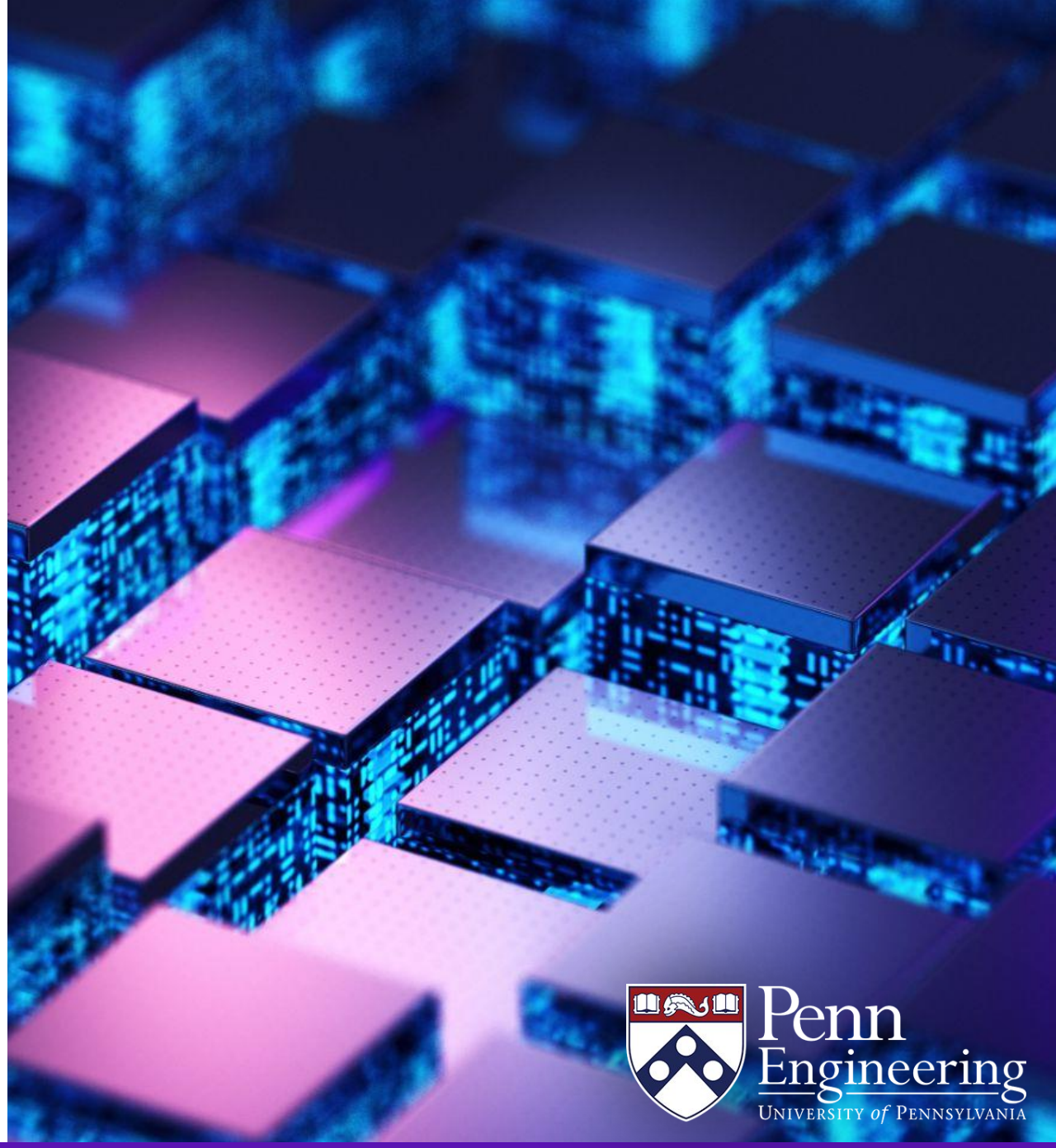
EAS 5830: BLOCKCHAINS

Post-Quantum Cryptography

Professor Brett Hemenway Falk



Penn Engineering
University of Pennsylvania

Cryptographic Hardness Assumptions

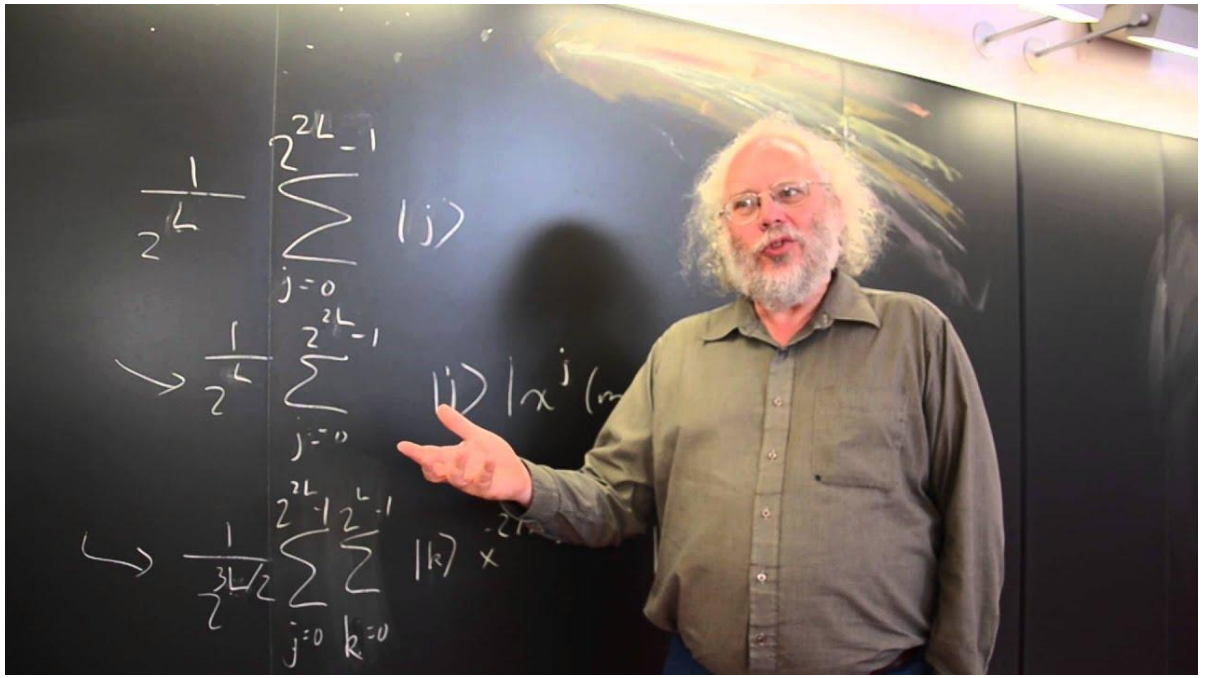
- Most public-key cryptography relies on hardness of certain number-theoretic problems
  - Discrete-Log (El-Gamal, DSA)
    - Blockchains signatures!
  - Factoring (RSA)

- Quantum computers could solve these problems efficiently!

Shor's Algorithm

- Published in 1994

- Shows how to solve factoring and discrete-log problems in polynomial-time *using a quantum* computer



Quantum Computing Today

- Successfully factored 15, 21 and 35 using Shor's algorithm
- IBM's biggest quantum computers have ~1000 qubits. It would likely require more than a 1M qubit quantum computer to break an 256-bit ECDSA signature scheme
- "When will useful quantum computers be constructed? The most optimistic experts estimate it will take 5 to 10 years. More cautious ones predict 20 to 30 years. (Similar predictions have been voiced, by the way, for the last 20 years.)"

Post-Quantum Cryptography

- Factoring- and DL-based cryptography are vulnerable to quantum attacks
- Lattice-based cryptography is believed to be secure
- Symmetric-key crypto (e.g. AES, SHA) is believed to be secure
- NIST is standardizing “post-quantum” cryptographic tools

Are Blockchains Post-Quantum?

- No known quantum attacks on SHA
  - PoW is “post-quantum”
  - Hash chains are post-quantum
- ECDSA is vulnerable to quantum attacks
  - Attacker with quantum computer could forge signatures (and empty wallets)
  - Bitcoin provides modest protection
    - Address is hash of public-key
    - Public-key is not revealed until account is used to send money
    - Address that has received payments but never sent them is quantum safe
- Many “post-quantum” signature schemes exist
  - Not currently implemented in blockchain systems

Moving to Post-Quantum Cryptography

- NIST began soliciting PQC candidates in 2016
  - Anyone can submit a candidate
  - Candidates are publicly examined
- After 3 rounds, 3 digital signature candidates were chosen to be finalized
  - CRYSTALS-Dilithium (Lattice-based)
  - FALCON (Lattice-based)
  - SPHINCS+ (Hash-based)

PQ Signatures have worse parameters

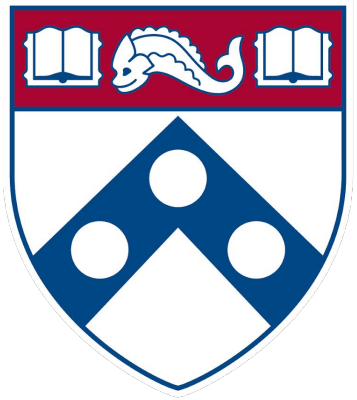
Scheme	PK (bytes)	Signature (bytes)
ECDSA	64	64
Crystals-Dilithium	1320	2420
Falcon	897	666
Sphincs+	32	6856

Making Ethereum Post-Quantum

- Need to replace ECDSA signatures with a PQ signature scheme
- Massive engineering challenge
  - Requires hard fork
  - Everyone needs to upgrade their wallet software
- Account abstraction is a stepping stone
  - Hold funds in contract “wallets” (rather than Externally Owned Accounts)
  - Contracts can require Post-Quantum signatures to take an action
  - Still need ECDSA to get transactions on chain

Quantum Cryptography

- Post-quantum cryptography is cryptography on a classical computer that's secure against quantum attacks
- Quantum cryptography is cryptography *using* a quantum computer
  - First quantum key-exchange in 1984
  - Now being commercialized
    - IDQuantique
    - QuantumXC
- Hardware for quantum key exchange is simpler than hardware for general-purpose quantum computing



Penn
Engineering
UNIVERSITY of PENNSYLVANIA