

Post-Quantum MLS

Joël Alwen, **Britta Hale**, Marta Mularczyk, Xisen Tian

Approach 1 : Hybrid Ciphersuite (short term)

Approach : Use PQ/Classic Hybrid KEM.

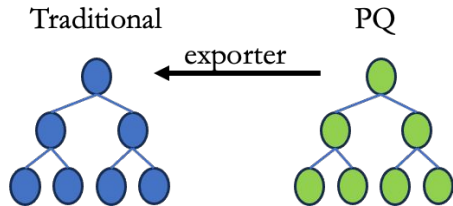
- E.g. draft-mahy-mls-xwing-00
- Pro: Relatively, low engineering effort.
 - No changes to MLS or HPKE.
 - Large overlap with needs of other Hybrid KEM applications. (except for de-randomized KeyGen)
- Con: Somewhat rigid:
 - Fixes both PQ and classic KEM in one package. (E.g. Kyber-768 + X25519).
 - **Must pay PQ efficiency cost for each KEM operation even if not needed for security.**
 - **Authenticity out of scope**

Approach 2 : Session Combiners (long term)

Approach : 2 parallel MLS sessions. 1 session is pure PQ and other is pure Classic. Each session with the same set of clients OR PQ session as supergroup.

“Glue” sessions together using Exporters/PSKs.

- Pro :
 - Flexible : Can combine any two KEMs.
 - Efficiency : Can do classic-only commits & updates.
 - **Modular: No code changes needed to MLS nor HPKE.**
- Con :
 - Operationally more complicated : need to keep 2 MLS sessions' membership synchronized.
 - Requires additional mechanisms to ensure commit messages from both sessions are applied

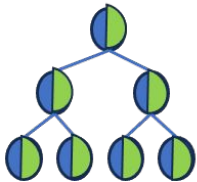


Approach 3 : MLS with 2 KEMs (long-term)

Approach : 2 KEM keys at each ratchet tree node from 2 different ciphersuites (i.e. 1 classic / 1 PQ). Each Commit operation uses either 1 type of KEM or both KEMs (in a combiner). Signature keys can be handled similarly if desired.

- Pro :
 - Flexible : Can combine any two KEMs.
 - Efficiency : Can do classic-only commits & updates.
 - **Operationally simple. Just 1 MLS session.**
- Con :
 - Requires either
 - registering a new cipher suite (where encryption takes an additional input indicating which KEMs to use; this may change the API of MLS / HPKE)
 - or changing MLS wire format (to indicate which KEMs to use)

Combined

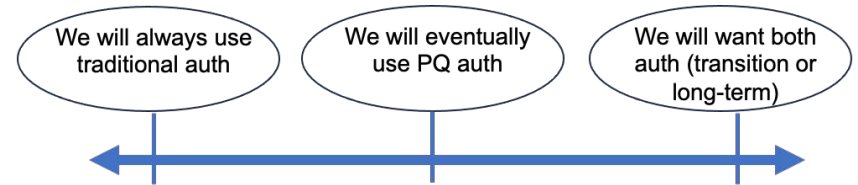


PQ Authenticity?

Up to now focus is only on PQ *privacy*.

What about PQ authenticity?

Q: What are the PQ authenticity concerns for the WG?



Q: How urgent is PQ authenticity (if planned)?

- Does not seem urgent if adversary is “record today, decrypt tomorrow”... but is relevant to other threats like “forging signatures on old messages”.
- PQ Signature standards lag behind PQ KEM standardization. So not clear yet which scheme to use... but that may be clear by the time the MLS approach is ready.