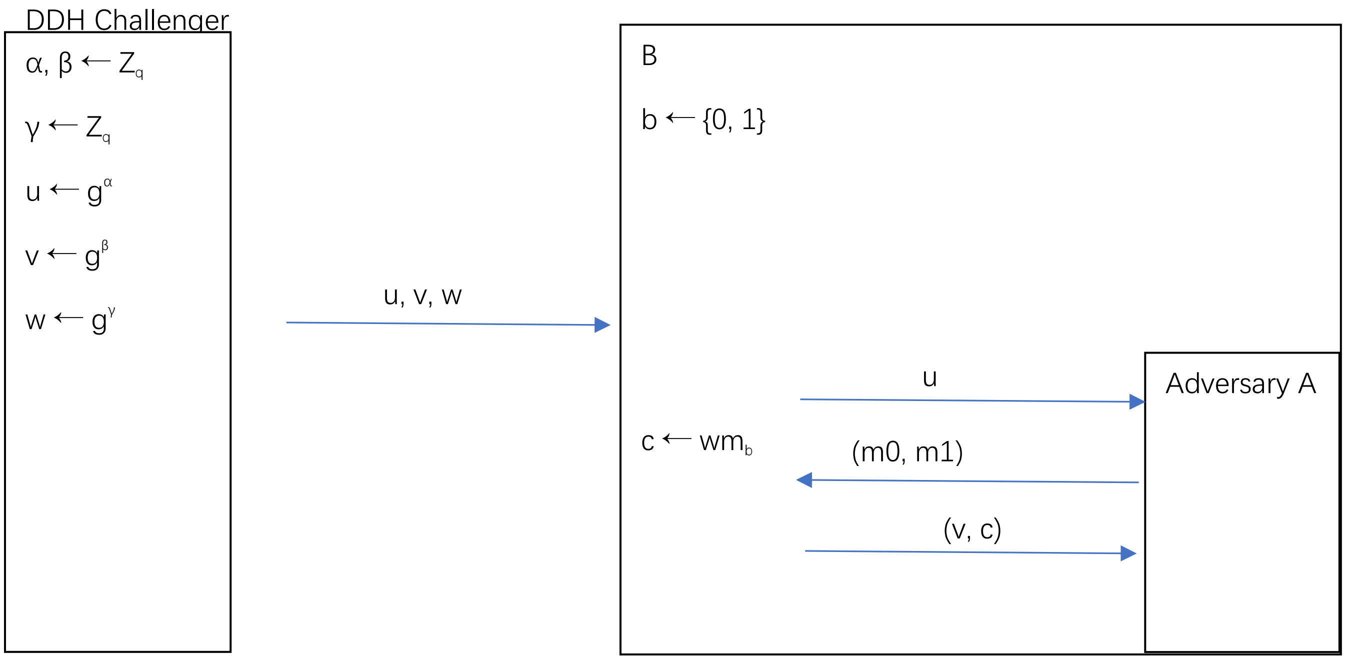
1.



$m_3 = [H(m)g^p]^k/(g^k g^p) = H(m)^k$

2.

(1)



Between A and B, there is SSadv*[A, E_{MEG}] = | Pr[W_0] – 1/2|

Between DDH challenger and B, there is DDHadv[B_{ddh}, G] = |Pr[W_0] – Pr[W_1]|

There is also Pr[W_1] = ½

According to equations above, SSadv*[A, E_{MEG}] = DDHadv[$_{Bddh}$, G]

Thus, E_{MEG} is semantically secure if DDH assumption holds in G.

(2)

|Pr[W0] – Pr[W1]| = DDHadv[B_{ddh}, G]

If DDH assumption does not hold in G, DDHadv[B_{ddh}, G] is not negligible.

Thus, adversary can distinguish whether a tuple (u, v, w) is DH-triple or not.

Therefore, SSadv[A, E_{MEG}] = 1.

(3)

$c_1 \leftarrow E(pk, m_1) = u^{\alpha}m_1$

$c_2 \leftarrow E(pk, m_2) = u^{\beta}m_2$

Thus $c_1c_2 = u^{\alpha}m_1u^{\beta}m_2 = u^{\alpha+\beta} m_1m_2$

$c \leftarrow E(pk, m_1m_2) = u^{\alpha+\beta}m_1m_2$

Therefore c_1c_2 equals to c.

(4)

According to the solution in the previous question, we already have a solution for E(pk, m_1) * E(pk, m_2) = E(pk, m_1 * m_2). We then replace m with g^{m}.

$c_1 \leftarrow E(pk, g^{m1}) = u^{\alpha}g^{m1}$

$c_2 \leftarrow E(pk, g^{m2}) = u^{\beta}g^{m2}$

With this transformation, $E(pk, g^{m1})E(pk, g^{m2}) = E(pk, g^{m1}g^{m2}) = E(pk, g^{m1+m2})$. Now we have an additive homomorphic property.