COSE and JOSE Registrations for Post Quantum Signatures

- draft-ietf-cose-dilithium-01
- draft-ietf-cose-falcon-01
- draft-ietf-cose-sphincs-plus-01

Mike Prorock
IETF 117, San Francisco
July 2023
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
Draft Updates

draft-ietf-cose-dilithium-01
draft-ietf-cose-falcon-01
draft-ietf-cose-sphincs-plus-01

UPDATED TEST VECTORS
LWE -> MLWE in Dilithium

Note to RFC Editor re NIST
Minor Editorial
Addition of acknowledgements and change log
Addition of OpenSSL based Test Vectors:
Help Wanted

- Test vectors, implementation tests, etc
- Parameter set finalization & feedback from NIST
Next Steps

- Request for working group last call
Resources

Work Item Repository (Issues, PRs, Details):

Datatracker(s):
https://datatracker.ietf.org/doc/draft-ietf-cose-dilithium/
https://datatracker.ietf.org/doc/draft-ietf-cose-falcon/
https://datatracker.ietf.org/doc/draft-ietf-cose-sphincs-plus/

NIST PQC:

Relevant Signature Schemes: