Terminology for Post-Quantum Traditional Hybrid Schemes

draft-ietf-pquip-pqt-hybrid-terminology

PQUIP – IETF 117 – 25th July 2023

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.

To discuss today

- Agreement on base definitions
- Splitting the draft?
- Call for contribution

Basic Definitions

- Initiated discussion on the mailing list about the following terminology:
  - Traditional Algorithm
  - Post-Quantum Algorithm
  - Post-Quantum/Traditional Hybrid Scheme
- Small number of responses but these were supportive of using these terms.
- Can we bank this decision?

Splitting the Draft?

- One option is to split this draft in two, forming one draft on terminology for hybrid KEMs and one on terminology for hybrid signatures.
- Pros of splitting:
  - KEMs discussion is likely to be more straightforward, so a KEMs draft could potentially be published more quickly.
  - IETF work is focused on hybrid KEMs rather than hybrid signatures now, so the terminology work could mirror that.
- Cons of splitting:
  - Potential for duplicated work, as there are lots of overlapping definitions.
  - Risk that the signatures work doesn’t get attention.
  - Potential for lack of alignment between drafts.
  - More effort required overall.
- What does the group want to do?

What else?

- What are we missing from the draft?
- Can we test the language against protocol drafts?
- Can we absorb language from other drafts?
- What do you need for this to be useful?

Get involved!

- Contact me at florence.d@ncsc.gov.uk or on the pqc list.
- Co-authors or other contributions very welcome.

Post-Quantum Algorithms (Bonus Slide)

- An asymmetric cryptographic algorithm that is believed to be secure against attacks using quantum computers as well as classical computers.
- Reasons for using “Post-Quantum”:
  - Most widely used term for this algorithm type.
  - Quantum-safe and quantum-resistant suggest properties of the security achieved by the algorithm, rather than the security goals.
  - Quantum-safe has previously been used to include both PQC and QKD.

Traditional Algorithms (Bonus Slide)

- An asymmetric cryptographic algorithm based on integer factorisation, finite field discrete logarithms or elliptic curve discrete logarithms
- Reasons for using “Traditional”:
  - It doesn’t begin with “C” or “PQ” so can form a helpful acronym.
  - Classical describes a type of computer and PQ algorithms are run on classical computers.
  - It is a single word and not too long or technical.
  - It doesn’t suggest that these algorithms are already insecure.

PQ/T Hybrid Scheme (Bonus Slide)

- A multi-algorithm scheme where at least one component algorithm is a post-quantum algorithm and at least one is a traditional algorithm.
- Reasons for using “PQ/T Hybrid Scheme”:
  - Does a good job of describing the components of the scheme.
  - Self-explanatory to a technical reader who hasn’t read this document.
  - Indicates separation between the two algorithm types.