COSE and JOSE Registrations for Post Quantum Signatures

draft-ietf-cose-dilithium-02
draft-ietf-cose-sphincs-plus-02

Mike Prorock
IETF 119, San Francisco
March 2024

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-02`
`draft-ietf-cose-sphincs-plus-02`

UPDATED NAMING :
Dilithium → ML-DSA
sphincs+ → SLH-DSA

Updated github locations:
https://github.com/cose-wg/

Significant trim down of drafts now that things are more clearly specified externally

Help Wanted

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

Next Steps

- Bring back over security considerations from -01 drafts into -03 after review for any changes from NIST adjustments to naming and parameters
- IANA registrations?
- Updating test vectors

Resources

Work Item Repository (Issues, PRs, Details):
https://github.com/cose-wg/draft-ietf-cose-dilithium
https://github.com/cose-wg/draft-ietf-cose-sphincs-plus

Datatracker(s):
https://datatracker.ietf.org/doc/draft-prorock-cose-post-quantum-signatures/
https://datatracker.ietf.org/doc/draft-ietf-cose-dilithium/
https://datatracker.ietf.org/doc/draft-ietf-cose-sphincs-plus/

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

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