# ACK / NACK / Re-sync

MLS Interim Jan 2019

# ACK

- How to acknowledge successful receipt and decryption of messages?
- Should these be used within the protocol?
  - If retransmits are included in MLS, should we track per-client delivery?
    - Avoid retransmit when already acked.
  - Would this scale to 100s, 1000s, 10,000s participants?
- Whether / how to authenticate ACKs?
  - Signatures?
  - Is recipient deniability something we care about?
  - What do we gain from authenticating ACKs?

# NACK

- Missed messages?
- Failed decryptions?
- Include retransmit within protocol?
  - Many providers will do this anyway. Safer to include, and prove.
  - Might loosen security guarantees - e.g. weaker notion of PCS.
  - Proof complexity!?!?
- Might require tie-in with application layer.
  - E.g. ephemeral messages.
- Authentication?
  - Signatures?
  - If none, then how does this affect PCS?

# Re-sync

- What if the session is borked?
- How to detect this?
- Individual messages failed to decrypt.
  - Session may still work, might be recoverable.
- Session is broken.
  - Maybe clients' current state is broken.
  - Possibly some shared recent state that might be usable for recovery.
    - How would this affect FS / PCS / formal analysis?
- Session is totally broken.
  - Globally, or just for one client?
  - Fetch new init secrets and re-establish?
  - Might explicitly break a strong notion of PCS.
  - Might maintain a weaker notion of PCS?
- Retransmit missed messages?