Terminology for Post-Quantum/Traditional Hybrid Schemes

draft-ietf-pquip-pqt-hybrid-terminology

PQUIP – IETF 119 – 19th March 2024

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 – not ready for publication yet.

Considerations following WGLC

- Benefits of waiting for language to evolve v. providing stable terminology for other drafts.
- The trouble with the word “composite”.
- What words do we actually want defined here?

Next steps

- New version before April interim meeting taking into account WGLC comments.

- Lots of discussions to add precision to use of the word composite.

Get involved!

- Please provide feedback on:
  - What terms you do or don’t want defined in this draft.
  - If this draft is helpful for you in writing protocol drafts, papers etc.
  - How it could be more helpful.
  - Anything else (related to the draft).

- Contact me at flo.d@ncsc.gov.uk or on the pqc list.