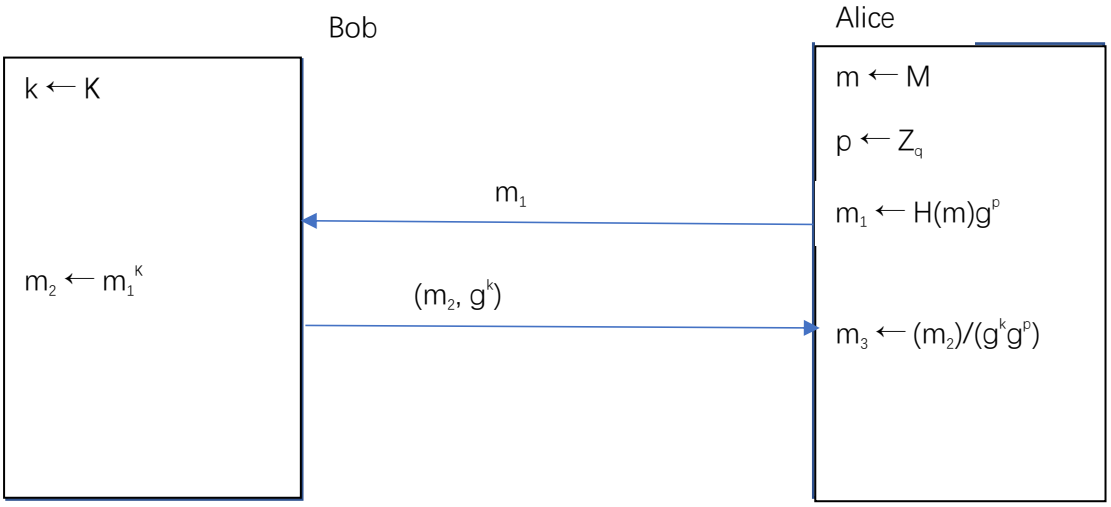
CSCI971 Modern Cryptography Assignment 8

Author: Weijian Ye

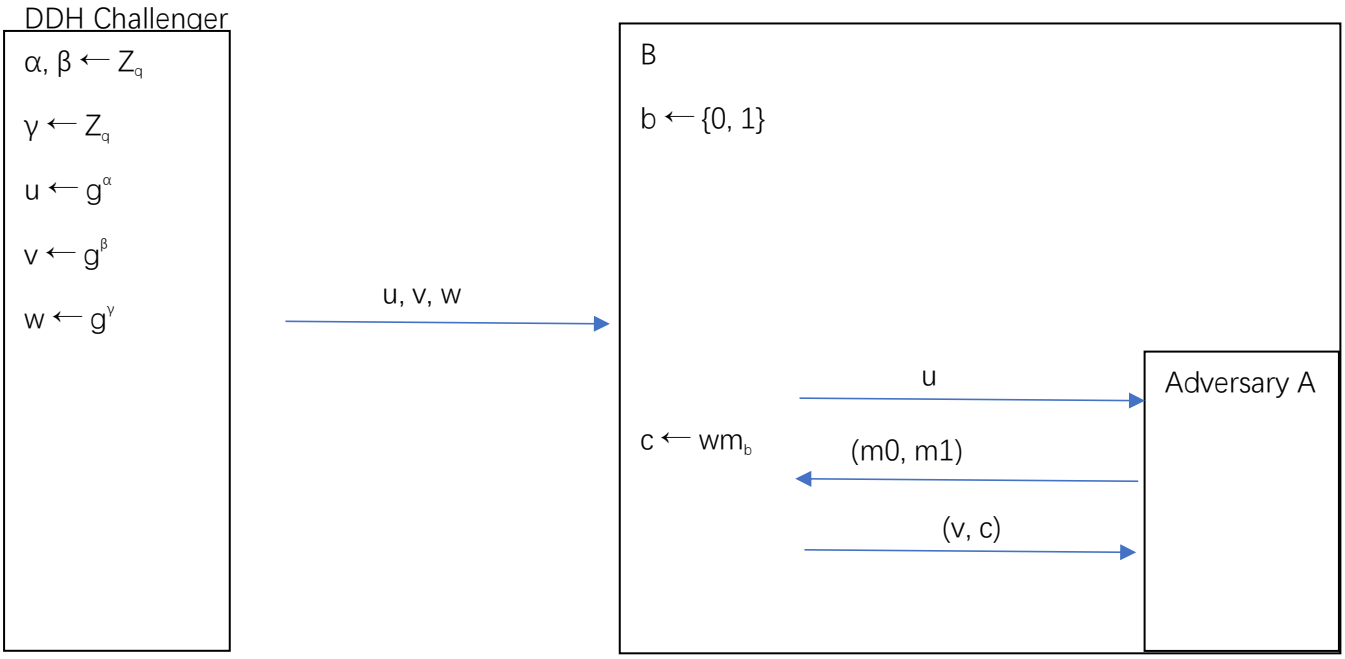
1.



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

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.