COSE and JOSE Registrations for Post Quantum Signatures

draft-prorock-cose-post-quantum-signatures

Mike Prorock
IETF 114, Philadelphia
July 2022
What’s the deal with PQC?

- Why introduce new forms of cryptography?
  - Shor’s Algorithm
- Why support existing standards / formats?
  - Easier path to developer adoption
  - Creates an upgrade path for standards compliant software
- What Algorithms and Why?
  - Signature and Key Representations are the building blocks for secure identifiers and credentials.
  - Stronger agility from supporting multiple primitives
    - Lattice schemes have the best security/size tradeoff
    - Hash schemes have well established security properties
- NIST has announced candidates to be standardized
What are our goals?

- SPHINCS+, Falcon, Dilithium
- Intuitive upgrade path for post quantum
  - Enable leapfrogging from RSA to PQ
- Minimum cryptographic agility
  - Anticipate potential exploits in emerging tech
- Set a path for future PQ algorithms
- IANA Registrations
  - Mitigate ambiguity / parameterization related faults
What is new with PQC?

- Keys and signatures are larger
  - trade off between signing and verification times

- Larger number of parameters for some algorithms
  - we need to keep optionality small based on expert feedback

- We need to be very clear about what parameters are in use with which signature schemes
Next Steps

- Details examples for Falcon and SPHINCS+
- Clarity on kty and alg in WG
- Test vectors, test vectors, test vectors

- Collaboration on OSS Implementations?
- Think about a separate spec for stateful schemes and/or key agreement?
  - XMSS / LMS
  - CRYSTALS-Kyber
Resources

Work Item Repository (Issues, PRs, Details):

Datatracker:

NIST PQC:

Relevant Signature Schemes:
https://pq-crystals.org/dilithium/
https://falcon-sign.info/
https://sphincs.org/