Hybrid key exchange for TLS 1.3

draft-ietf-tls-hybrid-design-latest

https://datatracker.ietf.org/doc/draft-connolly-tls-mlkem-key-agreement/
https://github.com/dstebila/draft-ietf-tls-hybrid-design

hybrid-design Named Groups

Two instances:

  - X25519Kyber768Draft00 (deployed in Chrome, Cloudflare)
  - SecP256r1Kyber768Draft00

- When FIPS 203 (ML-KEM) lands, those IANA entry values will need updating
- hybrid-design by itself looks done and will not be including IANA entries itself

Questions?

Hybrid key exchange for TLS 1.3

draft-ietf-tls-hybrid-design-latest

https://datatracker.ietf.org/doc/draft-connolly-tls-mlkem-key-agreement/
https://github.com/dstebila/draft-ietf-tls-hybrid-design