Post Quantum Crypto

6 May 2026
Lecture 6

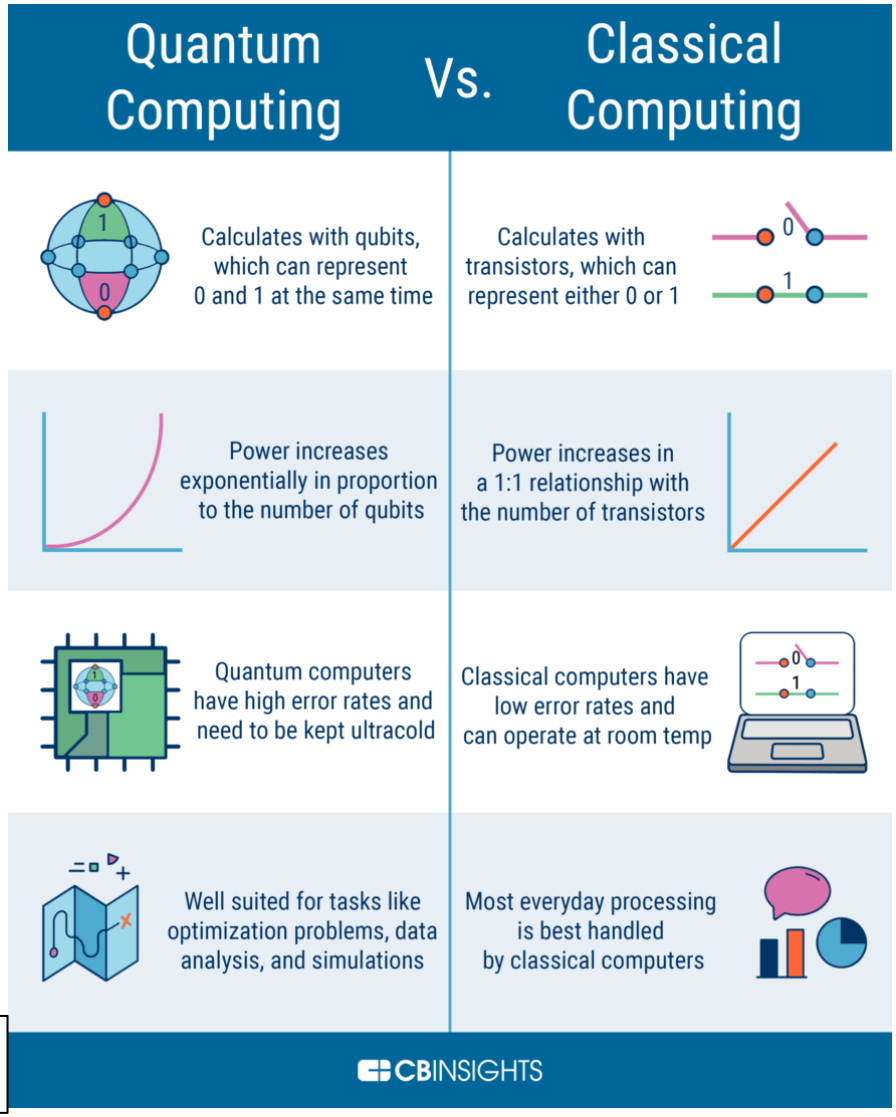
Some Slide Credits: Steve Zdancewic (UPenn)

Topics for Today

- Quantum and Post-Quantum Cryptography

- Sources:
  - HAC 8.2, 10.1-10.3
  - NIST SP 800-38D

Quantum Problems?



https://www.cbinsights.com/research/quantum-computing-classical-computing-comparison-infographic/

Quantum Algorithms

Shor's Algorithm

- Attacks RSA and Elliptical Curve
- Theory - Billions of operations on thousands of qubits
- Fault tolerant – trillions of operations on millions of qubits

RSA and Quantum Computers

RSA security is based on how long it takes to factor very large numbers

Shor's algorithm for quantum computers can factor numbers very fast

- 2021 paper showed how to factor 2048 RSA key in 8 hours
- Need ~20M qubits
- Max qubit size today is 6,100

How long until quantum computers reach millions of qubits?

- 5 years?
- 20 years?
- 25 years?

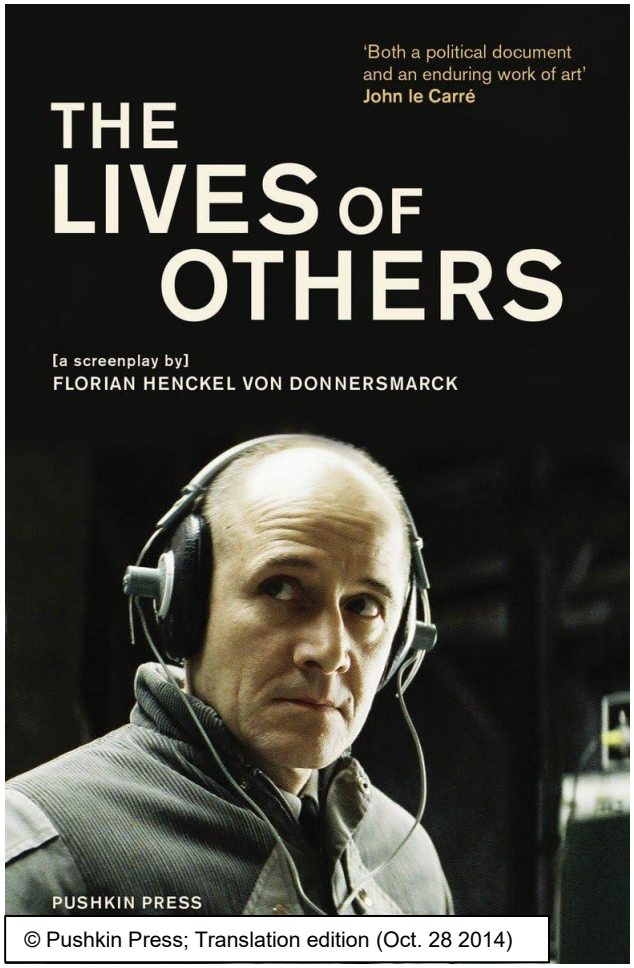
Research and governments working on post-quantum algorithms today

They’re getting bigger

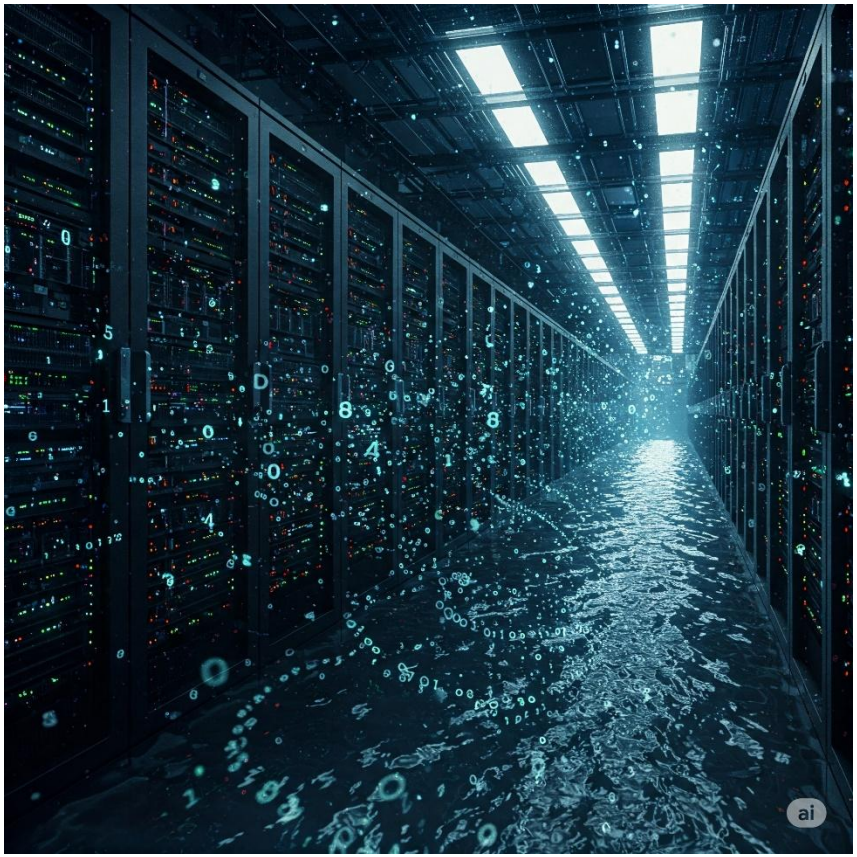
Year	Qubits	Organization	Country	Reference
2011	**128** annealer	D-Wave Systems	Canada	Nature news (2011)
2013	**512** annealer	D-Wave Systems	Canada	D-Wave Two — Wikipedia
2015	**1,000+** annealer	D-Wave Systems	Canada	D-Wave Systems — Wikipedia
2017	**2,000** annealer	D-Wave Systems	Canada	D-Wave Systems — Wikipedia
2018	**72** gate-based	Google	USA	Google AI Blog — Bristlecone
2020	**5,000+** annealer	D-Wave Systems	Canada	D-Wave Systems — Wikipedia
2021	**127** gate-based	IBM	USA	IBM Research — Eagle (127 qubits)
2022	**433** gate-based	IBM	USA	IEEE Spectrum — IBM roadmap
2023	**1,121** gate-based	IBM	USA	IEEE Spectrum — IBM Condor
2025	**6,100** gate-based*	Caltech (Endres Lab)	USA	Caltech news + Nature (Sept 2025)

Record Now Decrypt Later

Today



When a Quantum Computer Arrives



Post Quantum Crypto

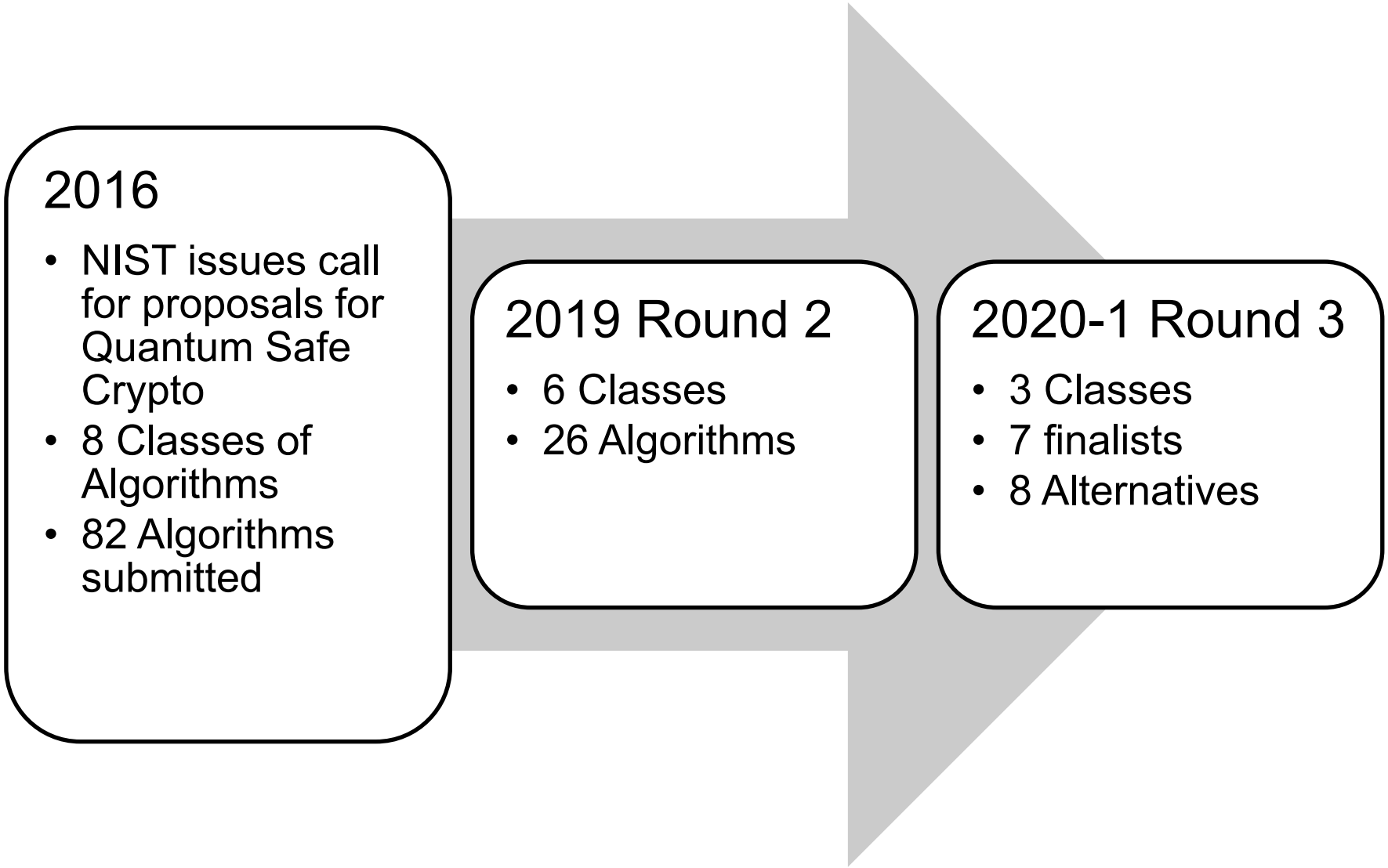
Code based encryption

- Error correcting algorithms
- Intentionally introduce errors
- Keys are big – 1MB

Lattices

- Encryption - 8KB public keys
- Signatures too

Standardizing Post-Quantum



PQC 3rd/4th Round Standards

2022 Round 3

Public/Private Keys

- Lattice Based and Learning with Errors:
  - CRYSTALS-Kyber

Digital Signatures

- Lattice Based
  - CRYSTALS-Dilithium
  - FALCON
- Hash based:
  - SPHINCS+

2025 Round 4 Selected

Public/Private Keys

- Code Based:
  - HQC

In the Pipeline

Backup Public/Private

- Code-based HQC
- In case CRYSTALS-Kyber has problems

Additional Digital Signature

Type	Signature
Lattice	HAWK
Code-Based	CROSS LESS
MPC in the Head	Mirath MQOM PERK RYDE SDitH
Multivariate	MAYO QR-UOV SNOVA UOV
Supersingular Eliptic Curve Isogeny	SQIsign
Symmetric based	FAEST

Conclusion

- Quantum and Post-Quantum Cryptography