# Terminology for Post-Quantum Traditional Hybrid Schemes

draft-ietf-pquip-pqt-hybrid-terminology

PQUIP – IETF 120

# Context

- An informational draft to standardise a glossary for Post-Quantum/Traditional Hybrids.
- Aims:
  - Ensure consistency across different protocols, standards and organisations.
  - Make it clear what security properties a particular hybrid construction claims.
  - Enable easier comparison of solutions.
- Adopted by PQUIP following IETF 116.
- WGLC between IETF 118 and 119

# Updates since WGLC

- Clarity on scope regarding definition of Traditional Algorithms and ruling out constructs that are not PQ/T Hybrid protocols.
- Add text to reduce ambiguity on definition of composite.
- Clearer info on security properties of PQC.
- Removal of separability definitions – more suitable for draft-ietf-pquip-hybrid-signature-spectrums

# Scope

- Anti-patterns – not currently included. We can add initial terminology, but significant analysis is out of scope. If there is strong appetite to do analysis of security of hybrids, then could be included there.

- Operational considerations – really interesting conversations about operational/impacts of hybrids – not in scope of terminology draft.

- Complexity – draft is not the place for discussion of this.

# Next steps

- Decide whether to go to WGLC or wait for other definitions.

- Contributions/suggestions/feedback
  - Michael.p1@ncsc.gov.uk or pqc mailing list