BLOCKCHAIN COMMONS

POST-QUANTUM CRYPTOGRAPHY

SYMMETRIC ENCRYPTION

- ChaCha20-Poly1305
  - ChaCha20: 256-bit stream cipher
    - Requires 2^{256} operations to brute force
    - Requrires 2^{128} under quantum attack (Grover's algorithm): still infeasible
  - Poly1305: 128-bit one-time authenticator
    - Requires 2^{128} operations to brute force
    - Requrires 2^{64} under quantum attack: not ideal, still beyond practical feasibility.
- Verdict: even with quantum attacks, ChaCha20-Poly1305 remains secure for the foreseeable future, though post-quantum cryptography research is ongoing to find even more robust replacements.

WHY POST-QUANTUM PUBLIC-KEY CRYPTOGRAPHY?

- **Symmetric encryption (ChaCha20-Poly1305, AES-256, etc.) survives quantum attacks**
  - Grover's algorithm reduces security by half (e.g., 256-bit → 128-bit), but this is still strong
  - Solution: Use 256-bit keys instead of 128-bit keys
- **Public-key cryptography (RSA, ECC, DH) is completely broken by Shor's algorithm**
  - Shor's algorithm solves factoring & discrete log in polynomial time → zero security
  - All current asymmetric systems fail under large quantum computers
  - Post-Quantum Cryptography (PQC) is needed to replace public-key cryptosystems
- **Symmetric crypto stays (with larger keys), but public-key crypto must be replaced**
  - ML-KEM (Kyber, etc.) replaces Diffie-Hellman/X25519 for key exchange
  - ML-DSA (Dilithium, Falcon, etc.) replaces RSA/ECDSA for digital signatures

ALGORITHMS

- ML-DSA (FIPS 204)
  - ***Module Lattice Digital Signature Algorithm***
  - Three levels: 44, 65, and 87
  - Based on, but not the same as "CRYSTALS-Dilithium"
  - Signatures are non-deterministic
  - Not linearly composable like Schnorr signatures (no current PQC DSA is)
- ML-KEM (FIPS 203)
  - ***Module Lattice Key Encapsulation Mechanism***
  - Three levels: 512, 768, and 1024
  - Based on, but not the same as "CRYSTALS-Kyber"

IT'S ALL ABSTRACTED!

- Paradigms for signatures & for key encapsulation are uniform
  - Future-proofed because it's easy to make changes
- You can choose a signature method
  - ML-DSA, ECDSA, Ed25519, Schnorr, SSH
- You can choose an encryption method
  - ChaCha20-Poly1305, ML-KEM
- Not crypto-agile, but crypto-agnostic

NO SLH-DSA YET

- Stateless Hash-Based Digital Signature Standard (FIPS 205)
- Based on, but not the same as SPHINCS+

- It's very large!
- It's redundant with ML-DSA
- But easy to add due to abstraction

PQC CHALLENGES

- Quantum signatures are significantly slower & larger
- Hybrid Quantum is needed
  - Uses PQC to strengthen classic cryptography
  - Emerging approaches from Apple (PQ3) & Signal (PQXDH)
- Use PQC for initiation & periodic rotation
  - Use strong classic cryptography for ongoing usage
- Our recent work uses PQC for Symmetric Key Exchange
  - Then continues with ChaChaPoly
- We still need to release an envelope-cli that fully embraces PQC

COMPARISON OF STRUCTURE SIZES

BETWEEN CLASSICAL AND QUANTUM CRYPTOGRAPHY

		Private Key	Public Key	Size of Signature or Encapsulated Key
Classical	BIP-340 Schnorr	32	32	64
	ECDSA	32	33	64
	Ed25519	32	32	64
Quantum	ML-DSA 44	2560	1312	2420
	ML-DSA 65	4032	1952	3309
	ML-DSA 87	4896	2592	4627
	X25519	32	32	32
	ML-KEM 512	1632	800	768
	ML-KEM 768	2400	1184	1088
	ML-KEM 1024	3168	1568	1568

COMPARISON OF STRUCTURE SIZES BETWEEN CLASSICAL AND QUANTUM CRYPTOGRAPHY