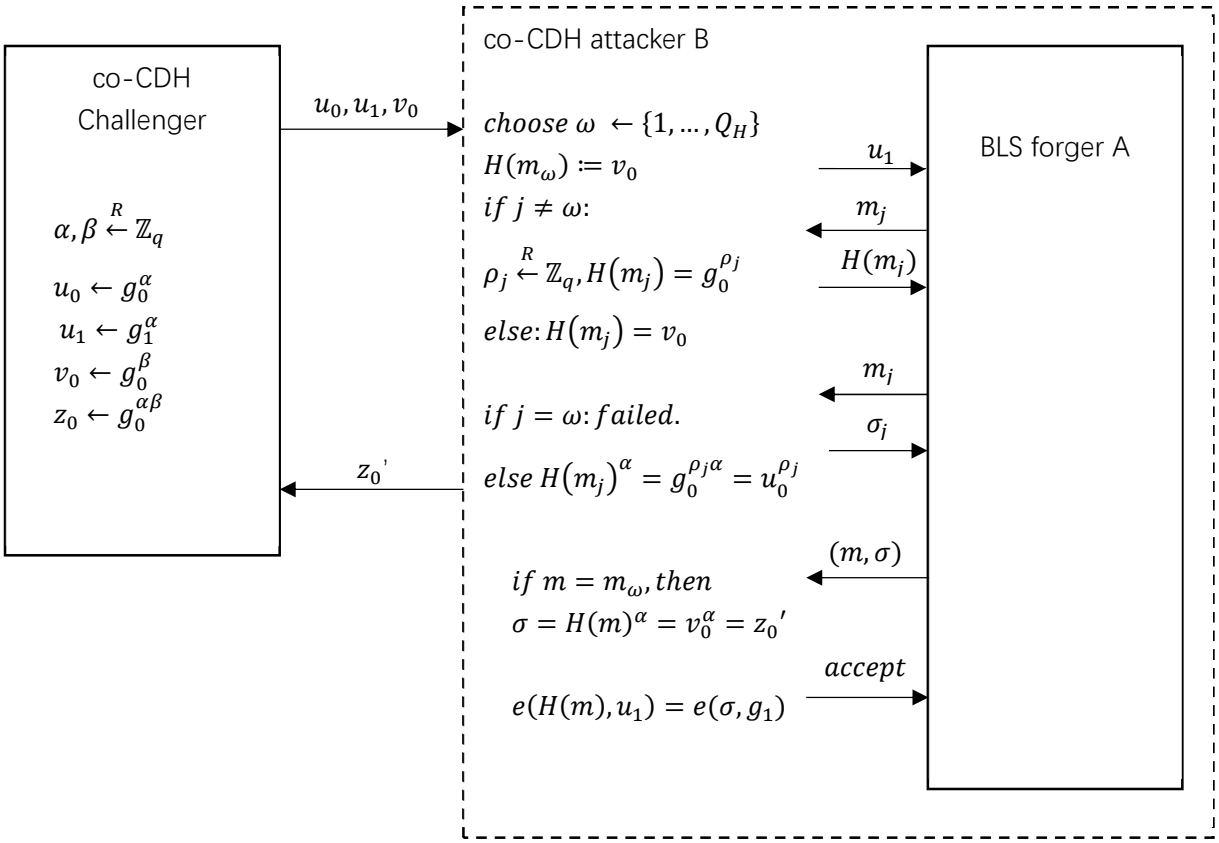
a). $V(pk, m, \sigma)$: $e(H(m), u_1) = e(H(m), g_1^{\alpha}) = e(H(m), g_1)^{\alpha} = e(H(m)^{\alpha}, g_1) = e(\sigma, g_1)$

b). **Prove:**




$$SIG^{RO}Adv[A, S_{BLS}] \leq 2.72 \cdot Q_H \cdot coCDHadv[B, e]$$

So BLS signature scheme is secure assuming co-CDH assumption holds in paring e and H is modeled as a random oracle.