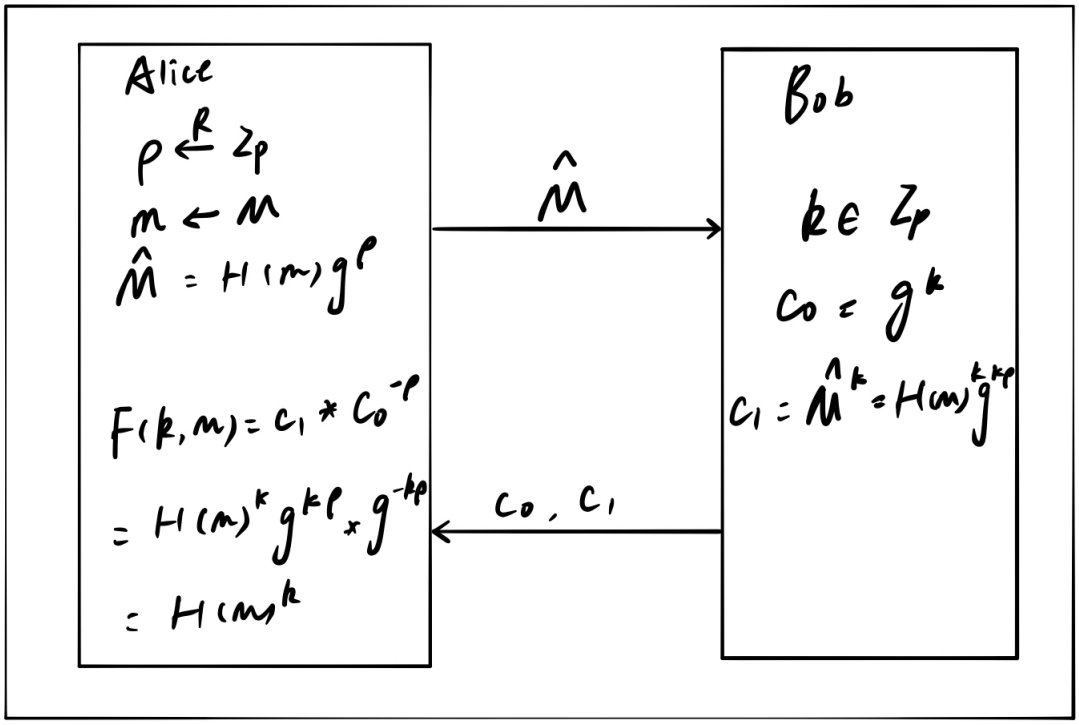
Homework 9: Digital Signature: Due by 12:00AM Thursday, 5 December 2019

Yao Xiao

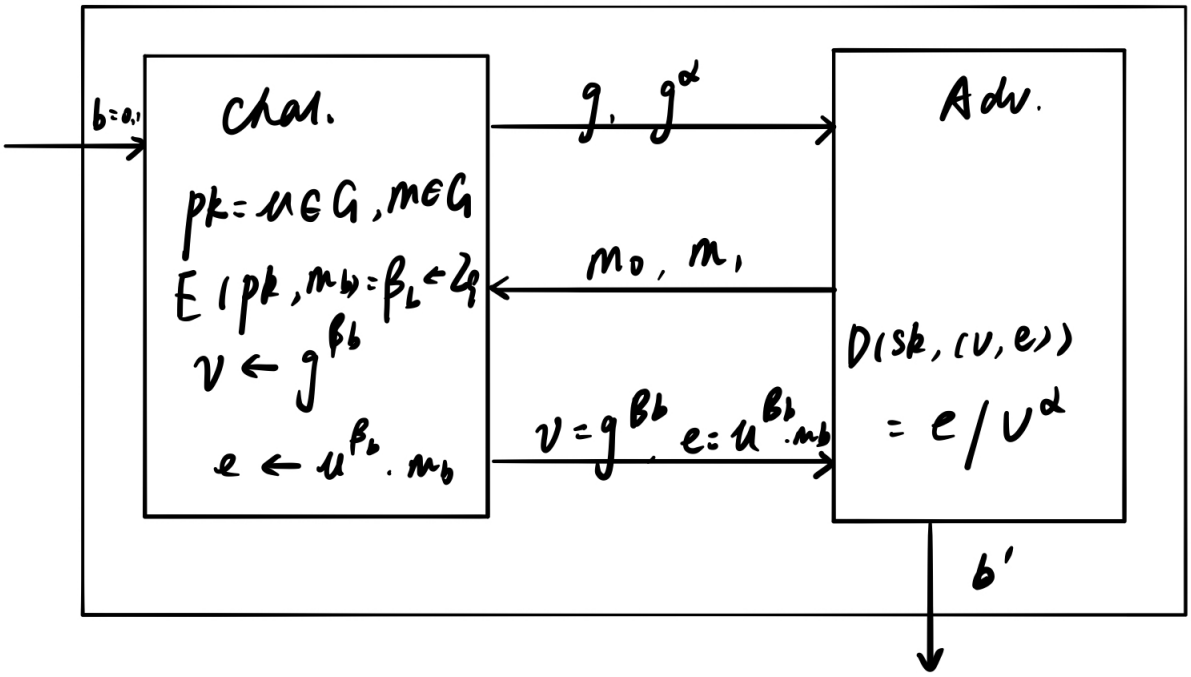
January 1, 2020

1. Answer to question 1:



Finally, Alice compute $u = H(m)^k \cdot g^{p \cdot k} \cdot g^{-p \cdot k} = H(m)^k$, and get $F(k, m) = H(m)^k$

2. Answer to question 2:

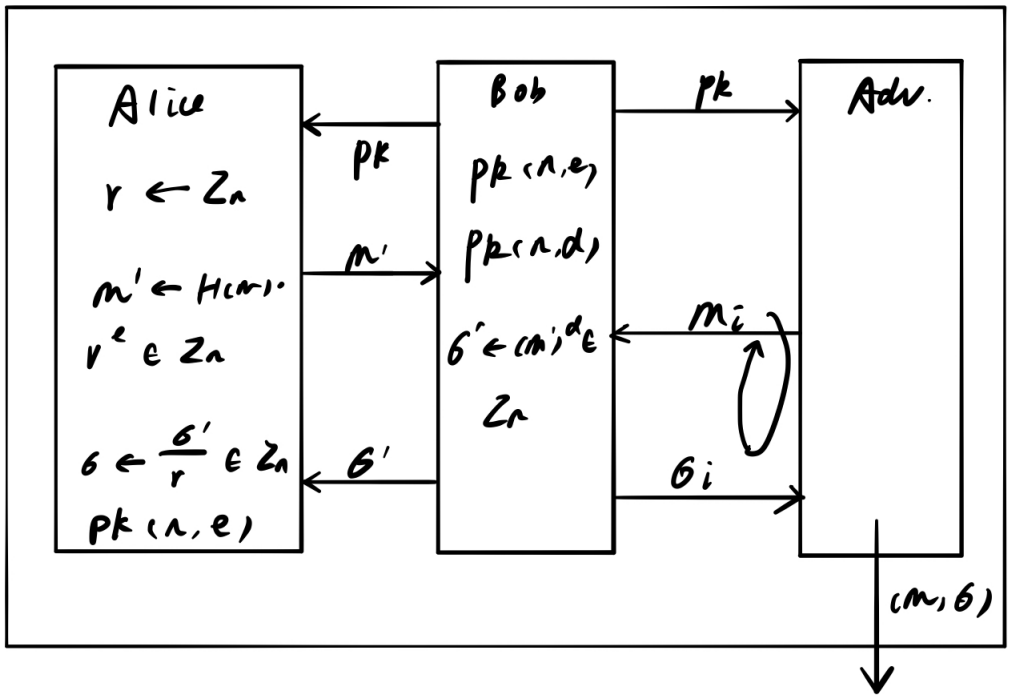


(a) In DHH assumption, adv. can't distinguish $g^{\alpha\cdot\beta}$ and g^c, if chal. encrypt the m_0 and send (v,e), adv. can not know v^α whether is $g^{\alpha\cdot\beta_0}$ or $g^{\alpha\cdot\beta_1}$, in the end it can't be distinguished from $(g^\alpha, g^\beta, g^{\alpha\cdot\beta})$ and (g^α, g^β, g^c).
So $Adv_S S[A, E] = |Pr[W_0] - Pr[W_1]|$ is negligible, the E_{MEG} is semantically secure.

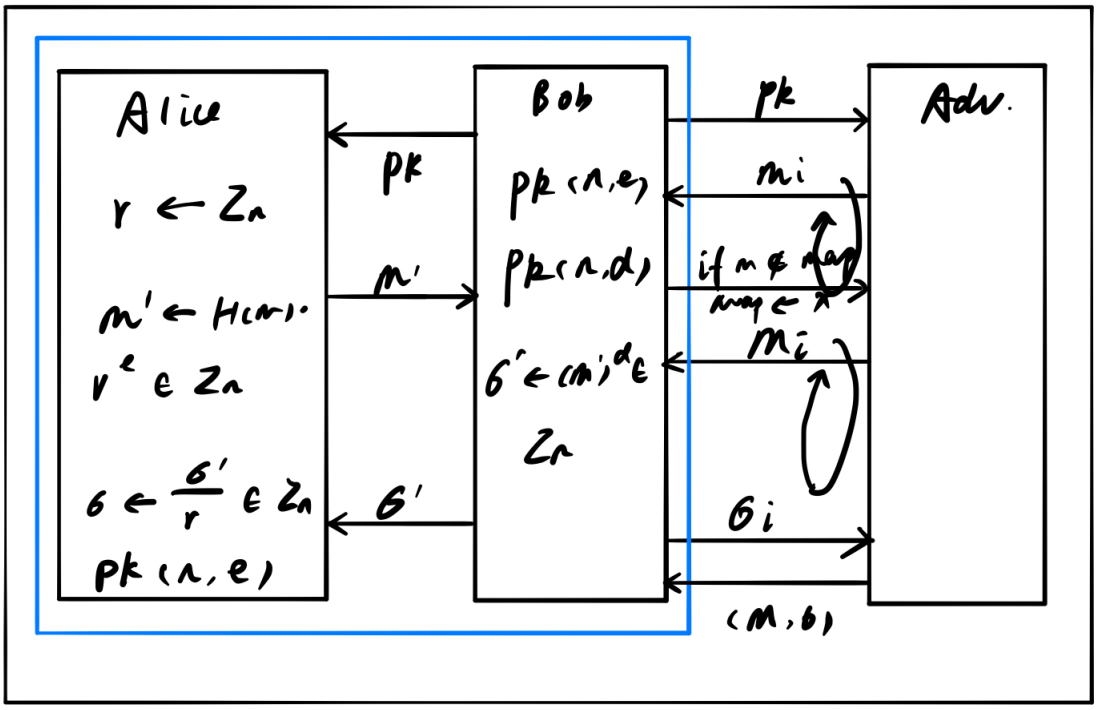
(b) If DHH assumption does note hold in G, adv. can distinguish $g^{\alpha\cdot\beta}$ and g^c, if chal. encrypt hte m_0 and send (v,e), adv. can know v^α whether is $g^{\alpha\cdot\beta_0}$ or $g^{\alpha\cdot\beta_1}$, in the end it can't be distinguished from $(g^\alpha, g^\beta, g^{\alpha\cdot\beta})$ and (g^α, g^β, g^c). or not.
So $Adv_S S[A, E] = |Pr[W_0] - Pr[W_1]| = 1$, the E_{MEG} is not semantic secure.

(c) when adv. compute $m_1 \cdot m_2 = D(sk, (v_1, e_1)) \cdot D(sk, (v_2, e_2)) = (e_1/v_1^\alpha) \cdot (e_2/v_1^\alpha)$
$\frac{u^\gamma \cdot (m_1 \cdot m_2 h)}{g^{\alpha\gamma}} = (u^\gamma \cdot (m_1 \cdot m_2)/g^{\alpha\gamma}) = m_1 \cdot m_2$
when chal. encrypt $m_1 \cdot m_2$ and $E(pk, (m_1 \cdot m_2)) = c$
$m_1 \cdot m_2 = \frac{u^c \cdot (m_1 \cdot m_2)}{g^{\alpha^c}} = (u^c \cdot (m_1 \cdot m_2/g^{\alpha^c}) = (u^\gamma \cdot (m_1 \cdot m_2)/g^{\alpha^\gamma})$
$c = \gamma = \beta_1 + \beta_2$
$E(pk, (m_1 \cdot m_2)) = c = \beta_1 + \beta_2$
So it is a multiplicative homomorphism.

3. Answer to question 3:



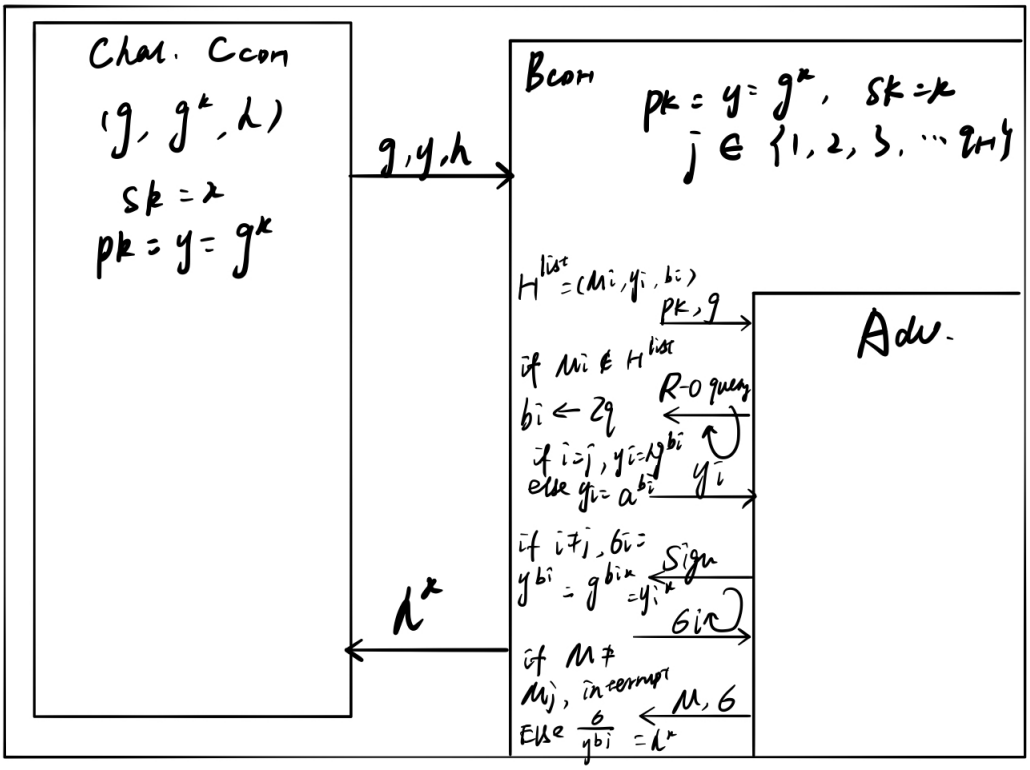
(a)



(b)

4. Answer to question 4:

(a) D $= g^a, h^b, e(g^a, g^b) \in G^4$ is a DH-tuple if $\alpha\beta = \gamma$. Then $\alpha\beta = \gamma \Leftrightarrow e(g^\alpha, g^\beta) = e(g, g^\gamma)$
In DDH assumption, when you get $g^a, h^b, e(g^a, g^b) == e(g, h)^{ab}$ can be computed. Once knowing $e(g, h)^{ab}$, it can see which group is $(g^a, h^b, e(g, h)^{ab})$.



(b)

$\sigma = y_j^x = (hg^{b_j})^x = h^x g^{b_j x} = h^x (g^x)^{b_j} = h^x y^{b_j}$