Post-Quantum MLS

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