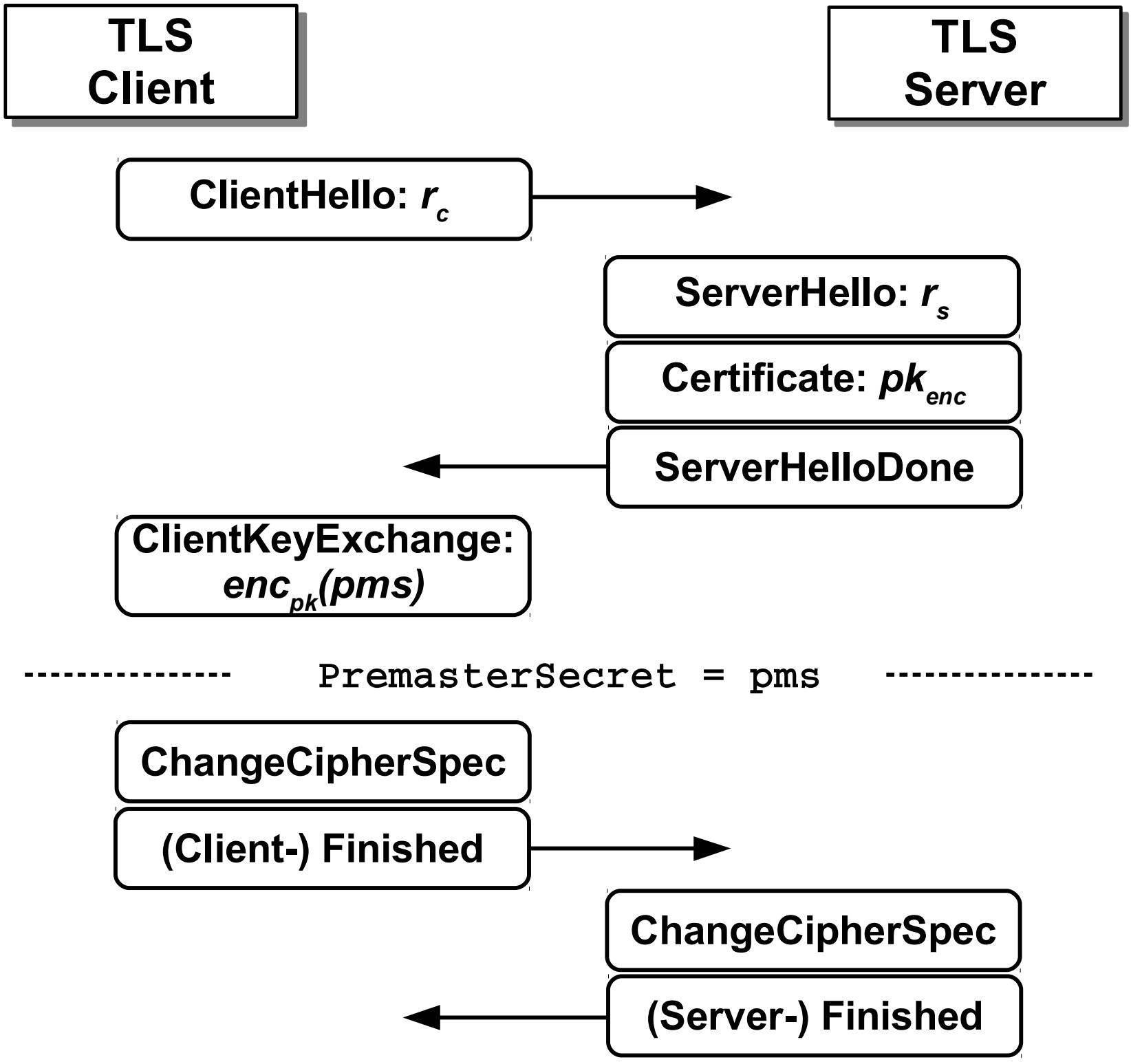
TLS Client
TLS Server
ClientHello: r_c
ServerHello: r_s
Certificate: pk_{enc}
ServerHelloDone
ClientKeyExchange: $enc_{pk}(pms)$
PremasterSecret = pms
ChangeCipherSpec
(Client-) Finished
ChangeCipherSpec
(Server-) Finished