Hybrid key exchange in TLS 1.3
draft-ietf-tls-hybrid-design-06

Douglas Stebila, Scott Fluhrer, Shay Gueron
Quick Overview

Goal: Add post-quantum privacy to TLS in hybrid mode

• We use both convention and postquantum cryptography

Method: Define new groups that consist of both an ECC group as well as a postquantum KEM

• Each allowed combination is given a unique identifier
• We use concatenation to combine key shares and the shared secrets

This draft provisionally defines four combinations:

x25519+Kyber768    secp384r1+Kyber768
x25519+Kyber512    secp256r1+Kyber512
Open Questions

• Are these the correct combinations?
  One suggestion (from the Kyber team) was to define the single initial group X25519Kyber768Draft00 at code point 0xfe31
  • Draft00 to indicate that this is Kyber according to the Round 3 specification, rather than the final FIPS specification

• Should we align this with draft-ounsworth-cfrg-kem-combiners?
  Current draft gives HKDF_extract the input ‘k1 || k2’; the Ounsworth draft makes it ‘H( H(k1 || c1) || H(k2 || c2) )’

• Anything else before we RFC?