PQ MLS Combiners

Joël Alwen, Britta Hale, Marta Mularczyk, Xisen Tian

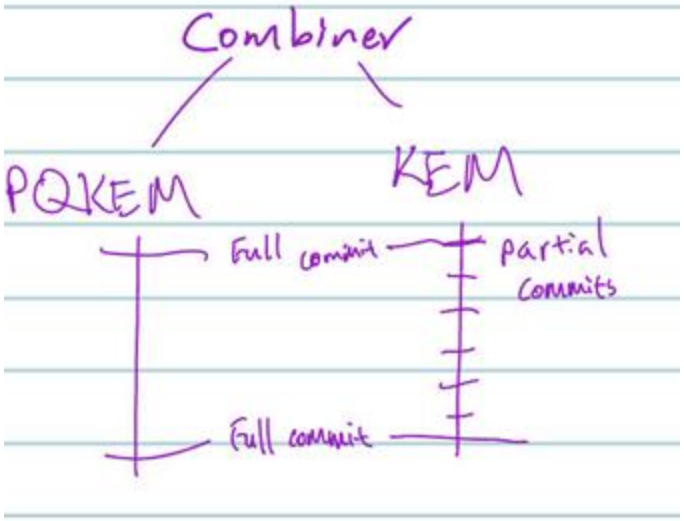
Motivation

- Alternative to a hybrid (e.g. PQ/T) ciphersuite approach

- ***Flexibility:*** PQ updates and commits are tunable

Exporter Combiner

Uses T and PQ MLS sessions which are combined via exported PSKs.



- PARTIAL Commit
  - Traditional-only commit in the traditional MLS group
- FULL Commit
  - PQ commit in PQ group, exporter key generated and used as PSK along with a traditional commit in the traditional group
- Flexibility on PQ ratchet window

Beyond PQ Confidentiality – Modes

- PQ Confidentiality-Only mode
- PQ Confidentiality + Authenticity mode
  - PQ signatures are used to authenticate PQ updates in PQ group. The exporter key inherits this attestation and its inject into the traditional key schedule allow for PQ/T AEAD.
  - This does not include PQ non-repudiation

Examples (and many more in between)

- single FULL Commit in PQ/T Confidentiality Only mode followed by PARTIAL Commits from that point onwards
  - PQ/T confidentiality, T update authenticity, T data authenticity, T non-repudiation
    T PCS, and PQ/T forward secrecy

- frequent FULL Commits in PQ/T Confidentiality Only mode
  - PQ/T confidentiality, T update authenticity, T data authenticity, T non-repudiation
    PQ/T PCS, and PQ/T forward secrecy

- frequent FULL Commits in PQ/T Confidentiality + Authenticity mode
  - PQ/T confidentiality, PQ/T update authenticity, PQ/T data authenticity, T non-repudiation
    PQ/T PCS, and PQ/T forward secrecy.