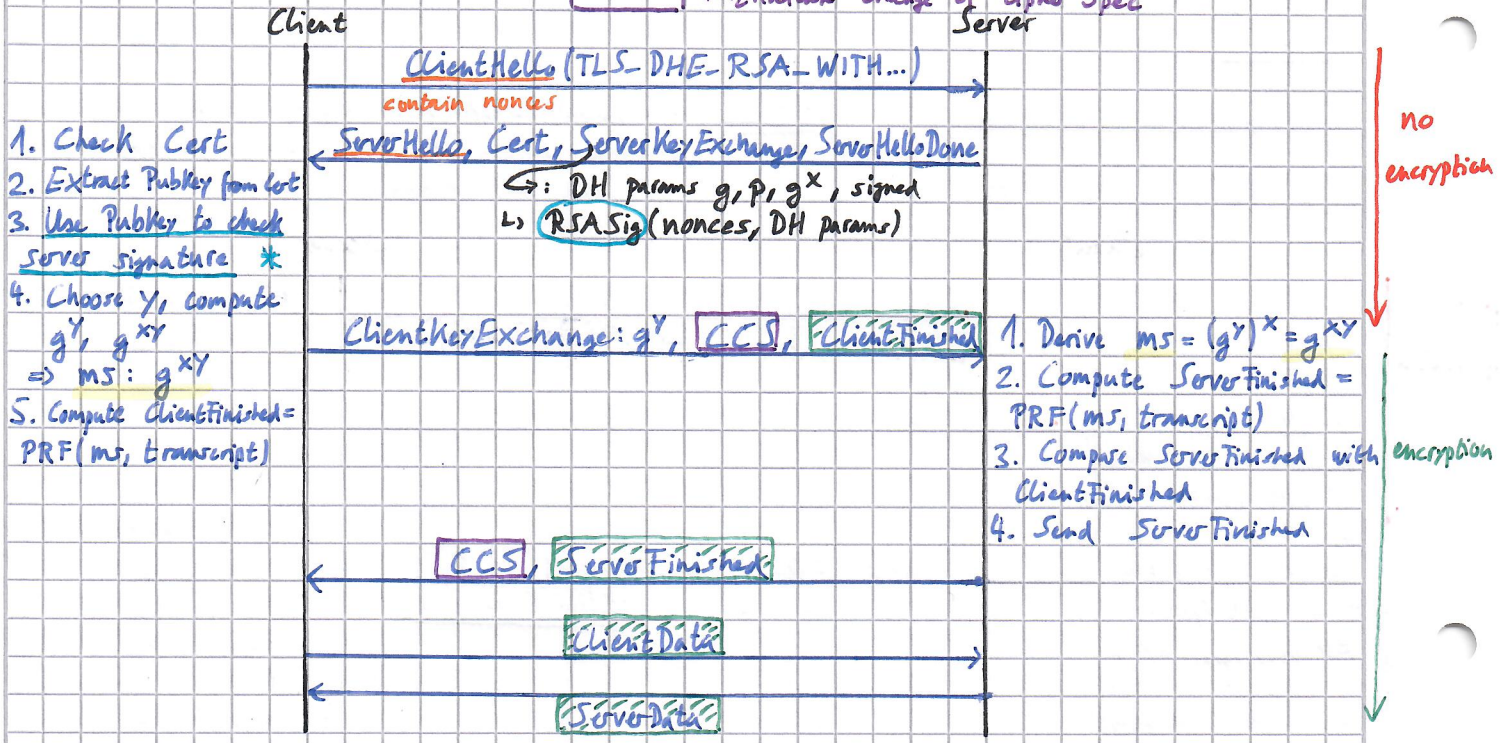
TLS_DHE_RSA_WITH...

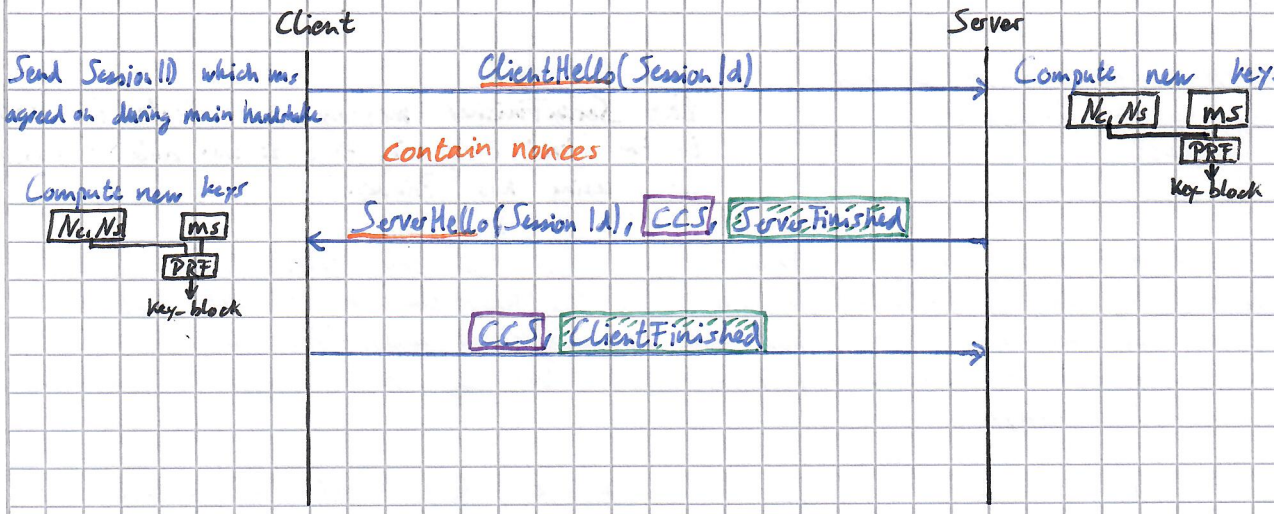
▨ : encrypted with ms using record-layer crypto

▭ : indicate change of cipher spec



(*) Server is authenticated by signing nonces, DH params with its privkey.

Handshake protocol – session resumption → 1-RTT



⇒ We compromise forward security since we reuse the mastersecret! If ms is compromised, we can decrypt previous sessions