A path forward for PQ KEMs

IETF 125 · Shenzhen · CFRG

Nick Sullivan, CFRG Co-Chair

The problem

IETF needs guidance on which PQ KEMs to use in standards-track protocols.

Candidates: ML-KEM, NTRU, Classic McEliece, FrodoKEM, NTRU Prime, HQC.

IETF 123 poll: first produce a KEM security requirements document.

Proposed approach

Current gap

No requirements document exists. The Fluhrer draft covers ML-KEM only.

Path forward

Adopt per-KEM security evaluation docs.

Eligibility: extensive public cryptanalysis via an open process. Target: ~6 weeks.

Questions

1. Do we need a design team for the common evaluation criteria?
2. Or is mailing list discussion sufficient?

3. Who will write a security evaluation doc for a PQ KEM?