CHALLENGES AND OPPORTUNITIES IN POST-QUANTUM CRYPTOGRAPHY FOR NETWORKS AND PROTOCOLS

Sofía Celi
Brave Software, Inc

The state

- NIST ran a process for selection of algorithms to standardise that are safe from quantum computers attacks
  - A first phase of the process ended this month. Announcement of "selected" algorithms for:
    - Key Exchange (KEMs)
    - Authentication (digital signatures)

See NISTs report: https://csrc.nist.gov/publications/detail/nistir/8413/final

The tradeoffs

SIGNATURE ALGORITHMS

Scheme Name	Problem	Public key size (bytes)	Signature size (bytes)
RSA-2048	Factoring	272	256
Ed25519	Elliptic curve discrete logarithm	32	64
Dilithium2	Lattice-based (MLWE/MSIS)	1312	2420
Falcon-512	Lattice-based (NTRU)	897	666
Rainbow-I-Classic	Multi-variate equations	161,600	66
Picnic (L1-FS)	Hash+Block Cipher	32	34032 (max)
XMSS	Hash-based	32	979
SPHINCS+ (128s)	Hash-based	32	8080
SQISign (6983)	Isogeny-based	64	204
MAYO	Multivariate Quadratic	830	420

The tradeoffs

- Bigger sizes, bigger computational times
- They don’t fit perfectly with all ‘DH-like’ actions
- Some schemes don’t have a perfect post-quantum counterpart:
  - OPRFs
  - Zero-Knowledge proofs
  - Threshold Signatures

Some focus

- Continue with experimentation
- Build designs that are generic for post-quantum but also for other ideas

- Workshop on the challenges/opportunities of putting post-quantum into networks and protocols: PQNet (https://sofiaceli.com/PQNet-Workshop/)
  - Next iteration in November (to coordinate with NIST)
  - Important notes:
    - https://sofiaceli.com/PQNet-Workshop/tls.html
    - https://sofiaceli.com/PQNet-Workshop/dnssec.html
- Let's start discussing over: pqc@ietf.org

THANK YOU!

@claucece