

Assignment Server

(AK_0, AK_1, AK_2)

CH_i

$$CH_i = h(AK_0, h(AK_1, h(AK_2, CK_i)))$$

Client C_i (generates CH_i)