Pure PQ key establishment?

- NIST-standardized PQ key establishment (ML-KEM) coming soon
  - How do we deploy them?
- Broad interest in standardizing hybrid PQ/Traditional algorithms
  - E.g., X25519 + ML-KEM-768
  - TLS, SSH, LAMPS
- Some interest in standardizing PQ algorithms alone
  - LAMPS, CNSA 2.0
  - TLS just decided *not* to do this

Should we have a consistent practice across IETF?

- I assume this would be either
  - Standardize both PQ/T hybrid + pure PQ
  - Standardize PQ/T hybrid only and wait on pure PQ

- Mostly you can register code points without a standard
- This is about what IETF recommends