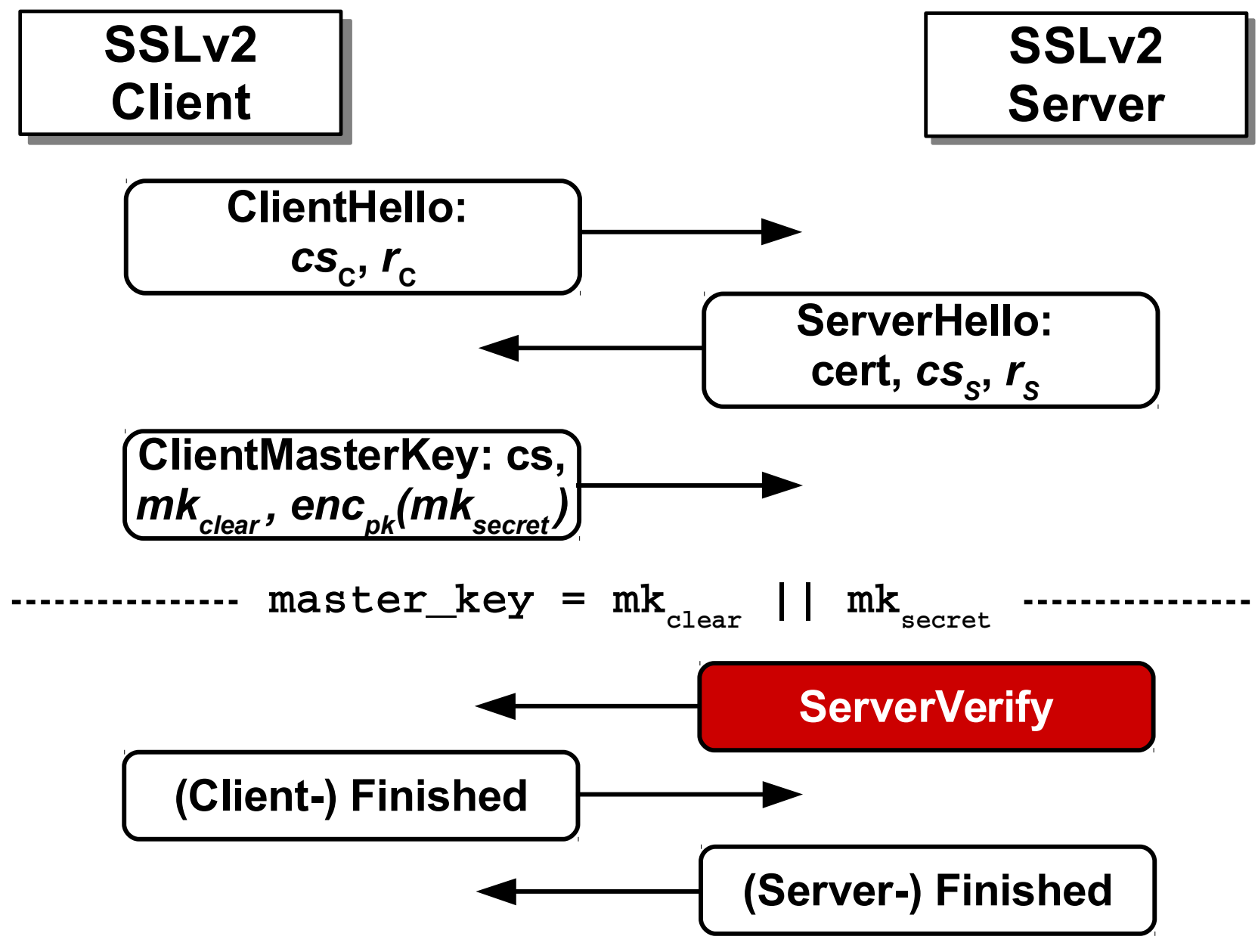
SSLv2 Client
SSLv2 Server
ClientHello: cs_c, r_c
ServerHello: cert, cs_s, r_s
ClientMasterKey: cs, mk_{clear}, $enc_{pk}(mk_{secret})$
master_key = mk_{clear} || mk_{secret}
ServerVerify
(Client-) Finished
(Server-) Finished