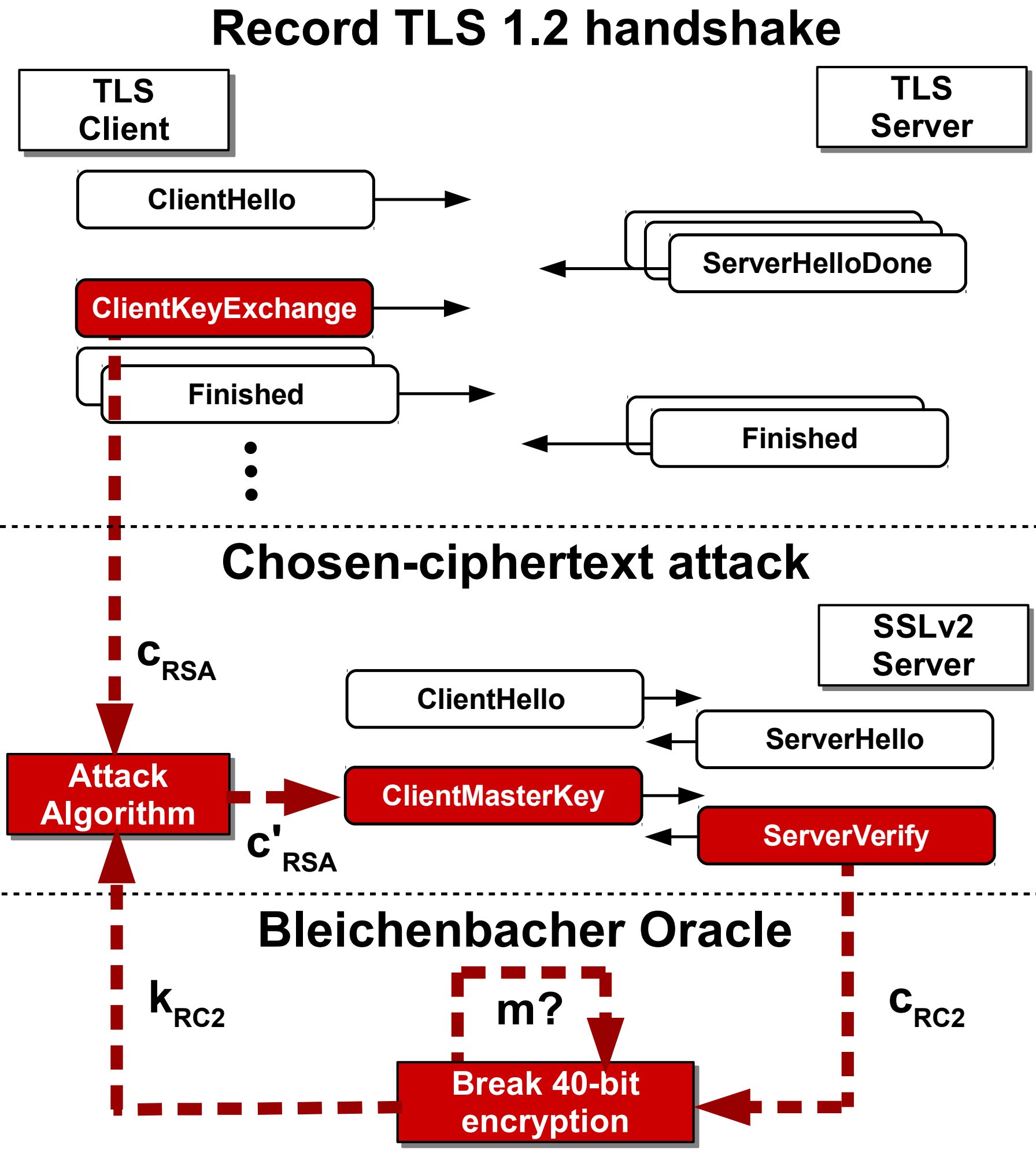
Record TLS 1.2 handshake
TLS Client
TLS Server
ClientHello
ServerHelloDone
ClientKeyExchange
Finished
Finished
Chosen-ciphertext attack
SSLv2 Server
c_{RSA}
ClientHello
ServerHello
Attack Algorithm
ClientMasterKey
ServerVerify
c'_{RSA}
Bleichenbacher Oracle
k_{RC2}
m?
c_{RC2}
Break 40-bit encryption