NANOG 95

Darn you, Dr. Peter Shor.

The Basics of Quantum Computing and the Threat to Asymmetric Encryption.

Bill Nelson, Not a Doctor.

28 Oct 2025

What We're Doing Here

- The goal is to understand the threat posed by quantum computing by developing a better understanding of:
  - The problem statement of what's called a cryptographically relevant quantum computer (CRQC).
  - How quantum computers work.
  - The state of the art of quantum computing.
  - The future timeline of quantum computing.
  - The mitigation methods available to become quantum computing resistant.
  - But, first, a very little bit about me…

What I am - A curious engineer.

- 26 Year IT Professional working as a Network Engineer building and operating different parts of the internet.
- Have worked for:
  - Internet Service Providers
  - Data Center Providers
  - Manufacturing Companies
  - Different Size Enterprises
- Currently work in an enterprise environment for a Cleveland, Ohio bank, operating their network and firewall devices.

What I am not - A quantum anything.

- Not a quantum physicist
- Not a quantum information scientist
- Not a quantum computer scientist

- The feeling of being an imposter up here is ***strong***.

Why Build Quantum Computers?

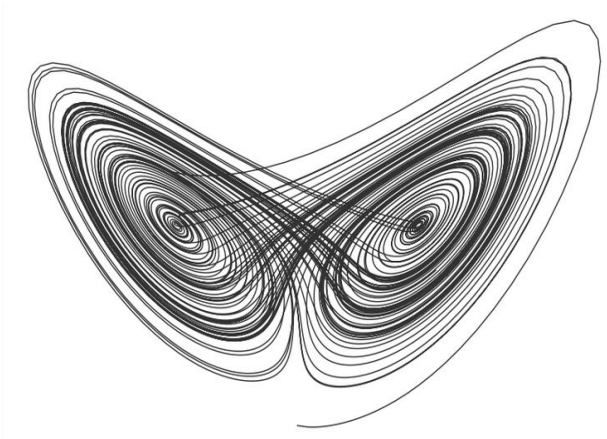
- Originally it was because classical computing hardware simply could not, and still cannot, keep up with the exponential growth simulating quantum mechanical systems takes.
- However, since 1994 it has also - and mostly - been a race to be able to decrypt data with them.

The Problem Statement of a Cryptographically Relevant Quantum Computer (CRQC.)

- All public-key (asymmetric) encryption security relies on the difficulty a classical computer has in solving two types of math problems:
  - Solving discrete logarithms over finite fields and elliptical curves.
  - Factoring large numbers into their prime components
- In 1994 Dr. Peter Shor from MIT discovered a quantum algorithm that excels at solving both of these problems.
- All widely used public-key cryptographic algorithms are then vulnerable to attacks based on Shor's algorithm, but the algorithm depends upon operations that can only be achieved by a large-scale quantum computer[1].

Quantum Concepts and Terms

- It's Weird
- It's Random but Probabilistic
- Wave-Particle Duality
- Wave Function/State Vector
- Measurement Collapse
- **Superposition**
- **Interference**
- **Entanglement**



*

NANOG™

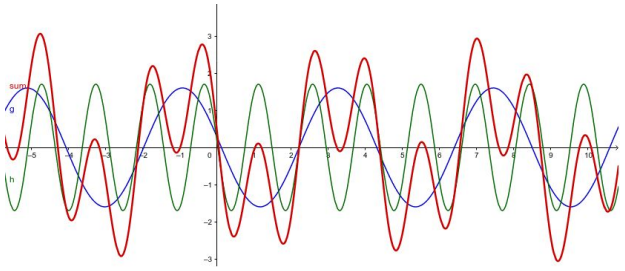
* This image is of the Lorentz Attractor and has **nothing** to do with quantum mechanics. Entanglement has no analogue in the classical world of physics. This is a surreal visual I thought might help imagine entanglement.

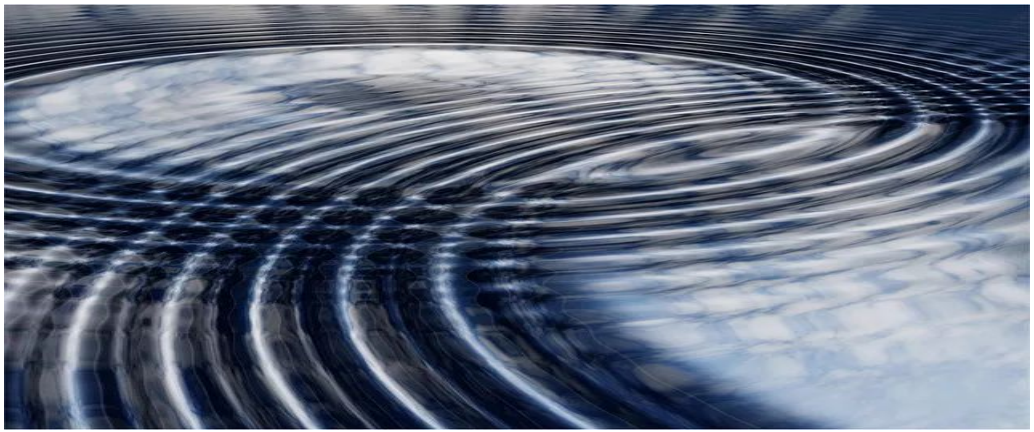
What Do We Need to Know About Quantum Mechanics?

- Classic physics defines the behavior for the large and quantum physics defines the behavior for the molecularly/atomically small.
- At quantum scale particles exist in multiple states at the same time as a probabilistic wave called a superposition.
- The particles will stay in a superposition of probabilistic states until they are measured, at which point the wave function “collapses” into a definite, classical state.

What Do We Need to Know About Quantum Mechanics? (2)

- Interference of Waves:
  - Constructive interference leads to a larger probability wave.
  - Destructive interference leads to a smaller probability wave.

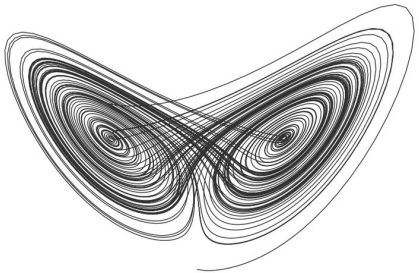




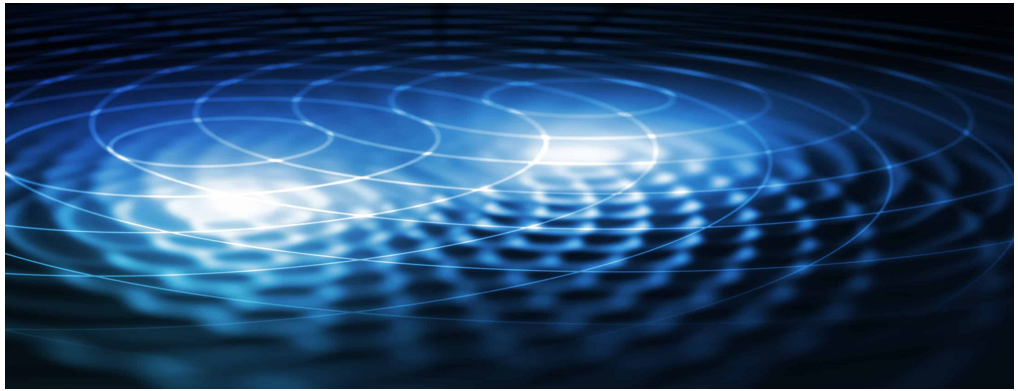
NANOG™

What Do We Need to Know About Quantum Mechanics? (3)

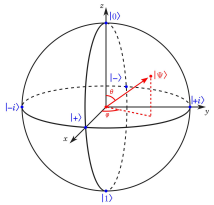
- Entanglement: When two quantum particles are entangled, the state of one particle cannot be described without describing the state of the other.
- No-Cloning Theorem: You cannot duplicate a qubit of an unknown quantum state.



NANOG™



The Qubit

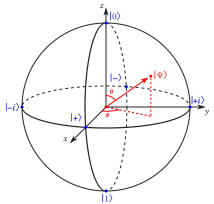


The qubit is the fundamental unit of quantum information.

- Physically, a qubit can be any two-state quantum system.
- Analogous to a classical bit, a qubit can also be in a state of superposition of both a 1 and a 0 at the same time.
- Qubits can be entangled with each other allowing quantum computers to perform ***certain*** calculations exponentially faster than classical computers.

NANOG™

The Qubit (2)

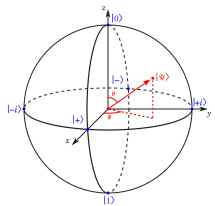


- All qubit implementations are inherently unstable and noisy.
- Decoherence is the state where all of the quantum information has been lost due to noise.
- Types of noise
  - Thermal
  - Electromagnetic
  - Vibration
- Other sources of errors
  - Control signal errors
  - Measurement errors

NANOG™

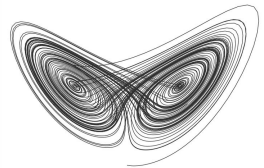
The Logical Qubit - From Many Comes One

- A logical qubit is a combination of physical qubits using special rules called quantum error correction codes.
- If one physical qubit makes a mistake, the others can help figure out what went wrong and fix it.
- The logical (also called an error-corrected) qubit stores quantum information more reliably than any single physical qubit alone.

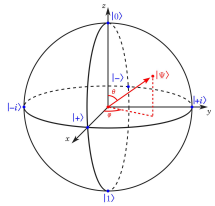


The Entangled Qubit - Quantum Parallelism

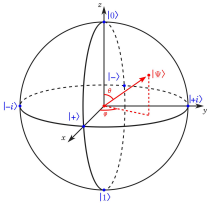
- One qubit can represent 2^1 or 2 states at once.
- Two entangled qubits can represent 2^2 or 4 states at once.
- Three entangled qubits can represent 2^3 or 8 states at once.
- …
- 32 entangled qubits can represent 2^{32} or 4,294,967,296 states at once.
- N entangled qubits can represent 2^N states at once.



NANOG™

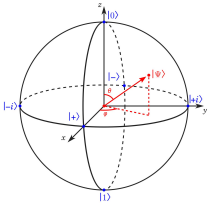


What is a Quantum Logic Gate?



- Quantum logic gates are the components that make up quantum circuits which are what implement quantum algorithms.
- A quantum logic gate performs calculations on qubits by altering:
  - The probabilities of measuring a 1 or a 0.
  - The relative phase between the qubits' interfering waves.

What is a Quantum Logic Gate? (2)



- Quantum logic gates are imposed on the qubits by way of different types of electromagnetic pulses.
- Quantum logic gates have worse error rates than logical qubits, which limits circuit depth which limits algorithm complexity.

A Three-Qubit Computer Computing Example

|000>

|001>

|010>

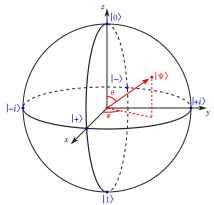
|011>

|100>

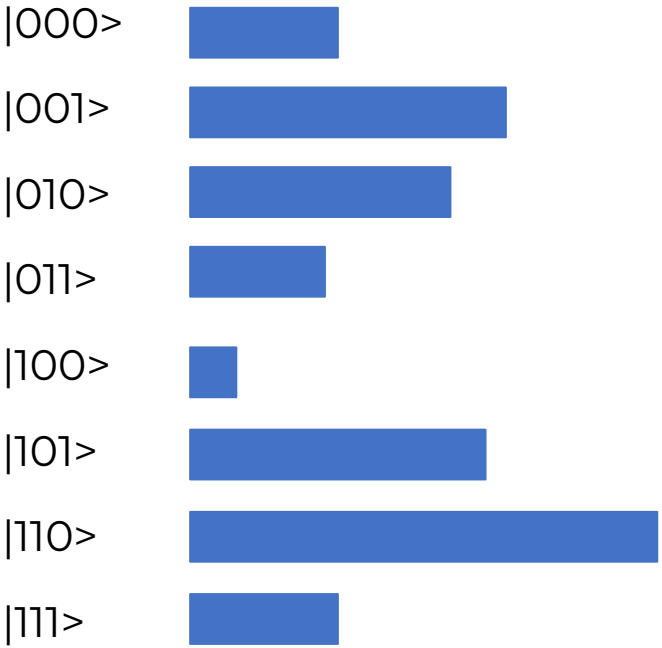
|101>

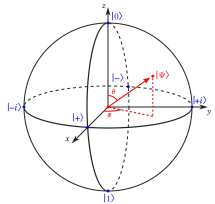
|110>

|111>



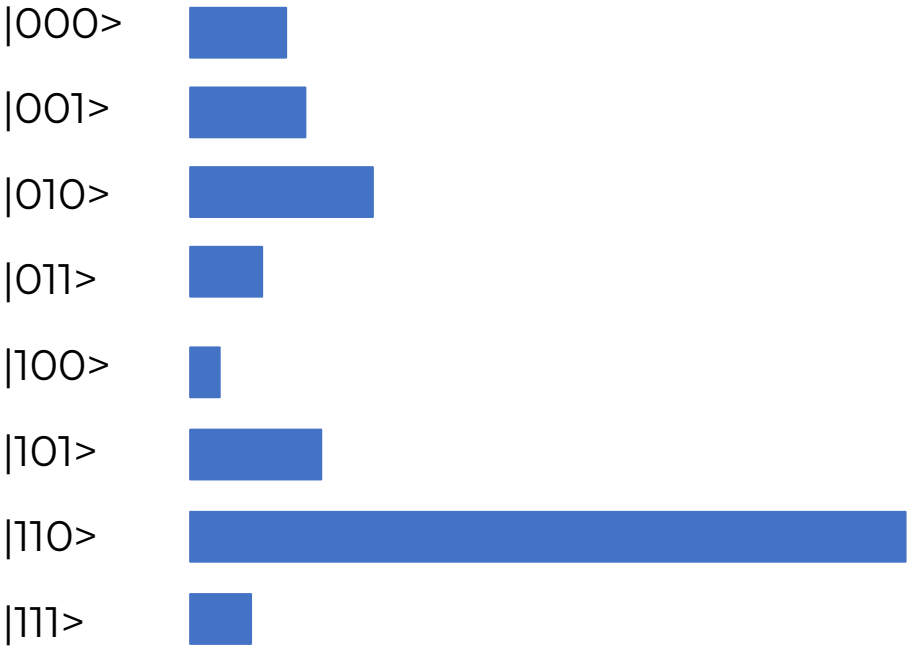
A Three-Qubit Computer Computing Example

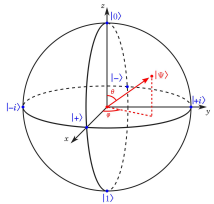




NANOG™

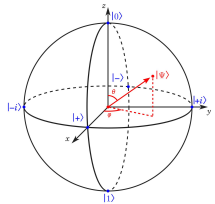
A Three-Qubit Computer Computing Example





NANOG™

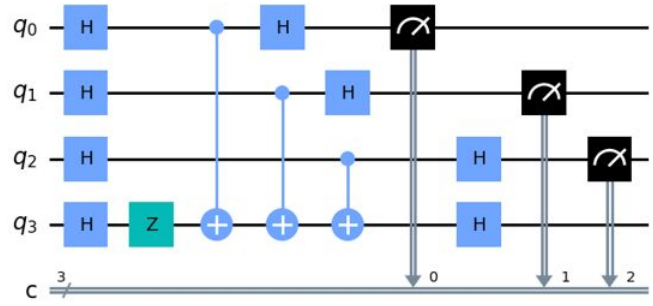
A Three-Qubit Computer Computed Example



NANOG™

The State of the Art - What Variables to Track.

- The number of physical and logical qubits in a QPU.
- The error rate trends of logical qubits.
- The error rate trends of quantum logic gates.



NANOG™

The State of the Art - A Theoretical Danger Zone

- It will take a minimum of 4,098 logical qubits to run Shor's algorithm to break an RSA-2048 bit key. [6]
- Using the math from [6] shows the number of gate operations required to break said key is 6.08×10^{14} operations.

The State of the Art

- Qubit Count
  - Oct 2023: Microsoft/Atom's QPU with 1,225 physical qubits [7]
  - Dec 2023: IBM's Condor QPU with 1,121 physical qubits making up 12 logical qubits. [8]
  - Dec 2023: IBM's Heron R1 QPU with 133 logical qubits. [9]
  - May 2024: Chinese Academy of Science's Ziahong 3.0 QPU with 105 logical qubits. [10]
  - July 2024: IBM's Heron R2 QPU with 156 logical qubits. [11]

The State of the Art (2)

- Qubit Count (cont'd)
  - Nov 2024: Microsoft/Atom's QPU with 24 entangled logical qubits. [12]
  - Dec 2024: Google's Willow QPU with 105 logical qubits and a 49:1 physical to logical qubit ratio [13]
  - Feb 2025: Microsoft's Majorana 1 QPU with 8 error resistant physical qubits that make up 8 "topological" logical qubits. [14] Very much under peer review.
  - Feb 2025: Amazon's Ocelot QPU with 5 error resistant, logical "cat" qubits. [15]

Post Quantum Cryptography (PQC) Mitigation

“If you really have sensitive data, do it now.”

– Vadim Lyubashevsky, IBM Cryptography Researcher

Quantum Computing Timeline

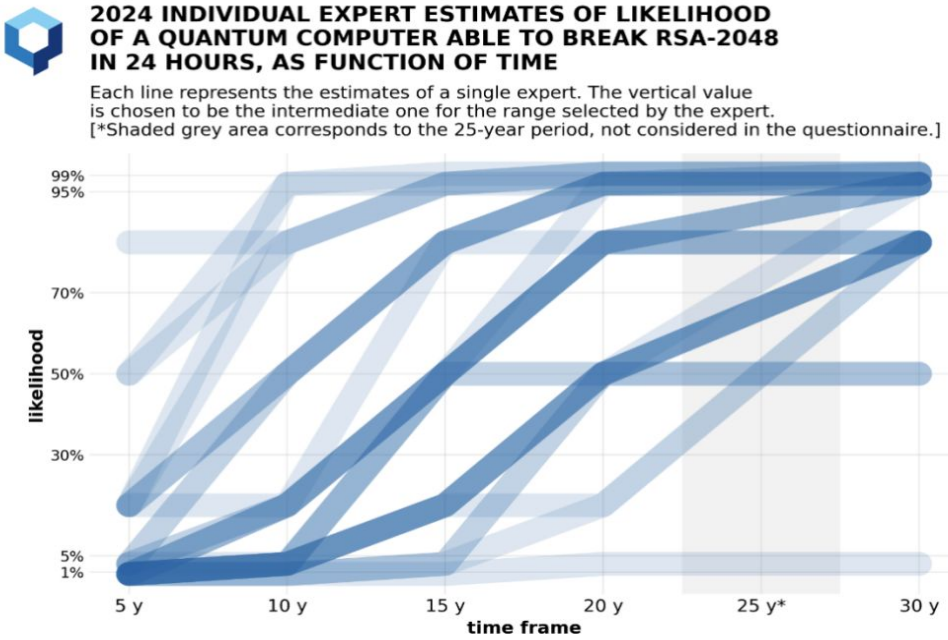
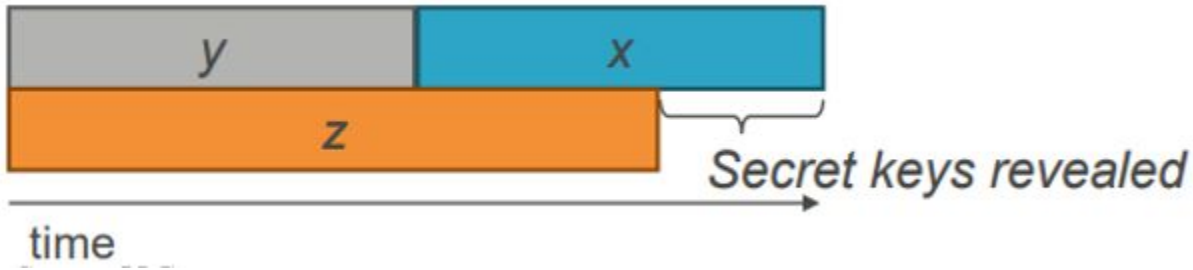


Image 1 - Variance in Expert Estimates [18]

Dr. Mosca's Inequality for Determining Risk

- If X + Y > Z then your data is at risk [21], where:
  - X is the amount of time that your data needs to remain secure.
  - Y is the amount of time it will take to transition your environment to post quantum cryptography (PQC) algorithms.
  - Z is the amount of time it will take to develop a CRQC capable of breaking existing asymmetric encryption algorithms.



PQC Mitigation: 10,000’ View

- You will find every piece of quantum broken/weakened encryption in your IT environment and replace it with standardized, quantum resistant encryption.
- You will document the work done and create centralized, operational documents in order to facilitate something called “crypto-agility.”
    - There is a good chance this work will need to be done more than once.
    - There should not be a reliance on institutional knowledge of individuals.

PQC Mitigation: Crypto-Agility Definition

- Crypto agility facilitates migrations between cryptographic algorithms without significant changes to the application that is using the algorithms. [20]
- Quantum computing is in its infancy and we need to be able to quickly adjust to newly developed/improved/broken algorithms.
- Example: SIKE was an algorithm that got broken late in the standardization process.
  - 4th and final-round NIST candidate
  - Broken in 62 minutes of compute time by a Belgian team using a single, legacy Intel Xeon core.[22]

PQC Mitigation: “New” Math

- NIST Post Quantum Cryptography:
  - **FIPS203**: Module-Lattice based key-encapsulation-method (ML-KEM) algorithm
  - **FIPS204**: Module-Lattice based digital signature standard (ML-DSA) algorithm
  - **FIPS205**: Stateless-Hash based digital signature standard (SLH-DSA) algorithm
  - **FIPS206**: FFT over NTRU-Lattice-Based digital signature standard (FN-DSA) algorithm.
  - **FIPS207**: Hamming-Quasi-Cyclic-Code based key-encapsulation-method (HQC-KEM) algorithm.

PQC Mitigation: IETF RFCs

- IETF RFCs:
  - RFC 8784: Mixing pre-shared keys in IKEv2
  - RFC 9242: IKE layer fragmentation
  - RFC 9370: Multiple key exchanges in IKEv2

PQC Mitigation: 1,000’ View

- Build awareness in the company
  - Senior Management, Legal and Risk Management will need to know
  - SMEs will want to chime in
- Build a team and assign responsibilities
- Develop a crypto inventory and data protection priority list
  - Crypto Bill of Materials/Crypto Agile Single Source of Truth?
- Evaluate solutions and implementation options
- **Experiment and test quantum resistant algorithms.**
  - **These are not drop in replacements for DH/RSA**
  - You’re going to need a real test environment. :-)
- Plan out the migration
- Execute the migration
- Review
- Stay up-to-date with quantum computing and PQC developments
- Repeat as needed
  - Use the crypto agile SSoT’s operational documents.

PQC Mitigation: Finding the Quantum Weak

- Investigate and develop a complete, end-to-end inventory of:
  - 3rd party application encryption
  - Source code encryption
  - OS/firmware/hardware encryption
  - Hardware Security Modules
  - Network encryption - data in flight
  - System encryption - data at rest
  - Cloud environment encryption
  - Vendor interaction encryption
  - Probably more I can’t think of…
  - Data flow diagrams and Visios will really help here…if they exist

PQC Mitigation: Crypto Inventory

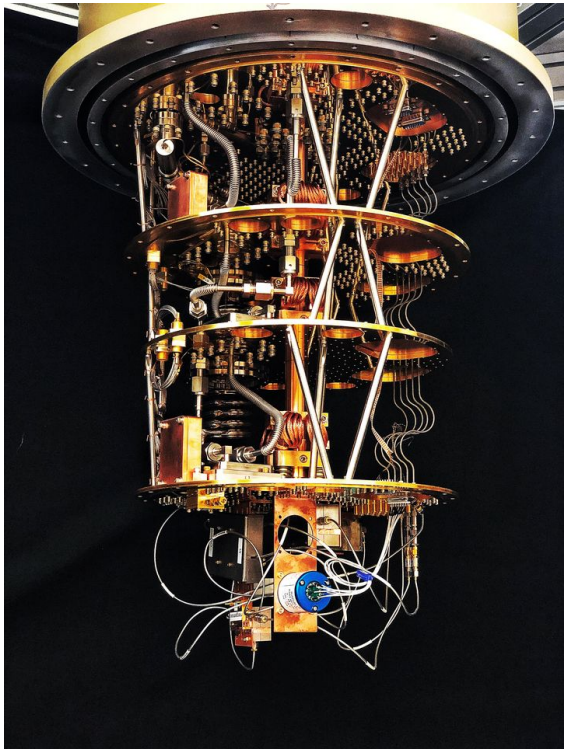
- Each item in the inventory should/could/may/must include:
  - Current key sizes and hardware/software limits on future key and signature sizes.
  - Latency and throughput thresholds
  - Processes and protocols used for crypto negotiation
  - Current key establishment handshake protocols
  - Where each cryptographic process is taking place in the stack.
  - How each cryptographic process is invoked (call to a crypto library, using a process embedded in the OS, calling an application, using cryptography as a service, etc)
  - Whether the implementation supports the notion of cryptographic agility.
  - Whether the implementation may be updated via software
  - Suppliers and owners of each cryptographic process
  - Sources of keys and certificates
  - Contractual and legal conditions imposed by and on the supplier
  - The support lifetime or expected end-of-life of the implementation
  - Sensitivity of the data being protected.
  - And probably some other things…

PQC Mitigation: Vendor/Change Management

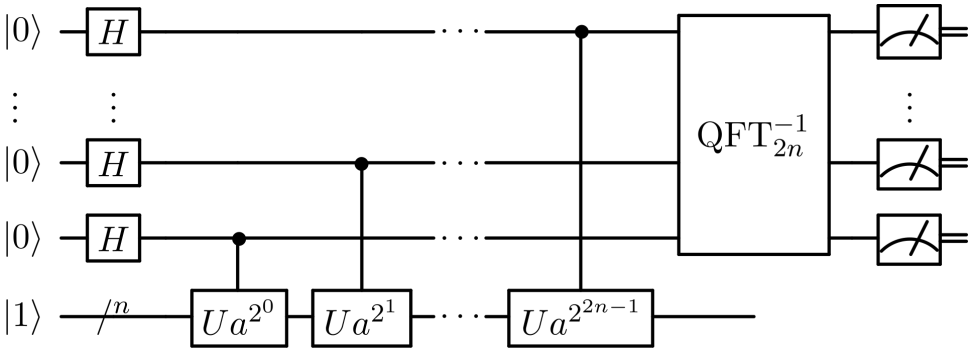
- From this point on, every vendor, architecture change, or hardware/software/firmware release needs to describe the encryption in detail so that PQC readiness is understood and PQC algorithms are implemented where able.

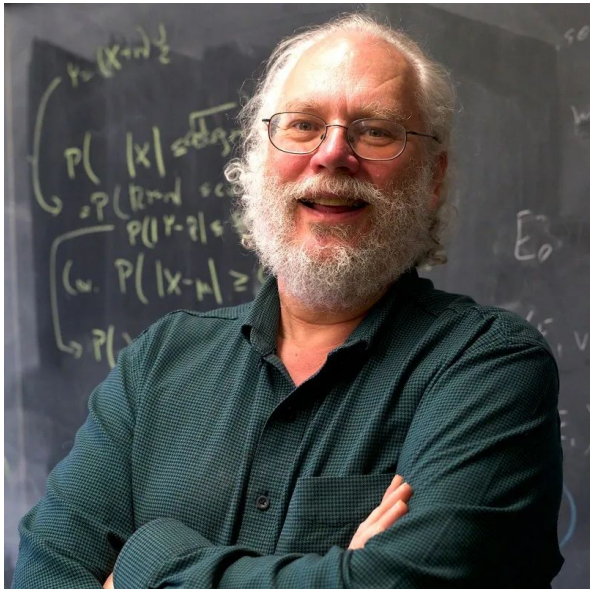
How to Roughly Go About “Quantuming.”

- We need a problem and a quantum algorithm to map it to.
- There are multiple languages to write an algorithm for a quantum computer, depending on the platform. But, mostly Python libraries.
- Choose the number or qubits needed as inputs for our algorithm.
- Compile the algorithm into a series of logic gates in a quantum circuit.
- Insert the QPU into its holder at the bottom of the dilution refrigerator.
- Connect the control cables to the QPU that manipulate one qubit per cable.
- Prep the refrigerator, turn it on and wait a few days or so for the final (lowest) stage to cool down to milliKelvin temperatures
- Specify the number of shots (runs) that need to be made.
- Load and execute the circuit on the quantum computer.
    - Each shot gives a bit string as output.
- Measure and acquire data.
- Interpret the results and validate.



The Quantum Circuit - Shor's Quantum Subroutine





Questions?

28 Oct 2025

Thank you.

28 Oct 2025

NANOG™

References

[1]: NIST CWP, Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf

[2]: Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance, https://www.nature.com/articles/414883a

[3]: Demonstration of Shor's factoring algorithm for N = 21 on IBM quantum processors, https://pmc.ncbi.nlm.nih.gov/articles/PMC8368060/

[4]: NIST Releases First 3 Finalized Post-Quantum Encryption Standards, https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

[5]: NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption, https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption

[6]: How many logical qubits are needed to run Shor's algorithm efficiently on large integers (n>21024), https://quantumcomputing.stackexchange.com/questions/5048/how-many-logical-qubits-are-needed-to-run-shors-algorithm-efficiently-on-large

[7]: https://www.forbes.com/sites/moorinsights/2023/10/24/atom-computing-announces-record-breaking-1225-qubit-quantum-computer/

[8]: https://postquantum.com/industry-news/ibm-condor/

References (2)

[9]: https://postquantum.com/industry-news/ibm-133-qubit-heron-quantum/

[10]: https://quantumcomputingreport.com/chinese-scientists-describe-the-105-qubit-zuchongzhi-3-0-a-competitor-to-googles-willow/

[11]: https://postquantum.com/industry-news/ibm-heron-r2-quantum/

[12]: https://azure.microsoft.com/en-us/blog/quantum/2024/11/19/microsoft-and-atom-computing-offer-a-commercial-quantum-machine-with-the-largest-number-of-entangled-logical-qubits-on-record/

[13]: https://blog.google/technology/research/google-willow-quantum-chip/

[14]: https://www.sciencenews.org/article/microsoft-topological-quantum-majorana

[15]: https://www.amazon.science/blog/amazon-announces-ocelot-quantum-chip

[16]: https://quantumcomputingreport.com/ibm-continues-its-progress-towards-creating-useful-quantum-computing-systems/

[17]: https://spectrum.ieee.org/ieee-quantum-computing-hausi-muller

References (3)

[17]: https://www.quantinuum.com/blog/quantum-volume-milestone

[18]: https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/

[19]: https://quantumai.google/roadmap

[20]: Considerations for Achieving Crypto Agility Strategies and Practices, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.39.ipd.pdf

[21]: What is the Mosca Theorem, https://utimaco.com/service/knowledge-base/post-quantum-cryptography/what-mosca-theorem

[22]: NIST Post-Quantum Cryptography Candidate Cracked, https://cacm.acm.org/news/nist-post-quantum-cryptography-candidate-cracked/

PQC - Further Reading

https://csrc.nist.gov/projects/post-quantum-cryptography

https://csrc.nist.gov/Projects/post-quantum-cryptography/email-list

https://datatracker.ietf.org/doc/draft-ietf-pquip-pqc-engineers/

https://docs.paloaltonetworks.com/network-security/quantum-security/administration/quantum-security-concepts/how-rfc-8784-resists-quantum-computing-threats

https://docs.paloaltonetworks.com/network-security/quantum-security/administration/quantum-security-concepts/how-rfc-9242-and-rfc-9370-resist-quantum-computing-threats

https://www.ibm.com/quantum/blog/crypto-agility

PQC - Further Reading

https://quantumai.google/

https://www.nist.gov/cybersecurity/what-post-quantum-cryptography

https://www.cisa.gov/quantum

https://cloud.google.com/security/resources/post-quantum-cryptography

https://www.microsoft.com/en-us/research/project/post-quantum-cryptography/

https://www.dhs.gov/quantum

https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3498776/post-quantum-cryptography-cisa-nist-and-nsa-recommend-how-to-prepare-now/

https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography

https://pixelplex.io/blog/post-quantum-cryptography/

PQC - Further Reading

IBM Technology – Quantum-Safe Crypto-Agility: Secure Your Enterprise Future - https://www.youtube.com/watch?v=5jPvRs96Kx4

Barker E, Chen L, Moody D, Regenscheid A, Souppaya M, Newhouse B, Housley R, Turner S (2025) Considerations for Achieving Crypto Agility: Strategies and Practices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 39 ipd. https://doi.org/10.6028/NIST.CSWP.39.ipd

https://www.ibm.com/quantum/blog/crypto-agility

https://pqcc.org/wp-content/uploads/2025/05/PQC-Migration-Roadmap-PQCC-2.pdf

https://quantum.microsoft.com/en-us/quantum-ready/get-started

https://www.nccoe.nist.gov/sites/default/files/2022-07/pqc-migration-project-description-final.pdf

https://aws.amazon.com/blogs/security/aws-post-quantum-cryptography-migration-plan/

https://datatracker.ietf.org/doc/html/draft-hoffman-c2pq-07

https://www.gartner.com/en/articles/post-quantum-cryptography

PQC - Further Reading

https://postquantum.com/post-quantum/quantum-enterprise-changes/

https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

https://postquantum.com/post-quantum/practical-steps-quantum/

https://ionq.com/resources/glossary

https://ionq.com/resources/comparing-quantum-computers-metrics-and-monroney

https://postquantum.com/quantum-computing/quantum-computing-benchmarks/

https://ionq.com/resources/quantum-computing-101-introduction-evaluation-applications

https://live.paloaltonetworks.com/t5/quantum-security/ct-p/quantum-security

https://www.ibm.com/quantum/quantum-safe

https://www.cloudflare.com/learning/ssl/quantum/what-is-post-quantum-cryptography/

https://bughunters.google.com/blog/5108747984306176/google-s-threat-model-for-post-quantum-cryptography

https://www.nist.gov/quantum-information-science/quantum-computing-explained