Hybrid key exchange in TLS 1.3

draft-ietf-tls-hybrid-design-03

Douglas Stebila, Scott Fluhrer, Shay Gueron

UNIVERSITY OF WATERLOO

NSERC CRSNG

Motivation

- **Permit simultaneous use of traditional and post-quantum key exchange**

- Enable early adopters to get post-quantum security without discarding security of existing algorithms
- Why do this?
  - Uncertainty re: newer cryptographic assumptions
  - Temporary need to keep traditional algorithms for e.g. FIPS certification

Goals

Define data structures for negotiation, communication, and shared secret calculation for hybrid* key exchange

Non-goals

- Hybrid/composite certificates or digital signatures
- Selecting which post-quantum algorithms to use in TLS

* Some people use the word “composite” instead of “hybrid”.

Mechanism

Idea: Each desired combination of traditional + post-quantum algorithm will be a new (opaque) key exchange “group”

- **Negotiation**: new named groups for each desired combination will need to be standardized
- **Key shares**: concatenate key shares for each constituent algorithm
- **Shared secret calculation**: concatenate shared secrets for each constituent algorithm and use as input to key schedule

Other design options

Negotiation

- 2 vs ≥2 algorithms
- Extension for representing algorithm options and constraints

Key shares

- Separately list key shares for each algorithm
- Use extensions for extra key shares

Shared secret

- Apply KDF before inserting into key schedule
- XOR shares
- Insert into different parts of TLS key schedule

See Appendix A of draft for related work and Appendix B for detailed discussion of other design options.

Questions

- What else is required before this draft can advance?
  - Currently listed as a working group milestone for November 2021

- Should this document include concrete hybrid group combinations for e.g. existing elliptic curves + NIST PQCrypto Round 3 finalists?