Post-Quantum Algorithms Guidance

draft-prabel-pquip-pqc-guidance-01

L. Prabel , Sun S. , Guang Z. , G. Wang

presented at IETF 123

presentation at IETF 124

IETF 124, Montréal

Reminder: quick overview of the draft

Motivation & Relevance to PQUIP

Why this draft?

- Many PQC algorithms exist, but **information is scattered** across different sources.
- Compliance often requires evaluating **non-NIST schemes** (e.g., European Commission, BSI, ANSSI, …).
- Implementers and protocol designers need **concise**, **unified**, and **comparable** information.
- **Tradeoffs** (size, assumptions, status) between different algorithms can be **hard to track**.
- Relevant to **PQUIP charter** objectives.

Content

What's in the draft?

For a selection of PQC **KEMs** and **Signature** schemes, the draft provides:

- Parameter sizes;
- Claimed security level;
- Security models;
- Underlying security assumptions;
- Standardization status and references to specification;
- Notable characteristics.

➢ Focused on comparison and clarity, not deep technical detail.

➢ It's a curated **summary** to help people navigate the landscape of PQC algorithms.

Since IETF 123

Update to –v1

- Added comments about SUF-CMA security.
- Added general details about PQC Signatures and KEMs.

Feedback received during IETF 123

- "Importance of keeping the draft neutral, as this makes it a useful general reference on PQC".
  - ➢ **no recommendation in the draft, and we will keep it as neutral as possible.**
- "Clear interest in such a draft, but the appropriate format (RFC or living document) is an open question".
  - ➢ **an easily searchable and regularly updated living document sounds right, and received good feedback.**
- "The main challenge seems to be defining the scope and length of the algorithms list"
  - ➢ **for now, only NIST and ISO algorithms, but could be updated following future WG discussions.**

Next Steps

What to do next?

- Are the current **algorithms selection criteria** satisfactory?
- Should we **extend the scope** of the document?
- Interest in **adding specific schemes**?
- Suggestions for **presentation format** or **structure improvements**?

All comments and suggestions are welcome

Next Steps

What to do next?

- Are the current **algorithms selection criteria** satisfactory?
- Should we **extend the scope** of the document?
- Interest in **adding specific schemes**?
- Suggestions for **presentation format** or **structure improvements**?

WG Call for Adoption?

All comments and suggestions are welcome