Post-Quantum Hybrid ECDHE-MLKEM Key Agreement for TLSv1.3

Kris Kwiatkowski
Cryptography Architect
PQShield
kris@amongbytes.com

draft-kwiatkowski-tls-ecdhe-mlkem-02

Registers code-points for PQ/T hybrid key exchange in TLS

- ECDH/SecP256r1 + MLKEM-768 (`0x11EB`)
- X25519 + MLKEM-768 (`0x11EC`)

Goals

- Enables migration to post-quantum in the TLS following `draft-ietf-tls-hybrid-design`
- FIPS certifiable according to SP800-56Cr2

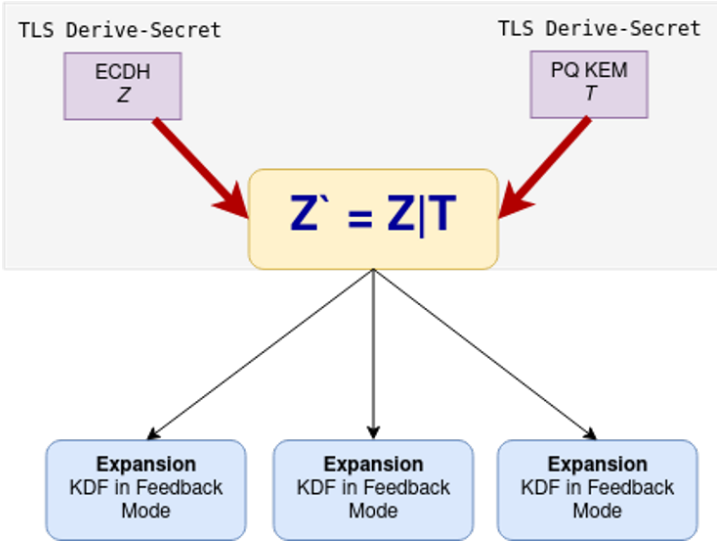
SP800-56C rev2

In addition to the currently **approved** techniques for the generation of the shared secret Z as specified in SP 800-56A and SP 800-56B, this Recommendation permits the use of a "hybrid" shared secret of the form $Z' = Z \| T$, a concatenation consisting of a "standard" shared secret Z that was generated during the execution of a key-establishment scheme (as currently specified in [SP 800-56A] or [SP 800-56B]) followed by an auxiliary shared secret T that has been generated using some other method. The content, format, length, and method used to generate T must be known

Construction

- **ECDH/SecP256r1 + MLKEM-768**
  - Construction: **ECDH/p256 || MLKEM-768**
  - Code-point name: `Secp256r1MLKEM768`
  - Value: `0x11EB`
  - Obsoletes: `SecP256r1Kyber768Draft00`

- **X25519 + MLKEM-768**
  - Construction: **MLKEM-768 || X25519**
  - Code-point name: `X25519MLKEM768`
  - Value: `0x11EC`
  - Obsoletes: `X25519Kyber768Draft00`



PQ SHIELD

Status (-02 version)

- X25519 + MLKEM-768 (`0x11EC`) already in use
  - Used by AWS, Chrome, Firefox, Safari
  - Deployed on Cloudflare & Google servers

Next (-03 version)

- Codepoint for ECDH/p384 + MLKEM-1024
- Suggestions related to public key validation were added

Questions

- Change NamedGroup to align with the order of shared secrets?
  - X25519MLKEM768 -> MLKEM768X25519 ?
- Adoption or leave it as a draft?
- RECOMMENDED=Y for curves that are currently recommended?