PQC for Engineers

draft-ietf-pquip-pqc-engineers-03

IETF 119 Brisbane, 19th March, 2024

Aritra Banerjee (Nokia)
K Tirumaleswar Reddy (Nokia), Dimitrios Schoininakasis (Nokia), Tim Hollebeek (DigiCert)
Quick recap of the draft

• The draft explains why engineers need to be aware of and understand post-quantum cryptography.

• It emphasizes the potential impact of Cryptographically Relevant Quantum Computers (CRQCs) on current cryptographic systems and the need to transition to post-quantum algorithms to ensure long-term security.

• Adopted by the WG following IETF 117
Changes since IETF 118

• Stateful hash-based signatures (LMS) sizes has been provided as a comparison to SPHINCS+, the XMSS and LMS section has been augmented

• Added a subsection on Ciphertext commitment in KEM verses DH

• Added the point of Hybrid KEMs being IND-CCA2 robust

• Names changed to ML-KEM, ML-DSA, SLH-DSA and FN-DSA, will be merged in the next version.
LMS key and signature sizes

• The LMS scheme is characterized by four distinct parameter sets

  • Underlying hash function (SHA2-256 or SHAKE-256)
  • The length of the digest (24 or 32 bytes)
  • Tree height - parameter that controls a maximal number of signatures that the private key can produce (possible values are 5, 10, 15, 20, 25)
  • The width of the Winternitz coefficients (see {{?RFC8554}}, section 4.1) that can be used to trade-off signing time for signature size (possible values are 1, 2, 4, 8).

• The draft features a table for length of digest, M = 32 bytes
Next Steps

• Sync Name change for PQC algorithms and merge with latest version

• Minor updates via PR on Github.
Contributing to this document

• Comments and Suggestions are welcome. Raise a PR and contribute.

• Thanks to all the Contributors and Reviewers.

• The document is being collaborated on: tireddy2/pqc-for-engineers (github.com)

• E-mail archive: pqc (ietf.org)