

Assignment Server

(AK_0, AK_1, AK_1)

(RH_0, \dots, RH_n)

$$RH_0 = h(AK_0, h(AK_1, h(AK_2, RC_0)))$$

⋮

⋮

$$RH_n = h(AK_0, h(AK_1, h(AK_2, RC_n)))$$

Relay R_0 (generates RH_i for n clients)