*

COSE and JOSE Registrations for Post Quantum Signatures

draft-ietf-cose-dilithium-00
draft-ietf-cose-falcon-00
draft-ietf-cose-sphincs-plus-00

Mike Prorock
IETF 116, Yokohama
March 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

- Based on feedback from 115 we have split into 3 drafts:
  - `draft-ietf-cose-dilithium-01`
  - `draft-ietf-cose-falcon-01`
  - `draft-ietf-cose-sphincs-plus-01`

`Does anyone in the group want a `+`?`

Help Wanted

- Naming is hard: Current `kty` by mathematical family - any better suggestions? One `kty` is where we started, where do we finish?

- Test vectors, test vectors, test vectors - need eyes in with additional implementations

- Parameter set finalization & feedback

kty + alg

Do we set up kty for addition of others by family? Or do we line up kty by function overlap?

NTRU - Falcon and others that are NTRU based (e.g. kem)

HASH - sphincs+

LWE - dilithium - short vectors / RLWE / LWE / SIS

this kty bugs me…

Other options: OKP, PQC (for all three), by name… does OKP imply CRV?

Next Steps

- Await finalization on parameter sets
- Optimize naming of `kty + alg`
- Eyes on editorial and language polishing
- General guidance from the group

Resources

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

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-falcon/
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/