COSE and JOSE Registrations for Post Quantum Signatures

*

draft-prorock-cose-post-quantum-signatures

Mike Prorock
IETF 113, Viena
March 21, 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
- But NIST hasn’t standardized yet….

What are our goals?

- Intuitive upgrade path for post quantum
    - Enable leapfrogging from RSA to PQ
- Minimum cryptographic agility
    - Anticipate potential exploits in emerging tech
- IANA Registrations
    - Mitigate ambiguity / parameterization related faults

What is new with PQC?

- Reliance on ‘alg’ as a MUST parameter
- Larger number of parameters for algorithms - we should reduce optionality based on expert feedback
- As security is often determined by parameterization we need to be very clear about what parameters are in use with which signature schemes

Next Steps

- Improve algorithm descriptions
- Refine the details regarding core cryptographic operations
  - Ascii art?
  - Pseudo code
  - Just reference the papers
- Additional Hash Based Sigs? (XMSS / LMS)
- Test Vectors
  - Example Serializations of JWK and JWS

Resources

Work Item Repository (Issues, PRs, Details):
https://github.com/mesur-io/post-quantum-signatures

Datatracker:
https://datatracker.ietf.org/doc/draft-prorock-cose-post-quantum-signatures/

NIST PQC:
https://csrc.nist.gov/projects/post-quantum-cryptography

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