QUIC and TLS

Adam Langley

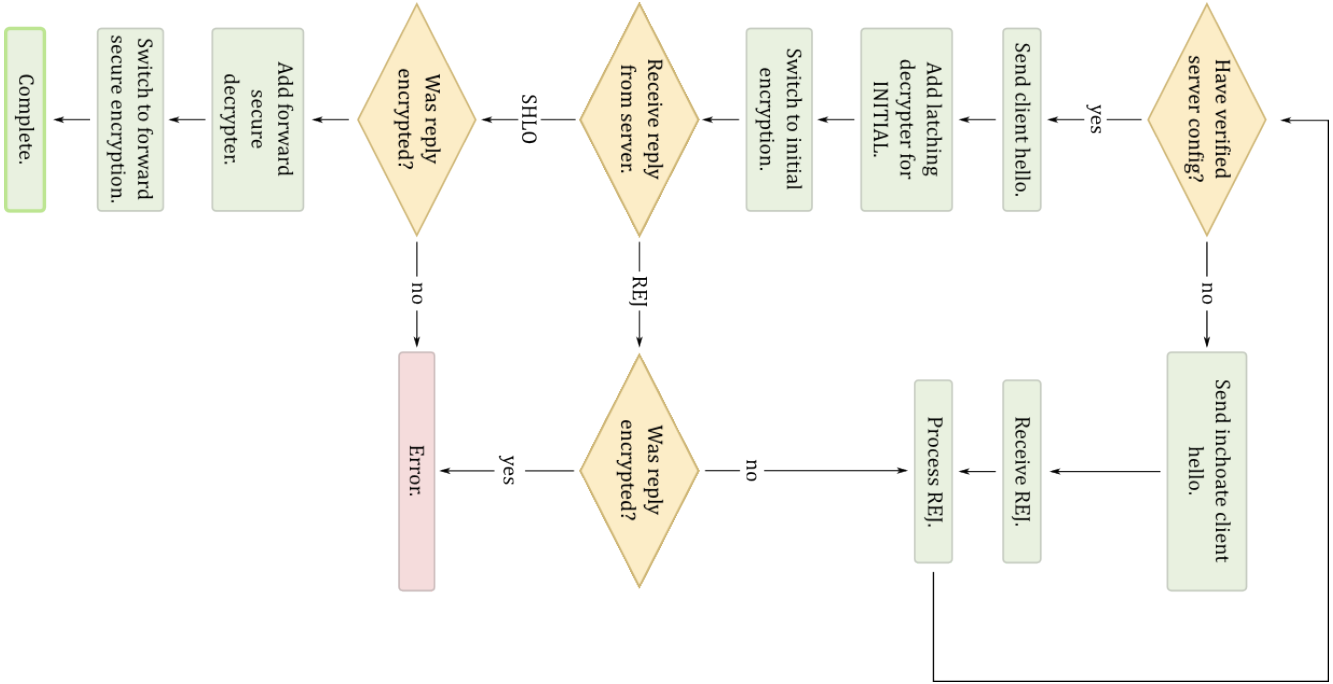
History

- The initial ideas for SPDY involved it being a UDP protocol.
- That was dropped to limit the scope.
- SPDY worked out OK and QUIC continues it by replacing TCP and TLS under SPDY/HTTP 2.

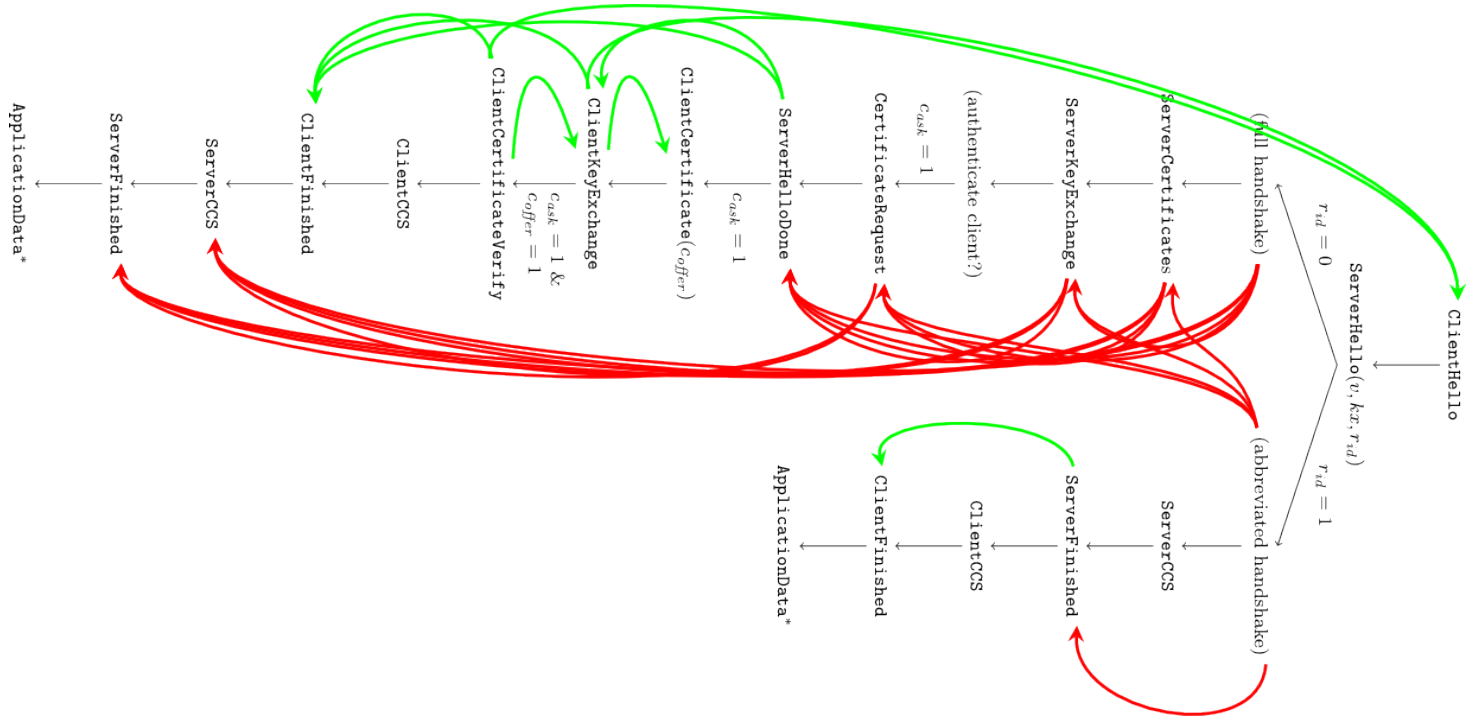
History (2)

- QUIC is primarily a Transport experiment, but security isn’t optional any more.
- In 2013 I designed and implemented QUIC Crypto, a 0-RTT capable security layer for QUIC.

QUIC State Machine.



(TLS State Machine)



QUIC Crypto in a slide.

- Server signs a config block, containing Diffie-Hellman parameters, supported ciphersuites etc.
- If the client knows nothing, it prompts for the config block.
- Otherwise, it calculates shared keys and starts talking.

QUIC Crypto upshots.

- 0-RTT
- No resumption
- Fast (curve25519, no online signatures).
- Forward secure to TLS’s level or better.

QUIC Crypto references

- Spec
- “How Se-cure and Quick is QUIC? Prov-able Se-cu-rity and Per-for-mance Analy-ses”, Ly-chev et al, to ap-pear in IEEE Se-cu-rity & Pri-vacy 2015
- “Multi-Stage Key Ex-change and the Case of Google’s QUIC Pro-to-col”, Fis-chlin and Günther, ACM CCS 2014.

QUIC Crypto and TLS 1.3

- TLS 1.3 looks quite a lot like QUIC Crypto at the moment, which is no accident.
- TLS 1.3 has rejected offline signing.
- QUIC’s anti-replay didn’t work and nobody noticed until a couple of weeks ago.

QUIC and TLS 1.3

- QUIC is a UDP based protocol so worries about spoofed source addresses, like DTLS.
- But QUIC provides ordering and reliability to the crypto handshake, so that’s more like TLS.
- The crypto part of QUIC can be separated from the transport parts.