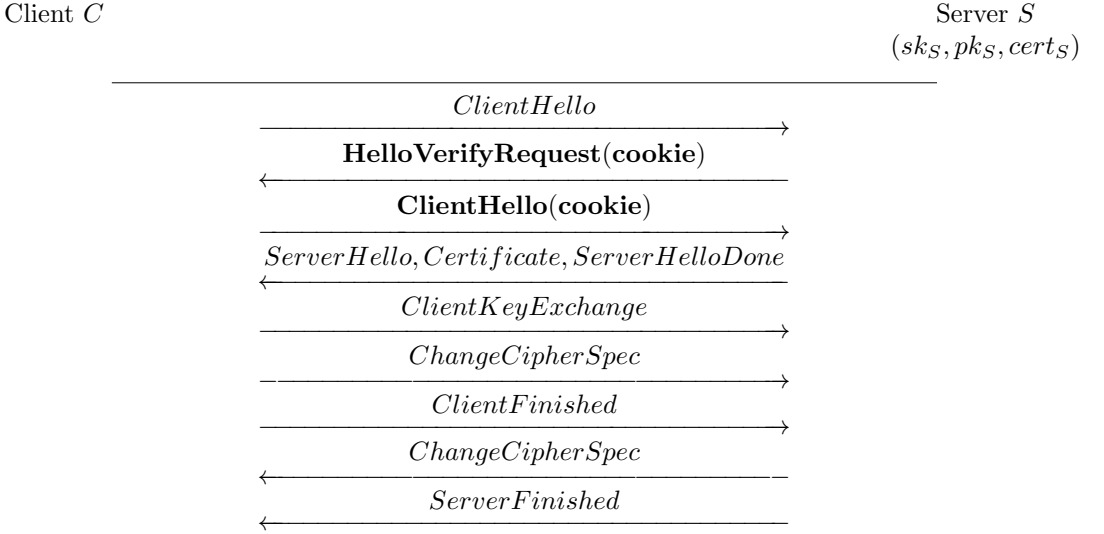
Client C
Server S
$(sk_S, pk_S, cert_S)$
$ClientHello$
HelloVerifyRequest(cookie)
ClientHello(cookie)
$ServerHello, Certificate, ServerHelloDone$
$ClientKeyExchange$
$ChangeCipherSpec$
$ClientFinished$
$ChangeCipherSpec$
$ServerFinished$