

client

server

client\_hello(crypt information,  $R_C$ )

server\_hello(crypt information,  $R_S$ )

