# Information Security Program in the Age of  Quantum Computers

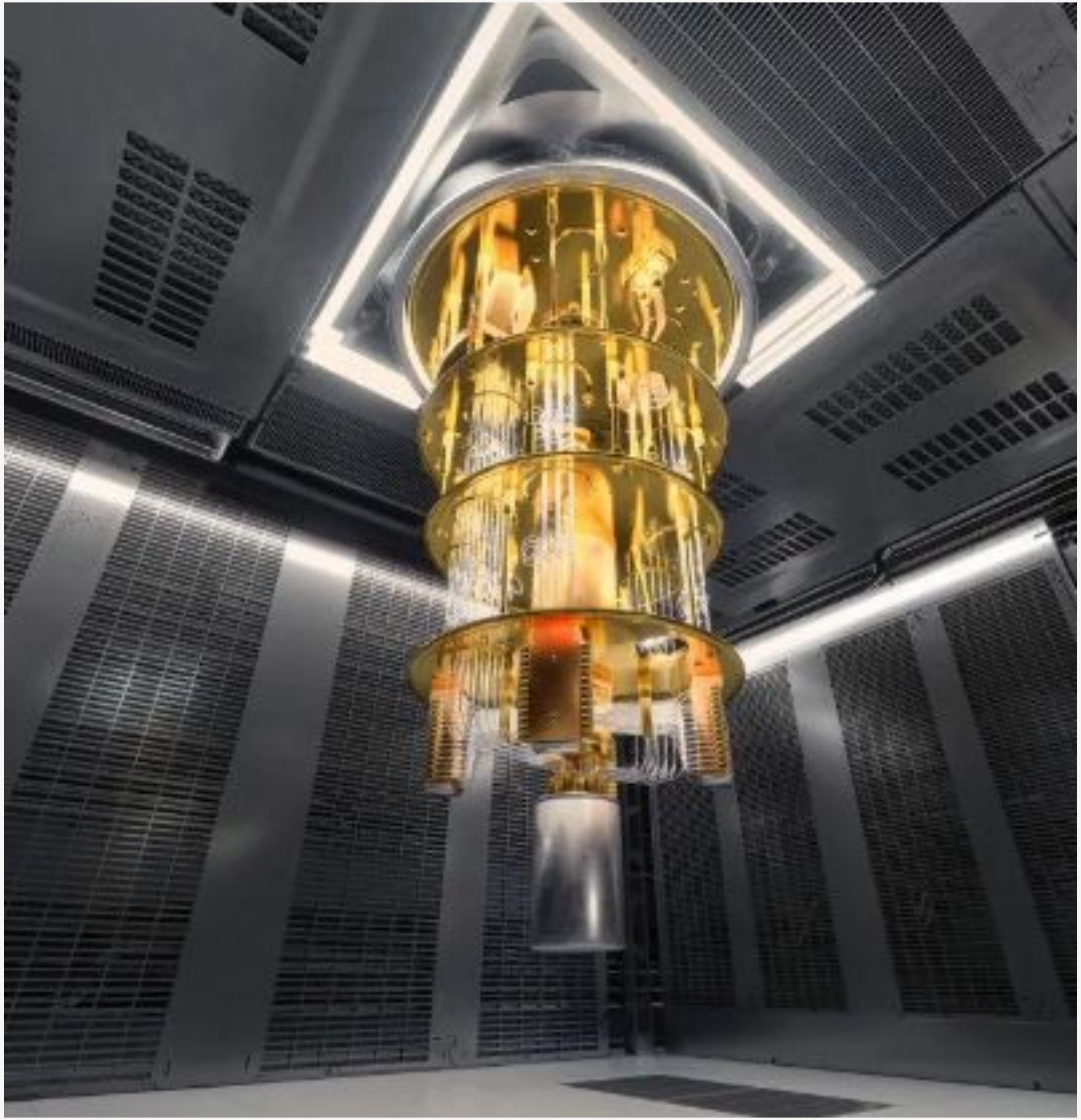
Yev Avidon, CISSP

Director – Data Protection @ Kroger

Past President @ ISC2 Los Angeles Chapter

SINC

2024 Midwest IT and Security Leaders Forum



# Is Quantum Readiness a Deceptive Marketing?

Yev Avidon, CISSP

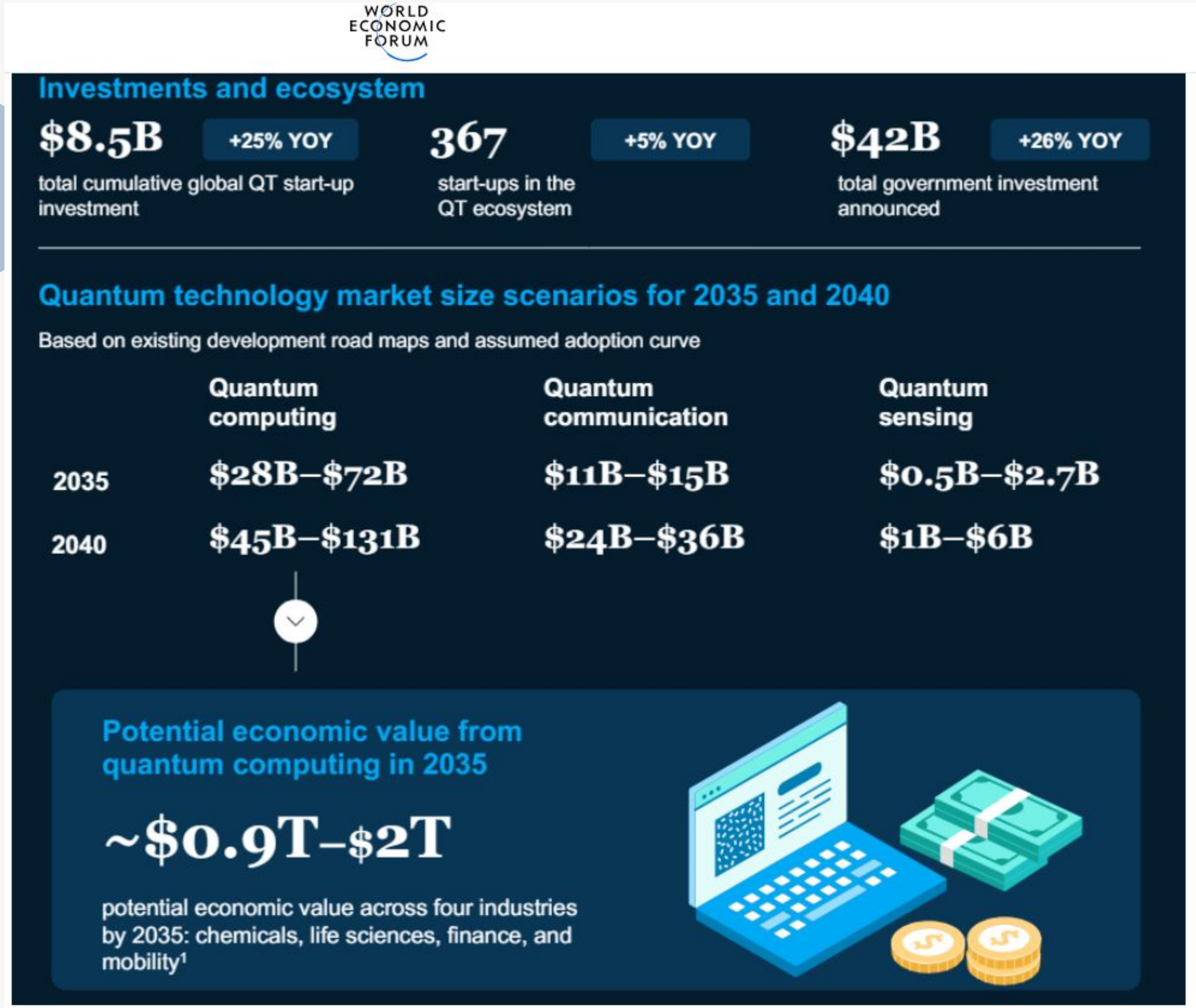
Director – Data Protection @ Kroger

Past President @ ISC2 Los Angeles Chapter

SINC

2024 Midwest IT and Security Leaders Forum

# Quantum Computers Promise



WORLD ECONOMIC FORUM

## Investments and ecosystem

**$8.5B** +25% YOY

total cumulative global QT start-up investment

**367** +5% YOY

start-ups in the QT ecosystem

**$42B** +26% YOY

total government investment announced

## Quantum technology market size scenarios for 2035 and 2040

Based on existing development road maps and assumed adoption curve

| | Quantum computing | Quantum communication | Quantum sensing |
|---|---|---|---|
| 2035 | $28B–$72B | $11B–$15B | $0.5B–$2.7B |
| 2040 | $45B–$131B | $24B–$36B | $1B–$6B |

## Potential economic value from quantum computing in 2035

**~$0.9T–$2T**

potential economic value across four industries by 2035: chemicals, life sciences, finance, and mobility[1]

Quantum technology could be worth trillions within the next decade.

Image: McKinsey

[Explainer: What is quantum technology and what are its benefits? | World Economic Forum (weforum.org)](https://www.weforum.org)

# Fact Sheet: Biden-Harris Administration Continues Work to Secure a Post-Quantum Cryptography Future

Fact Sheet: Biden-Harris Administration Continues Work to Secure a Post-Quantum Cryptography Future | ONCD | The White House

The Biden-Harris Administration is committed to investing in science and technology innovation to solve future problems for our nation, generate jobs and new economic engines, and advance U.S. leadership around the world. While quantum information science (QIS) holds the potential to drive innovations across the American economy, from fields as diverse as materials science and pharmaceuticals to finance and energy, future quantum computers may also have the ability to break some of today's most common forms of encryption.

Though a quantum computer powerful enough to break current forms of cryptography does not yet exist, the Biden-Harris Administration is preparing for and mitigating the risks to government and critical infrastructure systems posed by a potential future quantum computer and promoting U.S. and allied leadership in quantum technology.

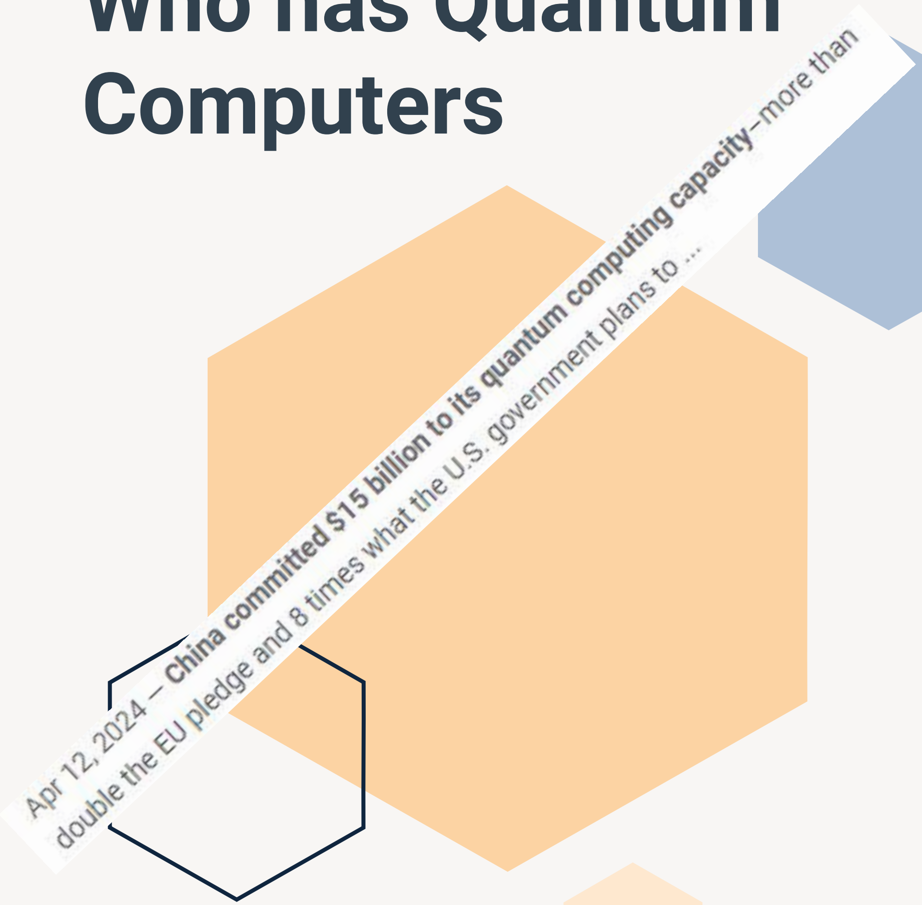
To protect against the potential risks to the economic and national security of the United States and our partners, this Administration has remained laser focused—as outlined in President Biden's National Security Memorandum 10 (NSM-10)—on post-quantum cryptography. Post-quantum cryptography is a foundational tool for assuring data safety and security for the nation and for our future.

In 2022, President Biden issued an executive order elevating the National Quantum Initiative Advisory Committee (NQIAC) to a Presidential Advisory Committee. The NQIAC consists of leaders in the field from industry, academia and the Federal Laboratories, and highlights the importance of a whole-of-government approach to QIS.

The Office of Management & Budget (OMB) issued Memorandum M-23-02, Migrating to Post-Quantum Cryptography, which lays out clear steps for agencies to follow in preparation for migrating to these new NIST cryptography standards. Those steps include conducting a comprehensive and ongoing cryptographic inventory and prioritizing critical and sensitive systems for migration.

The Office of the National Cyber Director (ONCD): Through the Biden-Harris Administration's National Cybersecurity Strategy released in March 2023, ONCD is working to prepare for the post-quantum future. This includes supporting the implementation of NSM-10 by conducting an inventory of government systems. This inventory will identify where there is vulnerable cryptography and what needs to be prioritized. ONCD is also working internationally with allies to create a cohesive message on the need to implement post-quantum cryptography. This work seeks to drive a collective call to action for government leaders and financial decisionmakers and start the cryptographic transition today.

# Who has Quantum Computers



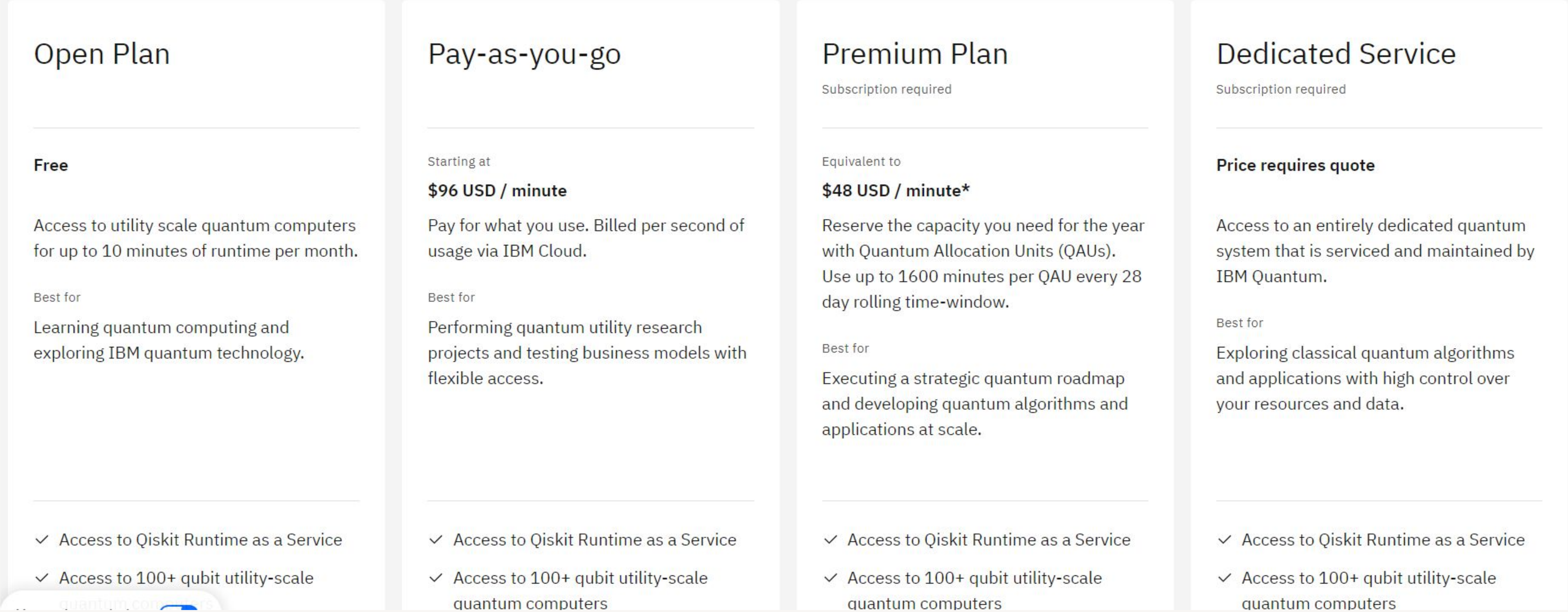
Apr 12, 2024 — **China committed $15 billion to its quantum computing capacity**—more than double the EU pledge and 8 times what the U.S. government plans to ...

In 2022, GlobalData said the U.S. was about five years ahead of China in the quantum computing race. Now, in 2024, the firm considers the two countries as “nearly equal” in the arena.

There are currently around 100 companies globally that are actively involved in the development of quantum computing technologies. These companies range from large tech giants like IBM, Google, and Microsoft to numerous startups focusing on various aspects of quantum computing, including hardware, software, and applications.

**United States:** The U.S. is a major player with significant investments from companies like IBM, Google, and Microsoft.
**China:** China has made substantial investments in quantum technology and has developed several quantum computing prototypes.
**Canada:** Known for its strong quantum research community, Canada is home to companies like D-Wave and has national strategies to support quantum technology.
**Germany:** Germany is heavily investing in quantum research and development, with numerous initiatives and collaborations.
**Japan:** Japan is also advancing in quantum computing with significant contributions from both government and private sectors.
**United Kingdom:** The UK has a robust quantum computing ecosystem with many startups and research institutions.
**France:** France is investing in quantum technologies through national programs and partnerships.

# Quantum Computers cost of Use



## Open Plan

**Free**

Access to utility scale quantum computers for up to 10 minutes of runtime per month.

Best for

Learning quantum computing and exploring IBM quantum technology.

- ✓ Access to Qiskit Runtime as a Service
- ✓ Access to 100+ qubit utility-scale quantum computers

## Pay-as-you-go

Starting at

**$96 USD / minute**

Pay for what you use. Billed per second of usage via IBM Cloud.

Best for

Performing quantum utility research projects and testing business models with flexible access.

- ✓ Access to Qiskit Runtime as a Service
- ✓ Access to 100+ qubit utility-scale quantum computers

## Premium Plan

Subscription required

Equivalent to

**$48 USD / minute***

Reserve the capacity you need for the year with Quantum Allocation Units (QAUs). Use up to 1600 minutes per QAU every 28 day rolling time-window.

Best for

Executing a strategic quantum roadmap and developing quantum algorithms and applications at scale.

- ✓ Access to Qiskit Runtime as a Service
- ✓ Access to 100+ qubit utility-scale quantum computers

## Dedicated Service

Subscription required

**Price requires quote**

Access to an entirely dedicated quantum system that is serviced and maintained by IBM Quantum.

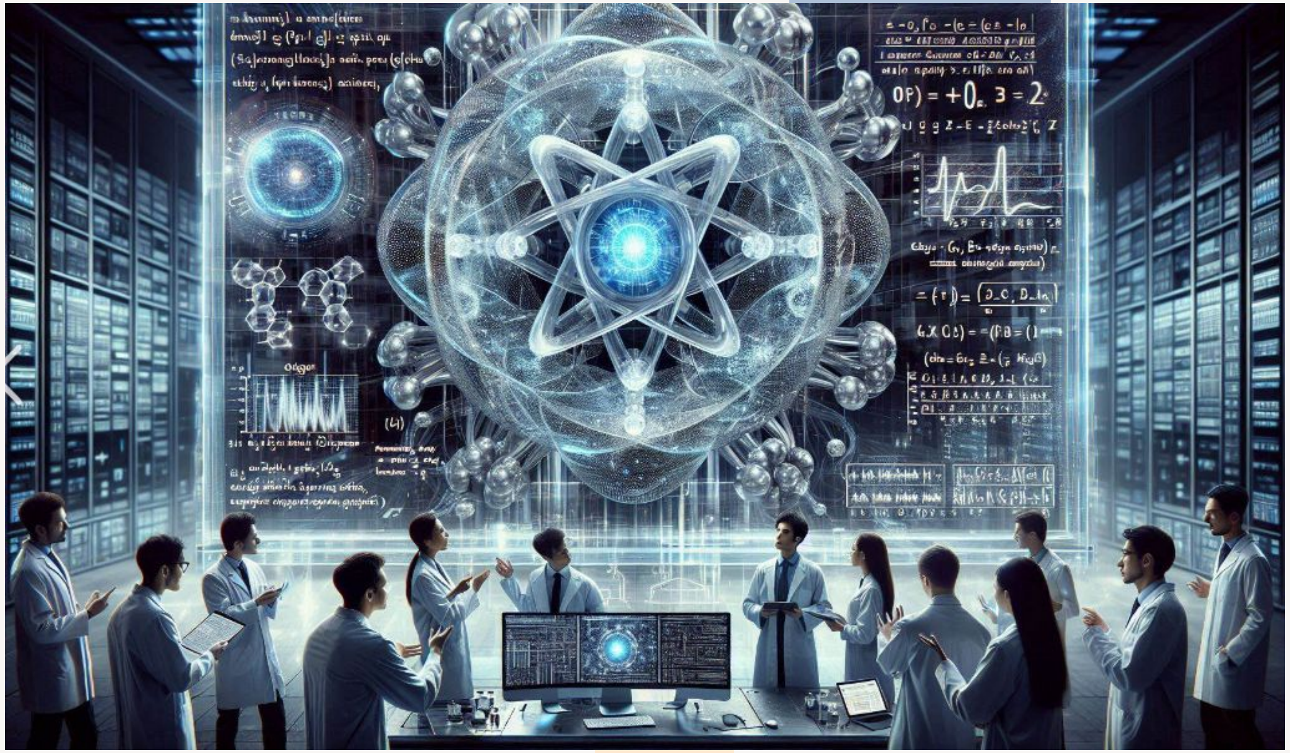
Best for

Exploring classical quantum algorithms and applications with high control over your resources and data.

- ✓ Access to Qiskit Runtime as a Service
- ✓ Access to 100+ qubit utility-scale quantum computers

Pricing | IBM Quantum Computing

# Quick Definitions



**Quantum Gates**: These are the building blocks of quantum circuits, similar to classical logic gates in traditional computing. They perform operations on qubits, changing their states through unitary transformations.
**Qubits**: These are the basic units of quantum information. They can exist in a superposition of states, meaning they can be both 0 and 1 simultaneously.
**Operations**: Quantum gates operate on qubits to perform computations. For example, a single-qubit gate might rotate the state of a qubit on the Bloch sphere, while a multi-qubit gate like the CNOT gate entangles two qubits.
**Quantum Circuits**: A sequence of quantum gates applied to qubits forms a quantum circuit, which can execute complex quantum algorithms.

In essence, quantum gates are the tools used to manipulate qubits, enabling the execution of quantum algorithms and ultimately harnessing the power of quantum computing.

# How Many Qubits will take to break Encryption Standards

The number of qubits required to break encryption depends on the type and strength of the encryption. Here are some estimates:

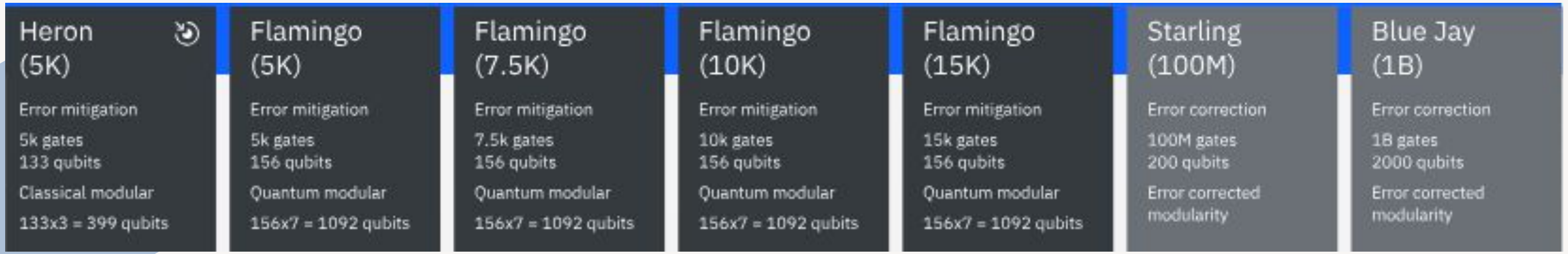
**RSA Encryption:** To break a 2048-bit RSA key, it is estimated that a quantum computer would need around 20 million qubits. However, recent research suggests that with optimized algorithms, it might be possible with fewer qubits, but still in the range of hundreds to thousands.

**AES Encryption:** For AES-128 encryption, approximately 2,953 logical qubits are needed, while AES-256 would require around 6,681 logical qubits.

**Bitcoin Security:** Breaking Bitcoin’s encryption could require a quantum computer with around 13 million qubits

Created by Copilot

# IBM Development Roadmap



Heron (5K)
Error mitigation
5k gates
133 qubits
Classical modular
133x3 = 399 qubits

Flamingo (5K)
Error mitigation
5k gates
156 qubits
Quantum modular
156x7 = 1092 qubits

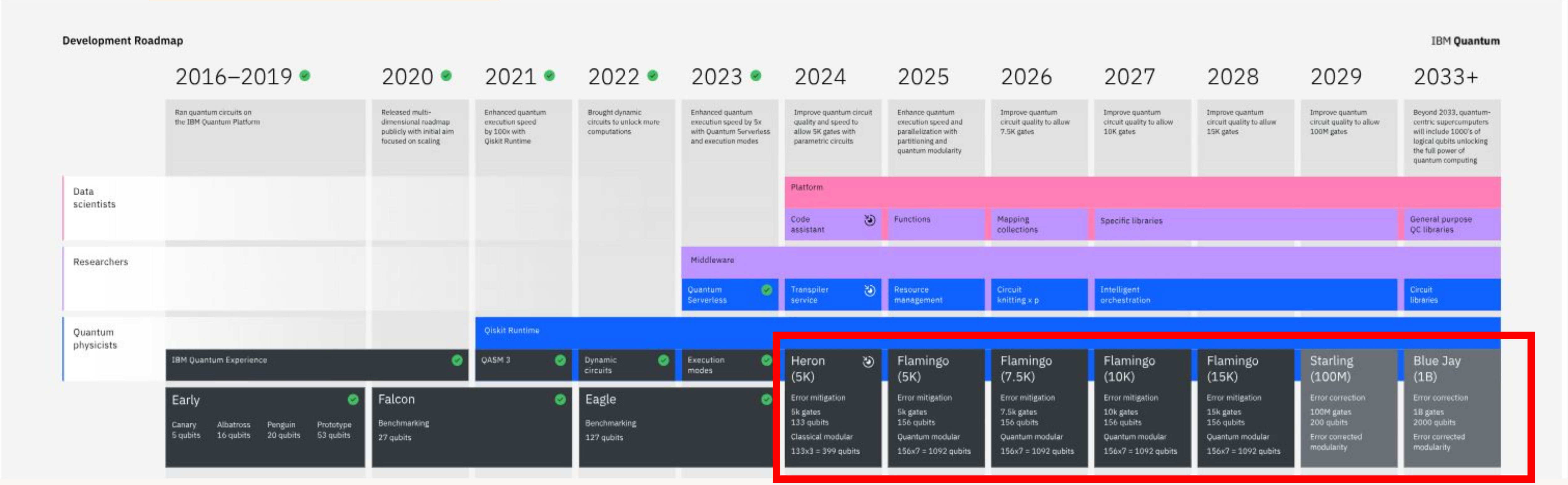
Flamingo (7.5K)
Error mitigation
7.5k gates
156 qubits
Quantum modular
156x7 = 1092 qubits

Flamingo (10K)
Error mitigation
10k gates
156 qubits
Quantum modular
156x7 = 1092 qubits

Flamingo (15K)
Error mitigation
15k gates
156 qubits
Quantum modular
156x7 = 1092 qubits

Starling (100M)
Error correction
100M gates
200 qubits
Error corrected modularity

Blue Jay (1B)
Error correction
1B gates
2000 qubits
Error corrected modularity



Development Roadmap

IBM Quantum

2016–2019 ✓
Ran quantum circuits on the IBM Quantum Platform

2020 ✓
Released multi-dimensional roadmap publicly with initial aim focused on scaling

2021 ✓
Enhanced quantum execution speed by 100x with Qiskit Runtime

2022 ✓
Brought dynamic circuits to unlock more computations

2023 ✓
Enhanced quantum execution speed by 5x with Quantum Serverless and execution modes

2024
Improve quantum circuit quality and speed to allow 5K gates with parametric circuits

2025
Enhance quantum execution speed and parallelization with partitioning and quantum modularity

2026
Improve quantum circuit quality to allow 7.5K gates

2027
Improve quantum circuit quality to allow 10K gates

2028
Improve quantum circuit quality to allow 15K gates

2029
Improve quantum circuit quality to allow 100M gates

2033+
Beyond 2033, quantum-centric supercomputers will include 1000's of logical qubits unlocking the full power of quantum computing

Data scientists
- Platform
- Code assistant
- Functions
- Mapping collections
- Specific libraries
- General purpose QC libraries

Researchers
- Middleware
- Quantum Serverless ✓
- Transpiler service
- Resource management
- Circuit knitting x p
- Intelligent orchestration
- Circuit libraries

Quantum physicists
- Qiskit Runtime
- IBM Quantum Experience ✓
- QASM 3 ✓
- Dynamic circuits ✓
- Execution modes ✓

Early ✓
Canary 5 qubits
Albatross 16 qubits
Penguin 20 qubits
Prototype 53 qubits

Falcon ✓
Benchmarking
27 qubits

Eagle ✓
Benchmarking
127 qubits

Heron (5K)
Error mitigation
5k gates
133 qubits
Classical modular
133x3 = 399 qubits

Flamingo (5K)
Error mitigation
5k gates
156 qubits
Quantum modular
156x7 = 1092 qubits

Flamingo (7.5K)
Error mitigation
7.5k gates
156 qubits
Quantum modular
156x7 = 1092 qubits

Flamingo (10K)
Error mitigation
10k gates
156 qubits
Quantum modular
156x7 = 1092 qubits

Flamingo (15K)
Error mitigation
15k gates
156 qubits
Quantum modular
156x7 = 1092 qubits

Starling (100M)
Error correction
100M gates
200 qubits
Error corrected modularity

Blue Jay (1B)
Error correction
1B gates
2000 qubits
Error corrected modularity

Technology | IBM Quantum Computing

# What are we trying to Protect

NIST’s new standards are designed for two essential tasks for which encryption is typically used:

General data encryption, used to **protect information exchanged across a network or sitting at rest on a computer**;

Digital signatures, used for **identity authentication**.

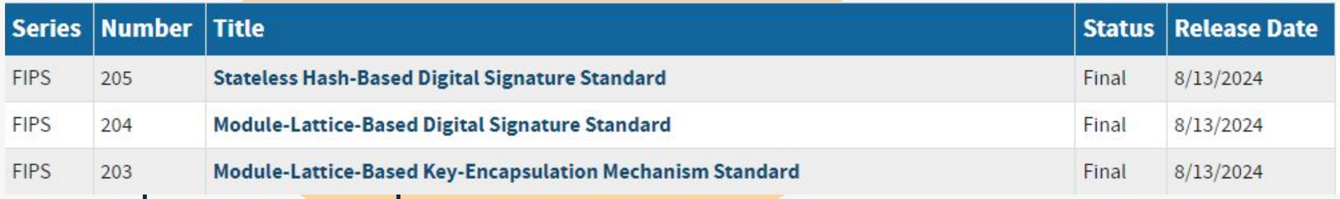
These standards replace current cryptographic standards that could be vulnerable to a future quantum computer. These standards allow federal agencies and industry to adopt and integrate these new tools into systems and products.

Fact Sheet: Biden-Harris Administration Continues Work to Secure a Post-Quantum Cryptography Future | ONCD | The White House

# National Institute of Standards and Technology (NIST)

| Year | # of Algorithms/standards |
|---|---|
| 2016 | 0 (Post Quantum Cryptography Standardization Project started) |
| 2017 | 69/0 |
| 2022 | 4/3 |
| 2024 | 4/3 will be 4 |

**CRYSTALS-Kyber:** This algorithm is used for public-key encryption and key encapsulation. It's known for its efficiency and strong security properties.
**CRYSTALS-Dilithium:** This is a digital signature scheme that provides strong security guarantees and is designed to be efficient in both signing and verification processes.
**SPHINCS+:** Another digital signature scheme, SPHINCS+ is based on hash functions and is designed to be secure even if other cryptographic assumptions fail.
**FALCON:** This digital signature algorithm is known for its compact signatures and efficient verification, making it suitable for various applications.



| Series | Number | Title | Status | Release Date |
|---|---|---|---|---|
| FIPS | 205 | Stateless Hash-Based Digital Signature Standard | Final | 8/13/2024 |
| FIPS | 204 | Module-Lattice-Based Digital Signature Standard | Final | 8/13/2024 |
| FIPS | 203 | Module-Lattice-Based Key-Encapsulation Mechanism Standard | Final | 8/13/2024 |

Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. In addition, the recipient of signed data can use a digital signature as evidence in demonstrating to a third party that the signature was, in fact, generated by the claimed signatory. This is known as non-repudiation since the signatory cannot easily repudiate the signature at a later time. SLH-DSA is based on SPHINCS$^{+}$.

Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory... This is known as non-repudiation since the signatory cannot easily repudiate the signature at a later time. This standard specifies ML-DSA, a set of algorithms that can be used to generate and verify digital signatures. ML-DSA is believed to be secure, even against adversaries in possession of a large-scale quantum computer.

A key-encapsulation mechanism (KEM) is a set of algorithms that, under certain conditions, can be used by two parties to establish a shared secret key over a public channel. A shared secret key that is securely established using a KEM can then be used with symmetric-key cryptographic algorithms to perform basic tasks in secure communications, such as encryption and authentication. This standard specifies a key-encapsulation mechanism called ML-KEM. The security of ML-KEM is related to the computational difficulty of the Module Learning with Errors problem. At present, ML-KEM is believed to be secure, even against adversaries who possess a quantum computer. This standard specifies three parameter sets for ML-KEM. In order of increasing security strength and decreasing performance, these are ML-KEM-512, ML-KEM-768, and ML-KEM-1024.

NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers | NIST

# Chinese Researchers Perform Space-to-Ground Communications With Lightweight Quantum Satellite

Chinese researchers report on a compact quantum microsatellite that achieves secure space-to-ground communications through quantum key distribution (QKD) with portable ground stations.

The microsatellite, weighing just 23 kilograms, represents a significant reduction in size and weight compared to previous quantum satellites, enabling more flexible and rapid deployment.

The system achieved real-time secure communication, sharing up to 0.59 million bits of secure keys in a single satellite pass.

Chinese Researchers Perform Space-to-Ground Communications With Lightweight Quantum Satellite (thequantuminsider.com)

# IBM’s Big Bet on the Quantum-Centric Supercomputer

…quantum computers and classical computers will work together to run computations beyond what’s possible on either alone.

Several supercomputer facilities around the world are already planning to incorporate quantum-computing hardware into their systems, including Germany’s Jupiter, Japan’s Fugaku, and Poland’s PSNC. While it has previously been called hybrid quantum-classical computing, and may go by other names, we call this vision quantum-centric supercomputing.

IBM’s Quantum-Centric Supercomputing Vision Is Coming - IEEE Spectrum

# 'Unbreakable' quantum communication closer to reality thanks to new, exceptionally bright photons

Scientists have created an "exceptionally bright" light source that can generate quantum-entangled photons (particles of light) which could be used to securely transmit data in a future high-speed quantum communications network.

A future quantum internet could transmit information using pairs of entangled photons — meaning the particles share information over time and space regardless of distance. Based on the weird laws of quantum mechanics, information encoded into these entangled photons can be transferred at high speeds while their "quantum coherence" — a state in which the particles are entangled — ensures the data cannot be intercepted.

'Unbreakable' quantum communication closer to reality thanks to new, exceptionally bright photons | Live Science

# Breakthrough quantum algorithm can break advanced data encryption

Researchers at MIT have achieved a breakthrough in quantum computing.
They have developed a novel algorithm that can enable quantum machines to quickly break the encryption methods that currently protect our digital world.

It also underscores the critical importance of developing new, quantum-resistant encryption methods.

The researchers discovered a technique to calculate exponents using a series of Fibonacci numbers. This method only needs simple multiplication, which is reversible, instead of squaring. Importantly, it requires just two quantum memory units to calculate any exponent.

Breakthrough quantum algorithm can break advanced data encryption (interestingengineering.com)

# How to Protect yourself in post Quantum World per Cybersecurity and Infrastructure Security Agency (CISA) and National Security Agency (NSA)

## 1. Establish a Quantum-Readiness Roadmap

**Assess Current Cryptographic Systems**: Identify and document all cryptographic systems and assets currently in use.
**Engage with Technology Vendors**: Discuss their plans for post-quantum cryptography (PQC) and ensure they align with your organization's needs.
**Prioritize Migration Efforts**: Focus on the most sensitive and critical assets first.

## 2. Develop a Cryptographic Inventory

**Catalog Cryptographic Assets**: Create a detailed inventory of all cryptographic algorithms, keys, and certificates in use.
**Evaluate Vulnerabilities**: Assess which assets are most vulnerable to quantum attacks.

## 3. Integrate Quantum Risk into Governance Structures

**Update Risk Management Processes**: Incorporate quantum risks into your existing risk management framework.
**Establish Policies and Procedures**: Develop policies for the transition to PQC and ensure they are communicated across the organization.

## 4. Acquire Necessary Talent and Training

**Hire Experts**: Bring in experts in quantum computing and cryptography.
**Train Existing Staff**: Provide training on quantum risks and PQC to current employees.

## 5. Monitor and Update Regularly

**Stay Informed**: Keep up-to-date with the latest developments in quantum computing and PQC.
**Review and Adjust**: Regularly review and adjust your quantum readiness plan as needed.

Quantum-Readiness: Migration to Post-Quantum Cryptography (cisa.gov)

# Small and Medium Companies

Policies

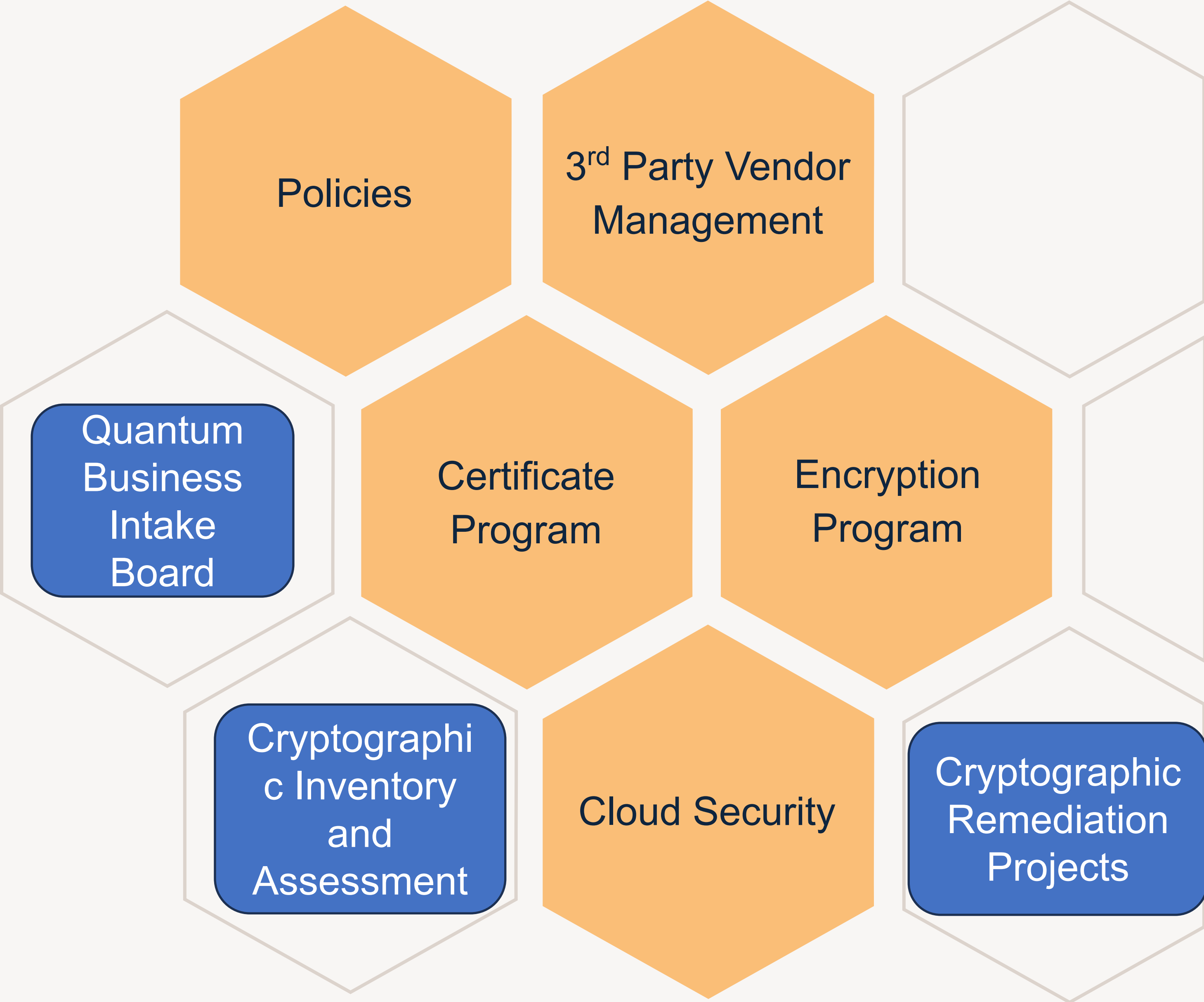
3rd Party Vendor Management

Certificate Program

Encryption Program

Cloud Security

# Large Companies



Policies

3rd Party Vendor Management

Quantum Business Intake Board

Certificate Program

Encryption Program

Cryptographic Inventory and Assessment

Cloud Security

Cryptographic Remediation Projects

# Summary

"Transitioning to post-quantum cryptography is a complex, multi-year process that requires careful planning to minimize disruption and ensure continued security," Soroko (SVP @ Sectigo) explains. "Early planning allows for a smoother transition when PQC standards become widely available."

# Thank you

- Yev Avidon, CISSP