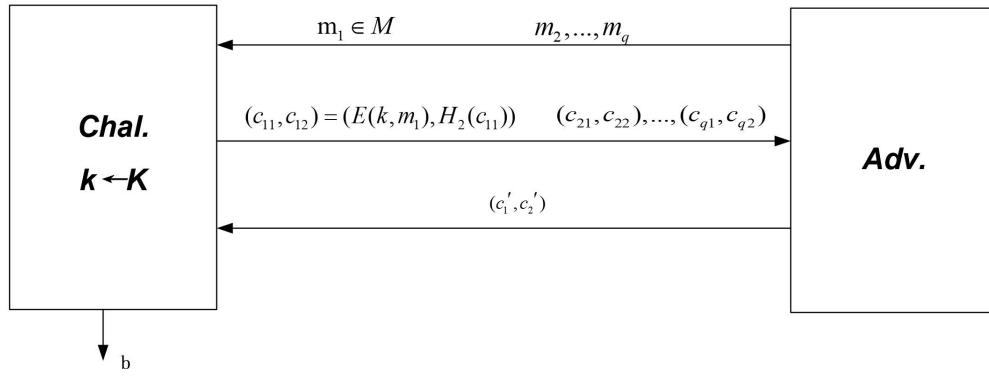


E<sub>1</sub>:

Define A's advantages:  $Adv_{ss}[A, E_1] = |\Pr[W_0] - \Pr[W_1]|$ . Obviously,  $Adv_{ss}[A, E_1]$  is not *negligible*.

E<sub>2</sub>:

Game as:



We know that attacker can estimate the value of  $c'_2$  from  $c'_1$ . The  $Adv[A, E_2]$  is not *negligible*.