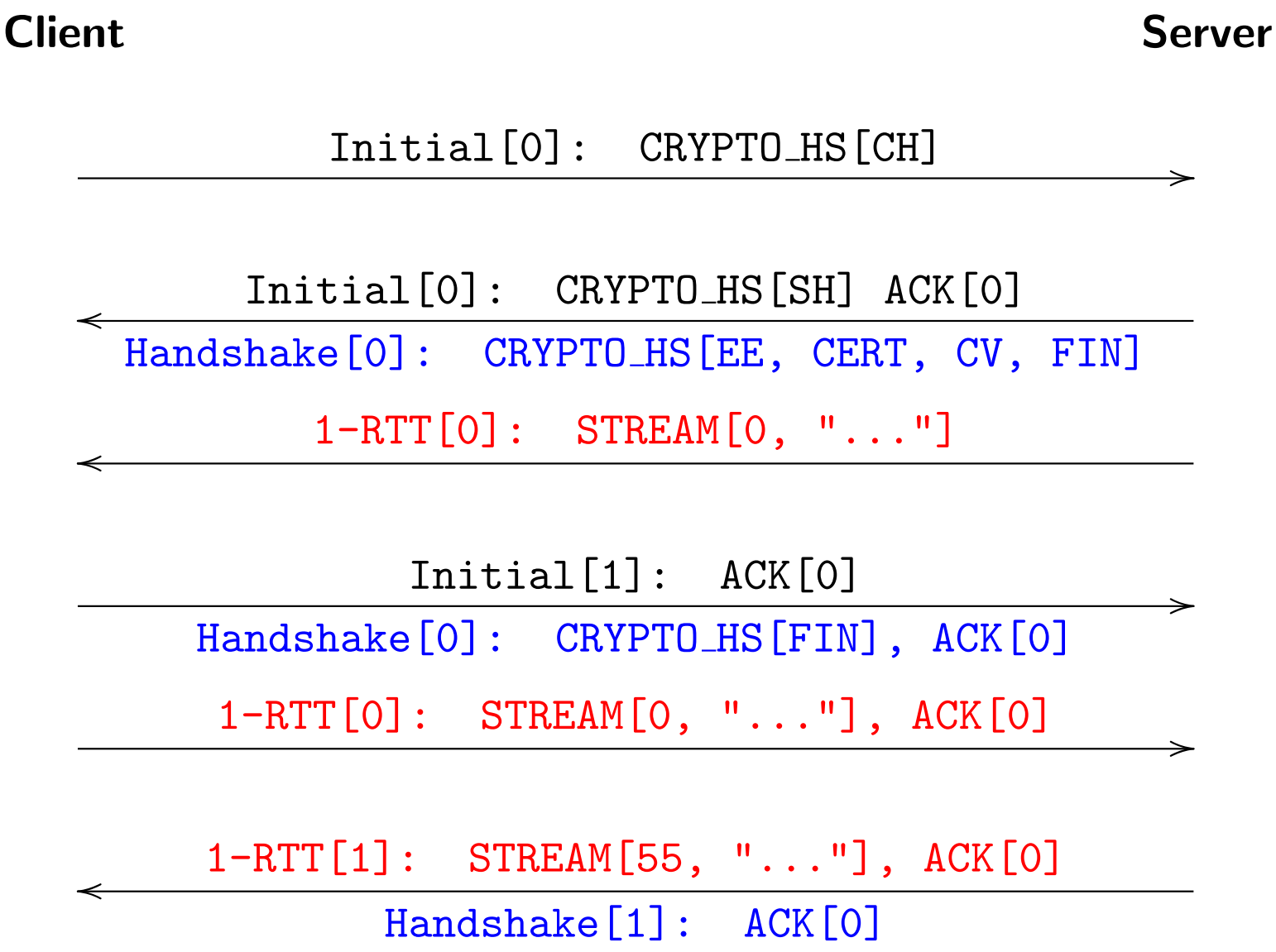
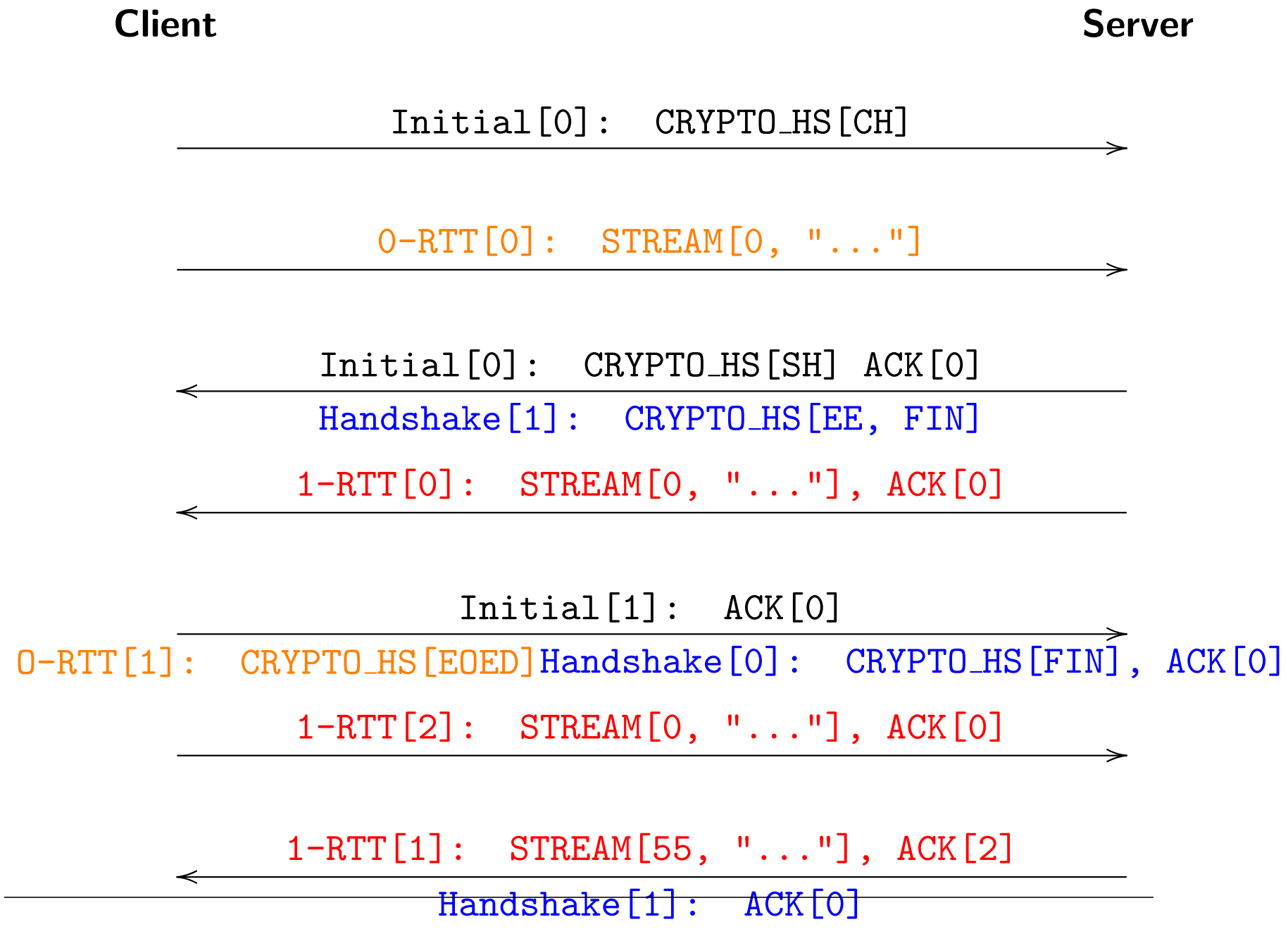
QUIC Handshake Flow

Eric Rescorla

Mozilla

ekr@rtfm.com


Client
Server
Initial[0]: CRYPTO_HS[CH]
Initial[0]: CRYPTO_HS[SH] ACK[0]
Handshake[0]: CRYPTO_HS[EE, CERT, CV, FIN]
1-RTT[0]: STREAM[0, "..."]
Initial[1]: ACK[0]
Handshake[0]: CRYPTO_HS[FIN], ACK[0]
1-RTT[0]: STREAM[0, "..."], ACK[0]
1-RTT[1]: STREAM[55, "..."], ACK[0]
Handshake[1]: ACK[0]


Client
Server
Initial[0]: CRYPTO_HS[CH]
0-RTT[0]: STREAM[0, "..."]
Initial[0]: CRYPTO_HS[SH] ACK[0]
Handshake[1]: CRYPTO_HS[EE, FIN]
1-RTT[0]: STREAM[0, "..."], ACK[0]
Initial[1]: ACK[0]
0-RTT[1]: CRYPTO_HS[EOED]
Handshake[0]: CRYPTO_HS[FIN], ACK[0]
1-RTT[2]: STREAM[0, "..."], ACK[0]
1-RTT[1]: STREAM[55, "..."], ACK[2]
Handshake[1]: ACK[0]