ML-KEM Post-Quantum Key Agreement for TLS 1.3

draft-ietf-tls-mlkem-05

https://datatracker.ietf.org/doc/draft-ietf-tls-mlkem/
https://github.com/tlswg/draft-ietf-tls-mlkem

A pure-PQ ciphersuite for TLS 1.3

- No purely post-quantum ciphersuites
- Fills in the other side of draft-ietf-tls-hybrid-design
- Needed because there are no documents that describe KEM-only key agreement in TLS
- If PQ-only works for your applications, clean key agreement, no hybrid duplicate shares or mixing and matching logic
- ML-KEM-1024 supports users who need to comply with the CNSA 2.0 draft
- I want to be able to do it 🐴

New NamedGroups: MLKEM512, MLKEM768, MLKEM1024

```
enum {

      ...,

       /* ML-KEM Key Agreement Methods */
       mlkem512(0x0200),
       mlkem768(0x0201),
       mlkem1024(0x0202)

      ...,

} NamedGroup;
```

Codepoints allocated:

512	MLKEM512	Y	N	[draft-connolly-tls-mlkem-key-agreement-03]	FIPS 203 version of ML-KEM-512
513	MLKEM768	Y	N	[draft-connolly-tls-mlkem-key-agreement-03]	FIPS 203 version of ML-KEM-768
514	MLKEM1024	Y	N	[draft-connolly-tls-mlkem-key-agreement-03]	FIPS 203 version of ML-KEM-1024

Client sends encaps key, server replies with ciphertext

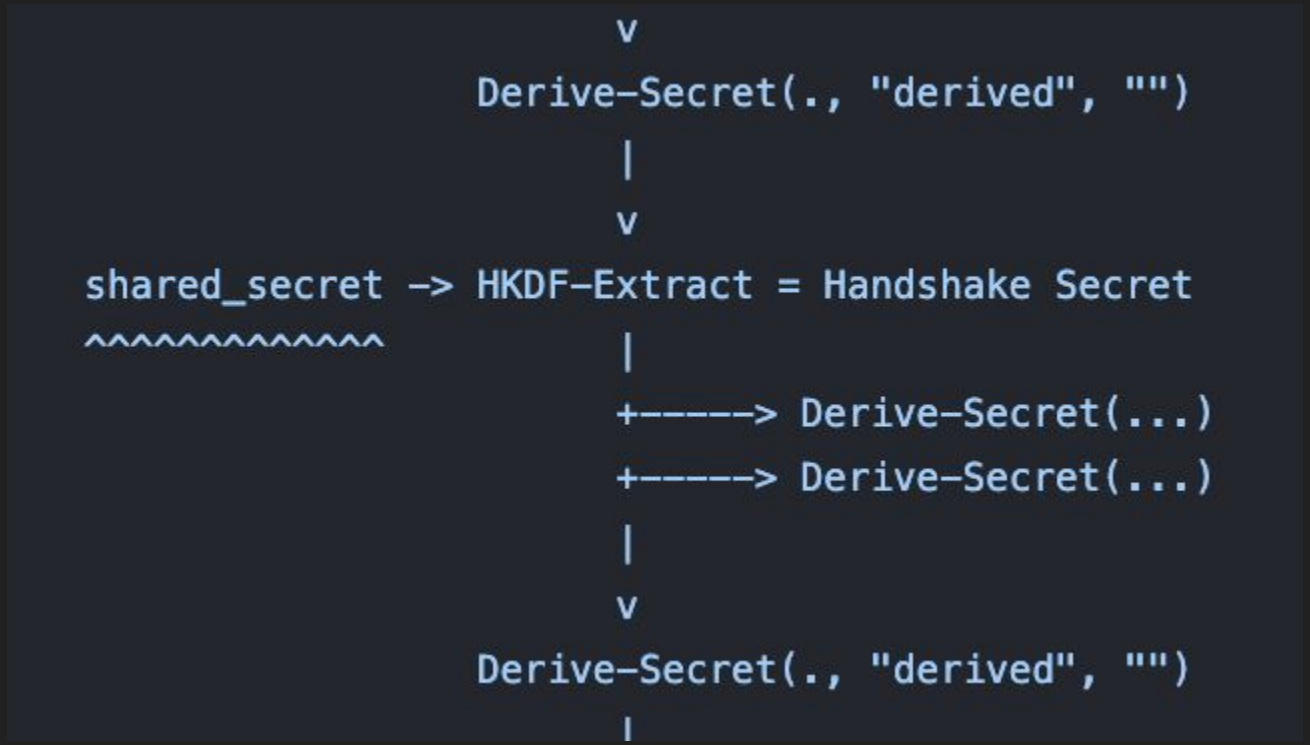
```
struct {
    NamedGroup group;
    opaque key_exchange<1..2^16-1>;
} KeyShareEntry;
```

These are transmitted in the `extension_data` fields of `KeyShareClientHello` and `KeyShareServerHello` extensions:

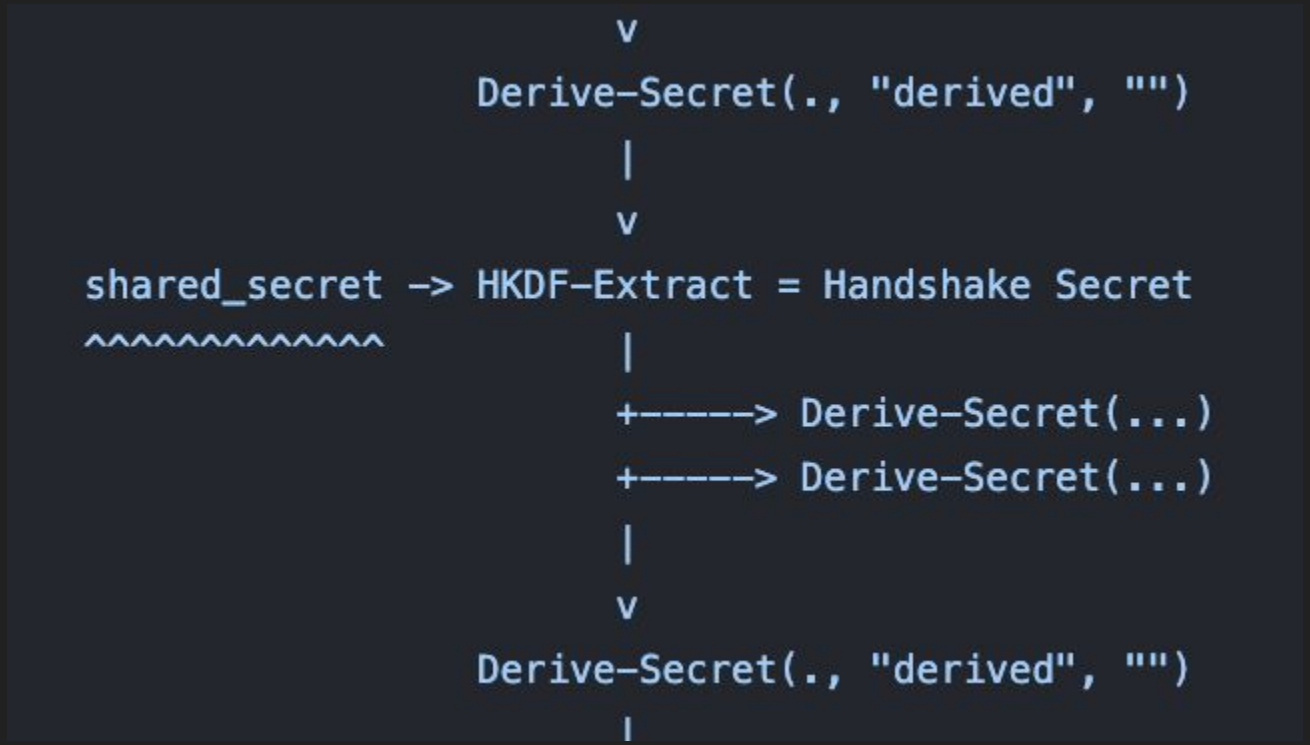
```
~~~
    struct {
        KeyShareEntry client_shares<0..2^16-1>;
    } KeyShareClientHello;

    struct {
        KeyShareEntry server_share;
    } KeyShareServerHello;
~~~
```

KEM shared secret is input to Handshake Secret derivation



KEM shared secret is input to Handshake Secret derivation



Updates as of `draft-ietf-tls-mlkem-05`

- Integrated review feedback
- Aligned with `-ecdhe-mlkem` on language about ML-KEM failures
- Fixed refs

Open Issues

- https://github.com/tlswg/draft-ietf-tls-mlkem/pull/6
  - Changes Recommended = N to Recommended = D
  - Does not align with `-ecdhe-mlkem`
  - Would require IETF Standards Action with Expert Review or IESG Approval
  - Would group ML-KEM with NULL ciphers, RC4, DES, EXPORT ciphers, MD5, etc

Timeline

- Resolve last issue
- WGLC?

ML-KEM Post-Quantum Key Agreement for TLS 1.3

draft-ietf-tls-mlkem-05

https://datatracker.ietf.org/doc/draft-ietf-tls-mlkem/
https://github.com/tlswg/draft-ietf-tls-mlkem