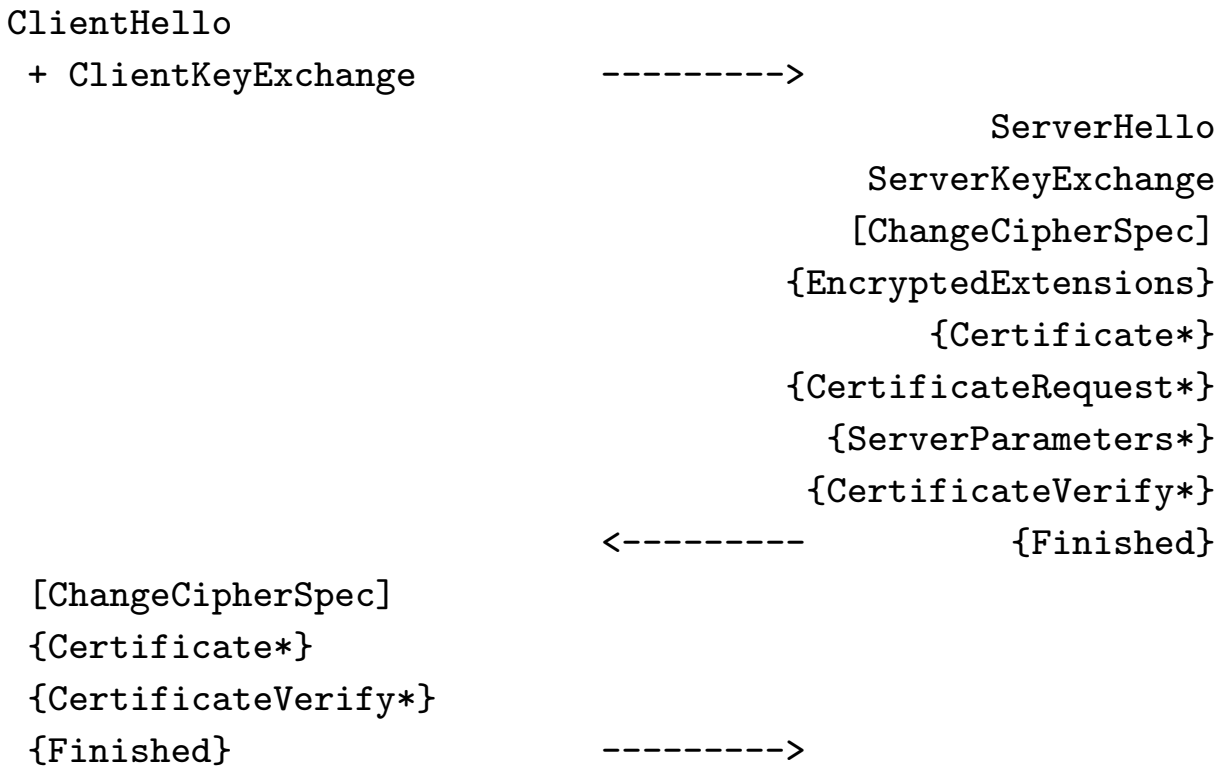
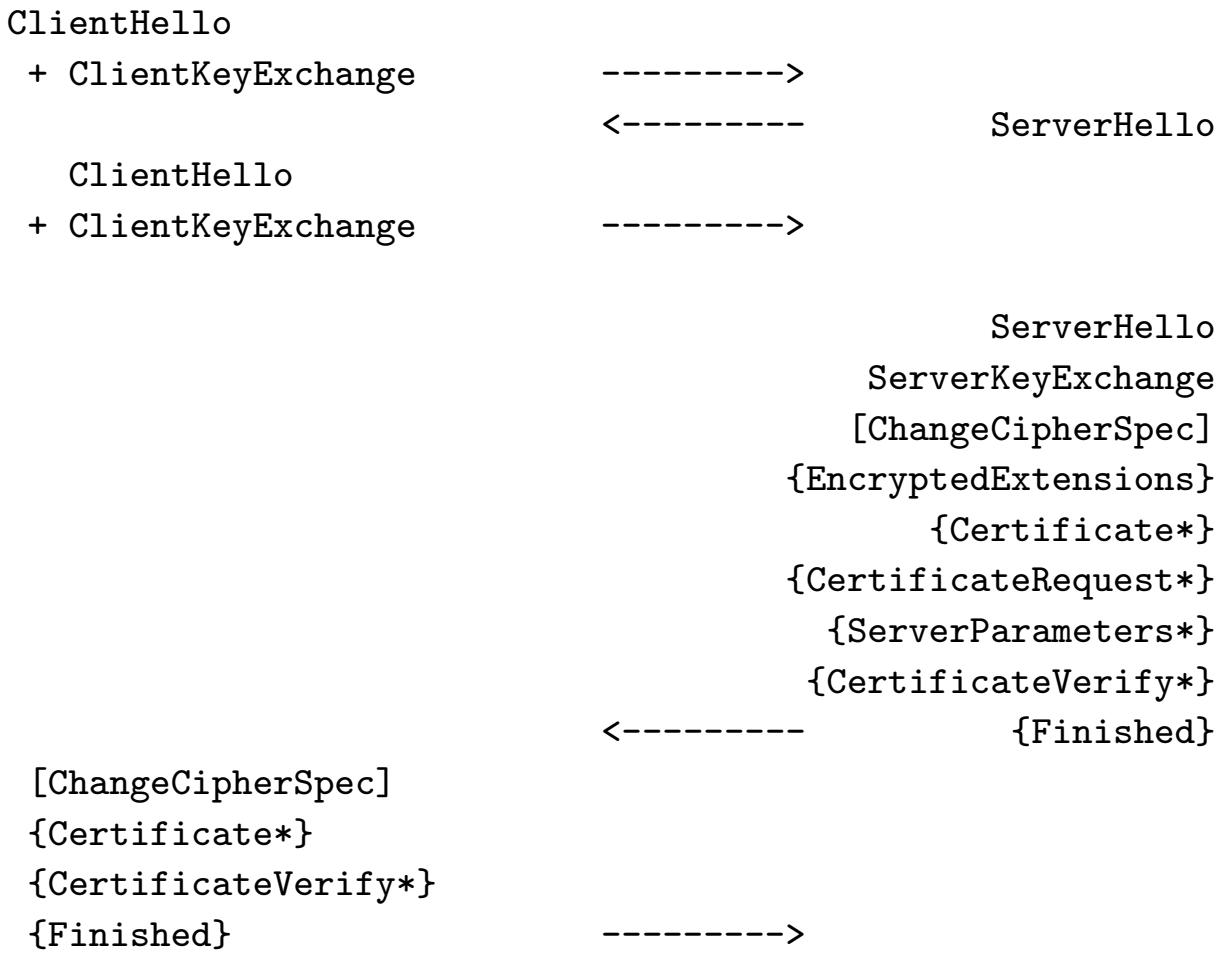
From yesterday

0. Encrypted Server Handshake	Yes
1. Keep SNI	Yes
2. Require SNI for TLS 1.3	Yes
3. Allow encrypted SNI	Yes
4. Require support for encrypted SNI	(No)
5. Provide an in-band SNI encryption at potential cost in RTs	(?)
6. Propose a DNS mechanism for distributing keys	Defer for #4
7. Support for all three topologies	Yes
8. No penalty for those who want to do SNI in the clear	Yes

Basic 1-RTT Handshake (shared group)



No shared group: correct/re-start



No shared group: encryption on second fight