Name: Yitian Shan

Student Number: 202118022

UOW Number: 7377587

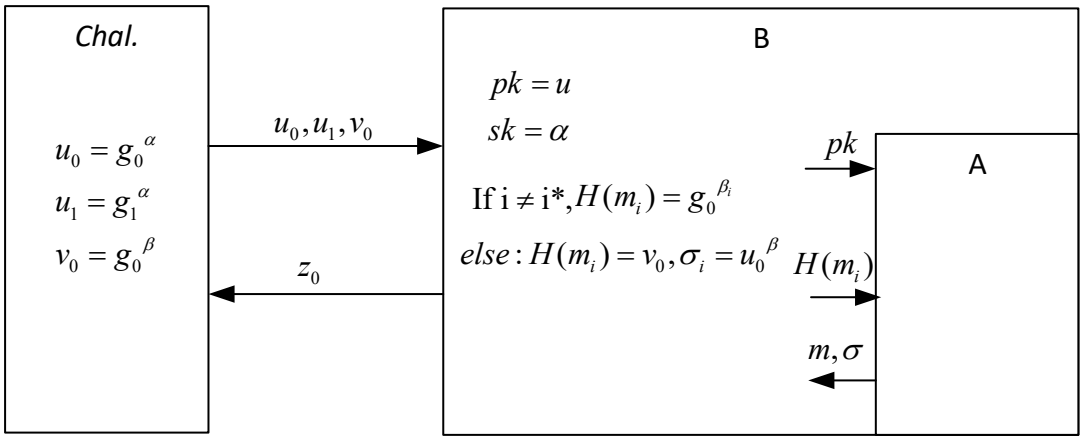
Date: 2021/11/20

1.

$\because e(g_0^{\alpha}, g_1^{\beta}) = e(g_0, g_1)^{\alpha\beta}$

$\therefore e(H(m), u) = e(H(m), g_1^{\alpha}) = e(H(m)^{\alpha}, g_1) = e(\sigma, g_1)$

2 .



$\because P_r\left[m = m_{i^*}\right] = \frac{1}{Q_{ro}}$

$so, ADV_{co-CDH} \geqslant \frac{1}{Q_{ro}} \cdot ADV_{SIG} \quad \rightarrow ADV_{SIG} \leqslant Q_{ro} \cdot ADV_{co-CDH}$

So BLS signature scheme is secure assuming coCDH assumption holds in pairing and is model as a random oracle.