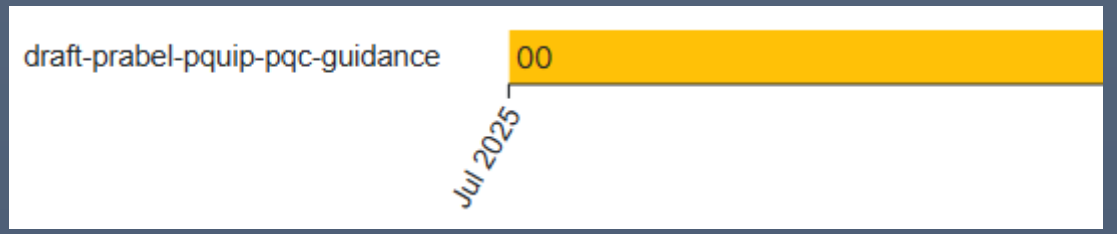
Post-Quantum Algorithms guidance

draft-prabel-pquip-pqc-guidance-00

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



IETF 123, Madrid

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., BSI, ANSSI, European Commission, ...).
- 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

Functionality	Type	Recommended	Acceptable	Deprecated
Key Exchange/ Key Encapsulation	Asymmetric	ML-KEM[1]	FrodoKEM[1] Classic McEliece[1]	ECDH[3] RSA[3]
Digital Signature – Stateless	Asymmetric	ML-DSA[2] SLH-DSA	FN-DSA[2]	ECDSA[3] EdDSA[3] RSA[3]
Digital Signature – Stateful	Asymmetric	XMSS LMS HSS		

Recommended Cryptographic Primitives from the PQC Migration Handbook (AIVD, CWI, TNO)

> *"The WG will document operational and design guidance which supports PQC transition."*
>
> *"The output of this WG is expected to inform protocol work and guidance developed by other WGs in the IETF."*

Extract from PQUIP charter

Intended Audience and Use Cases

Who is this draft for?

- Protocol designers
- Security-conscious developers evaluating tradeoffs
- Implementers of crypto libraries
- Standards bodies evaluating candidate algorithms
- Policymakers requiring a high-level overview

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.

Scheme	Public Key	Private Key	Ciphertext	Shared Secret	Claimed Security Level
FrodoKEM-640-AES	9616	19888	9720	16	1
FrodoKEM-640-SHAKE	9616	19888	9720	16	1
FrodoKEM-976-AES	15632	31296	15744	24	3
FrodoKEM-976-SHAKE	15632	31296	15744	24	3
FrodoKEM-1344-AES	21520	43088	21632	32	5
FrodoKEM-1344-SHAKE	21520	43088	21632	32	5

Content

What's **not** in the draft?

- × Not a recommendation list
- × Not a performance benchmark document
- × Not a formal security proof repository

Algorithms Selection Criteria

How were schemes selected and how will we add more schemes?

- **NIST** and **ISO** standardized algorithms
- Other schemes selected based on:
  - Recommendations from recognized **security agencies or organizations** (e.g., BSI, NCSC, ANSSI, …)
  - Wide **study** in academic and open-source communities
  - Availability of **implementations and benchmarks**
  - Clear relevance to **real-world deployments**

➢ Open to additions: looking for community input

Current list of PQC algorithms

3.1. Key Encapsulation Mechanism (KEM) Schemes

- 3.1.1. ML-KEM
- 3.1.2. FrodoKEM
- 3.1.3. Classic McEliece
- 3.1.4. HQC
- 3.1.5. NTRU

3.2. Signature Scheme

- 3.2.1. ML-DSA
- 3.2.2. FN-DSA
- 3.2.3. SLH-DSA
- 3.2.4. LMS
- 3.2.5. XMSS / XMSS^MT

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 non-NIST schemes?
- Suggestions for presentation format or structure improvements?

All comments and suggestions are welcome