"Alice, Bob, and the Quantum Quest: Embracing the Unknowns and Preparing for the Post-Quantum Crypto Future"

Marian Zaki, PhD

Assistant Professor of Computer Science and Cyber Engineering

Houston Christian University

About me ..

PhD in Computer Science
University of Pittsburgh

MS and BS in Computer Science
and Information Systems

Alice and Bob: A Cryptographic Love Tale

In a world of secrets, whispers, and code,
Where messages cross, encryption bestowed.
Alice and Bob, both cryptographers true,
Embark on a quest, their love shining through.

From the days of RSA, where primes reigned supreme,
To the lands of ECC, with elliptic curve dreams.
Their bond was secured in protocols tight,
Two hearts intertwined, in ciphers of light.

With classical schemes, they guarded their lore,
Shared secrets in whispers, on channels secure.
But whispers of quantum, a threat unforeseen,
Cast shadows of doubt on their digital sheen.

“Alice,” said Bob, with a cryptic refrain,
“The era is shifting; we must not remain.
Tied to the old, where quantum can spy,
Our keys from their chambers, our secrets shall die.”

Alice, with wisdom, a glint in her eye,
Nodded with grace, “It’s time to comply.
We’ll venture to realms where quantum’s advance,
Is met with new guards, where our love has a chance.”

They journeyed through lattices, post-quantum fields,
Explored every algorithm, each one they would wield.
From lattice to hash, they sought a new way,
To secure their love’s essence in cryptographic sway.

In hybrid solutions, they found a new song,
Combining the old and the new, both equally strong.
With crypto-agility, they shift and refine,
Finding new pathways where their hearts intertwine.

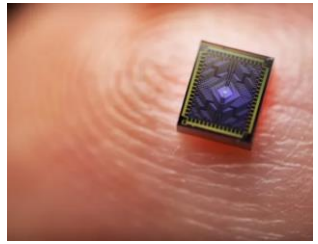
In post-quantum embrace, they whispered anew,
Secure in their bond, both timeless and true.
Quantum computing will bring no fear,
For their love is unbreakable, it’s crystal clear.

HOU·NET

Topics

01. State of Art
02. Moving from Fantastical to Feasible
03. Quantum Computing Global Landscape
04. The RoadMap: Quantum Preparedness Act
05. CISO’s Guide to Post-Quantum

THE CORPORATE GIANTS IN QUANTUM COMPUTING



Tunnel Falls, a 12-qubit silicon chip

DGX Quantum, the first-ever GPU-accelerated quantum computing system, integrating the NVIDIA Grace Hopper Superchip with Quantum Machines' OPX quantum control platform

The Quantum Artificial Intelligence Lab, an initiative collaboratively undertaken by Google, NASA, and the Universities Space Research Association.

. Cirq, a Python software library
. TensorFlow Quantum (TFQ) quantum machine library

. Q#
. Azure Quantum Copilot

Development Roadmap

IBM **Quantum**

	2016–2019 ✓	2020 ✓	2021 ✓	2022 ✓	2023 ✓	2024	2025	2026	2027	2028	2029	2033+
	Ran quantum circuits on the IBM Quantum Platform	Released multi-dimensional roadmap publicly with initial aim focused on scaling	Enhanced quantum execution speed by 100x with Qiskit Runtime	Brought dynamic circuits to unlock more computations	Enhanced quantum execution speed by 5x with Quantum Serverless and execution modes	Improve quantum circuit quality and speed to allow 5K gates with parametric circuits	Enhance quantum execution speed and parallelization with partitioning and quantum modularity	Improve quantum circuit quality to allow 7.5K gates	Improve quantum circuit quality to allow 10K gates	Improve quantum circuit quality to allow 15K gates	Improve quantum circuit quality to allow 100M gates	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 ✓	Heron (5K) ↻	Flamingo (5K)	Flamingo (7.5K)	Flamingo (10K)	Flamingo (15K)	Starling (100M)	Blue Jay (1B)
	Early ✓ Canary 5 qubits Albatross 16 qubits Penguin 20 qubits Prototype 53 qubits	Falcon ✓ Benchmarking 27 qubits		Eagle ✓ Benchmarking 127 qubits		Error mitigation 5k gates 133 qubits Classical modular 133x3 = 399 qubits	Error mitigation 5k gates 156 qubits Quantum modular 156x7 = 1092 qubits	Error mitigation 7.5k gates 156 qubits Quantum modular 156x7 = 1092 qubits	Error mitigation 10k gates 156 qubits Quantum modular 156x7 = 1092 qubits	Error mitigation 15k gates 156 qubits Quantum modular 156x7 = 1092 qubits	Error correction 100M gates 200 qubits Error corrected modularity	Error correction 1B gates 2000 qubits Error corrected modularity

Innovation Roadmap

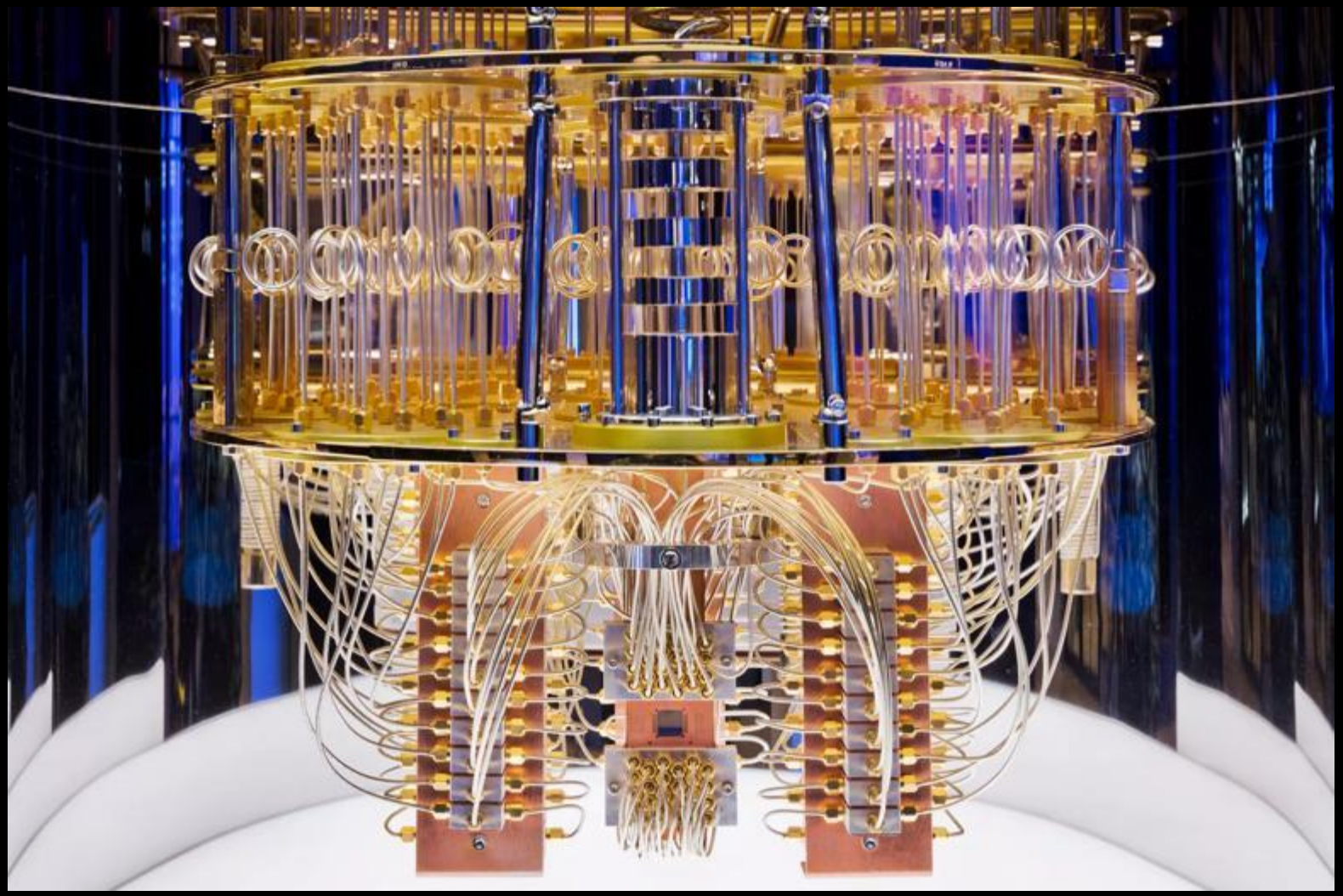
Software innovation	IBM Quantum Experience ✓	Qiskit ✓ Circuit and operator API with compilation to multiple targets	Application modules ✓ Modules for domain specific application and algorithm workflows	Qiskit Runtime ✓ Performance and abstraction through primitives	Quantum Serverless ✓ Demonstrate concepts of quantum-centric supercomputing	AI-enhanced quantum ✓ Prototype demonstrations of AI-enhanced circuit transpilation	Resource management ↻ System partitioning to enable parallel execution	Scalable circuit knitting Circuit partitioning with classical reconstruction at HPC scale	Error correction decoder Demonstration of a quantum system with real-time error correction decoder			
Hardware innovation	Early ✓ Canary 5 qubits Penguin 20 qubits Albatross 16 qubits Prototype 53 qubits	Falcon ✓ Demonstrate scaling with I/O routing with bump bonds	Hummingbird ✓ Demonstrate scaling with multiplexing readout	Eagle ✓ Demonstrate scaling with MLW and TSV	Osprey ✓ Enabling scaling with high density signal delivery	Condor ✓ Single system scaling and fridge capacity	Flamingo ↻ Demonstrate scaling with modular connectors	Kookaburra Demonstrate scaling with nonlocal c-coupler Demonstrate path to improved quality with logical memory		Cockatoo Demonstrate path to improved quality with logical communication	Starling Demonstrate path to improved quality with logical gates	
						Heron ✓ Architecture based on tunable-couplers	Crossbill ↻ Demonstrate m-couplers					

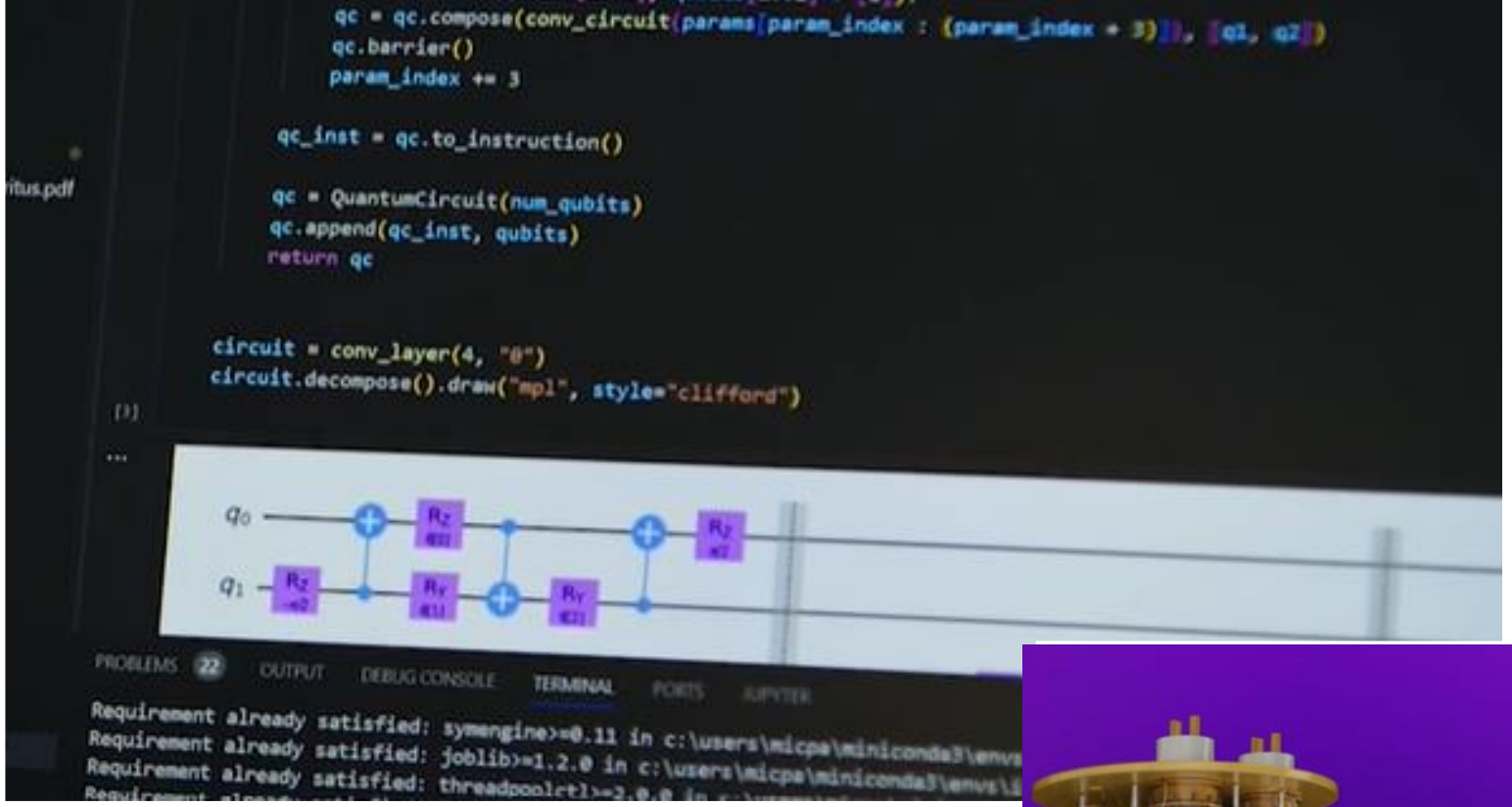
✓ Executed by IBM

↻ On target

IBM Quantum System Two, the world’s first modular utility-scale quantum computer system.

One at Cleveland Clinic (Courtesy: Cleveland Clinic)

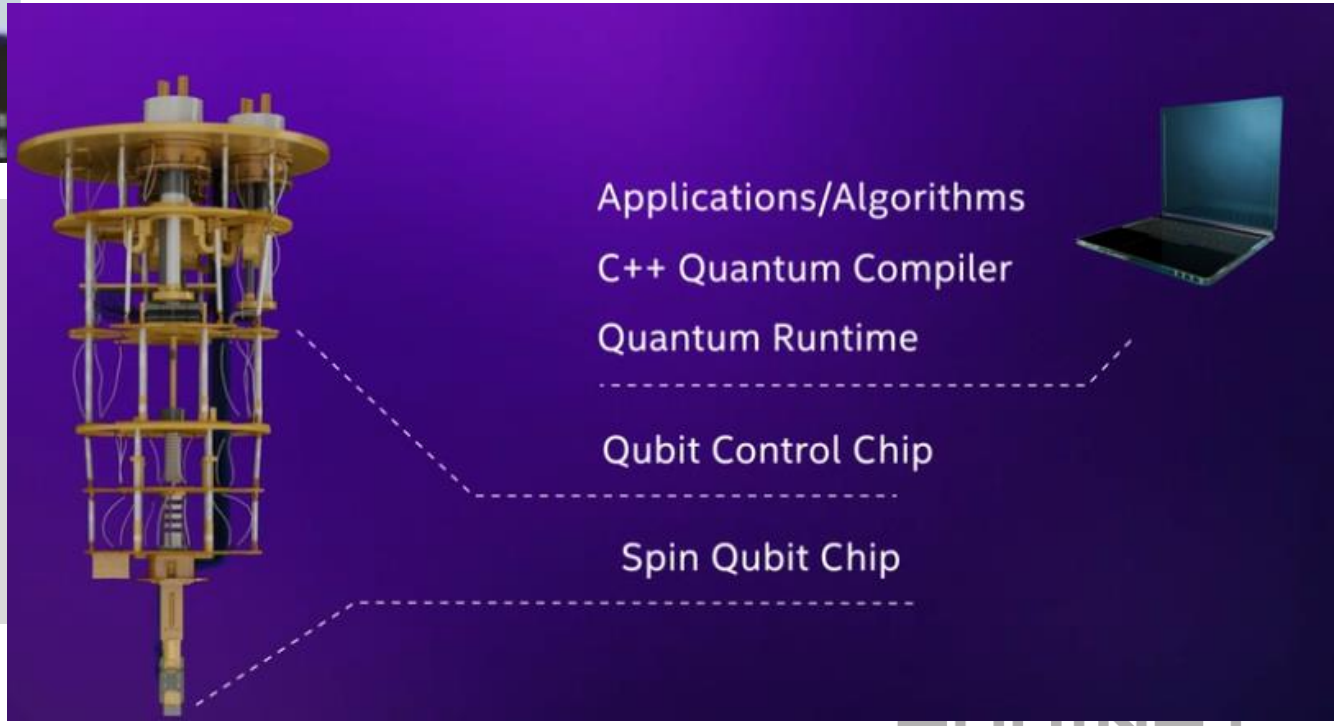




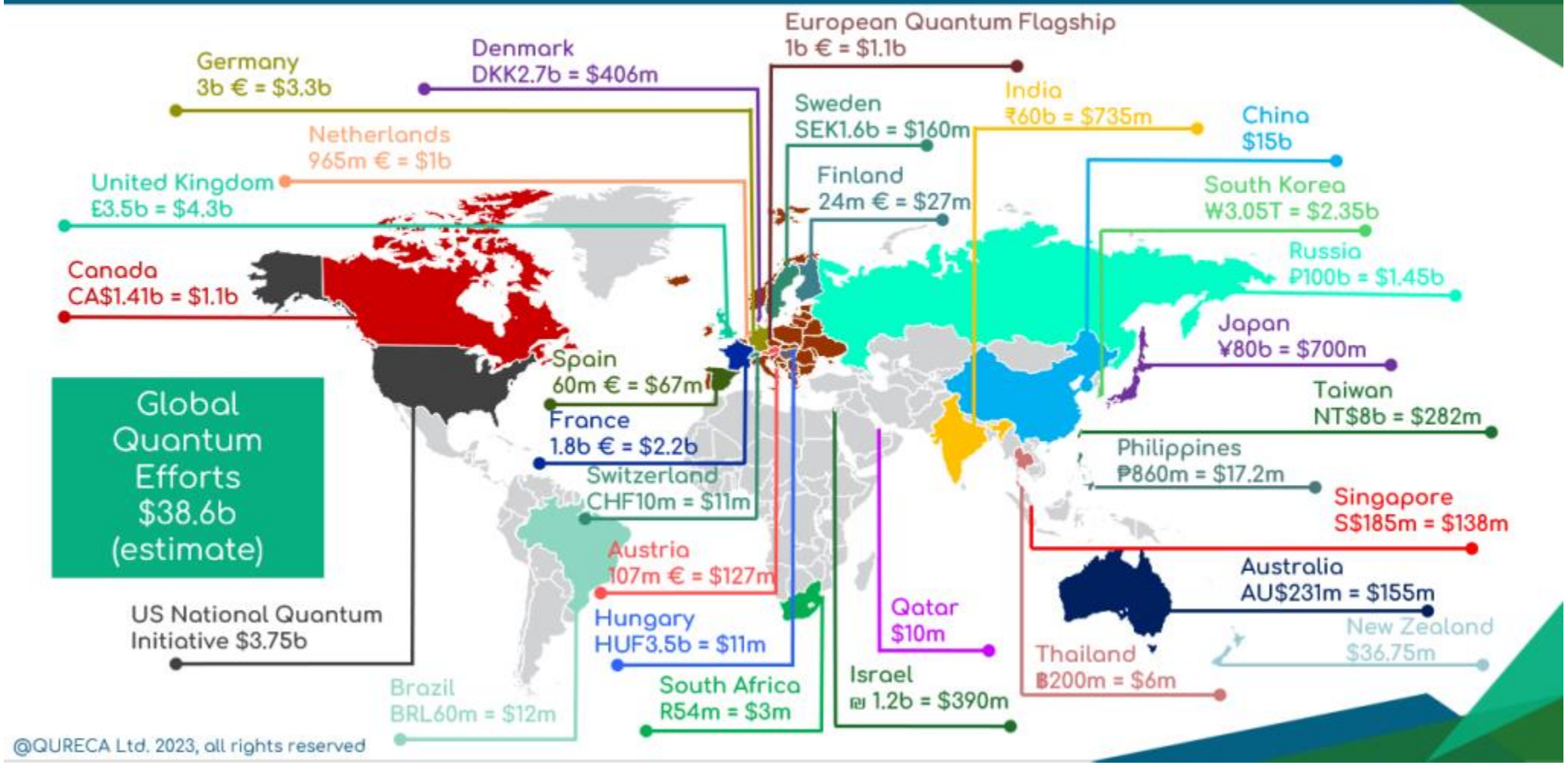
IBM Qiskit SDK v1.1

First Quantum SDK that interfaces with Python

- 550k Users
- 8K+ Open Source Contributors
- Over 3 trillion circuits run



Quantum effort worldwide



HOU·NET

Is History Repeating Itself?

- The 1998 DES $250K cracker changed the security posture of every single organization globally

- With modern cryptography, a security breach is never because someone broke the encryption, it's usually because EVERYTHING else can go wrong including key management.

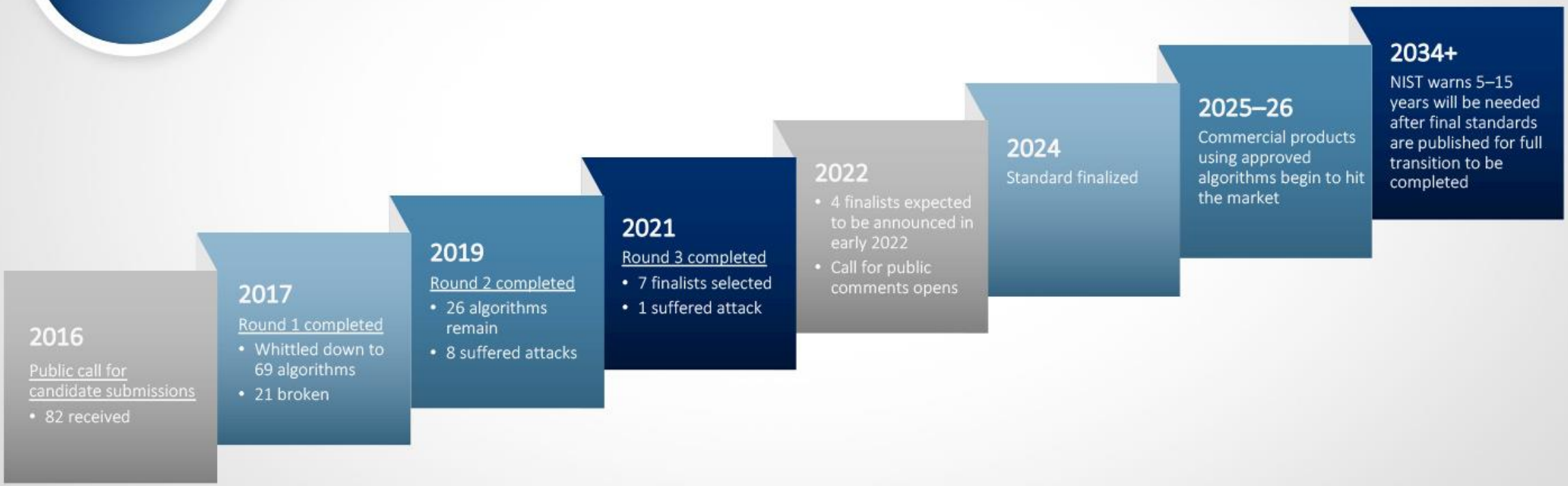
- This might not be the case anymore with **Cryptographically Relevant Quantum Computers** (QRQCs).

Shor's algorithm is the first quantum algorithm. It is expected that Shor's algorithm will be able to factor the large prime numbers of RSA - soon!!

Grover's search algorithm can expedite brute force attacks on symmetric keys – not quiet there yet!

HOU·NET

PQC Reaches an Inflection Point



HOU·NET

NEWS

NIST Releases First 3 Finalized Post-Quantum Encryption Standards

August 13, 2024

"These finalized standards include instructions for incorporating them into products and encryption systems," said NIST mathematician Dustin Moody, who heads the PQC standardization project. "We encourage system administrators to start integrating them into their systems immediately, because full integration will take time."

Moody said that these standards are the primary tools for general encryption and protecting digital signatures.

"There is no need to wait for future standards," he said. "Go ahead and start using these three. We need to be prepared in case of an attack that defeats the algorithms in these three standards, and we will continue working on backup plans to keep our data safe. But for most applications, these new standards are the main event."

NATIONAL ARCHIVES

FEDERAL REGISTER

The Daily Journal of the United States Government

Announcing Issuance of Federal Information Processing Standards (FIPS) FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard, FIPS 204, Module-Lattice-Based Digital Signature Standard, and FIPS 205, Stateless Hash-Based Digital Signature Standard

A Notice by the National Institute of Standards and Technology on 08/14/2024

HOU·NET

The Roadmap
Quantum Computing Preparedness Act

July 2024, Public Law No: 117-260

1. Create a comprehensive and ongoing cryptographic inventory to identify the quantum risk surface

Map out where the public-key cryptography exists

["M-23-02"] A strategy for organizations to evolve automated inventory capabilities

IBM Quantum Safe Explorer scans source code to identify and inventory cryptography usage creating a Cryptography Bill of Materials (CBOM)

The need for annual manual inventory is still there

Sustained investment in this process is critical to the successful migration to PQC

HOU·NET

The Roadmap
Quantum Computing Preparedness Act

July 2024, Public Law No: 117-260

2. ***Record-now-decrypt-later*** attacks mean migration must start before CRQCs are known to be operational

Conduct regular audits to assess the sensitivity and security of transmitted/stored data

NIST

Start integrating PQCs in your systems following the NISTs recommendations

Crypto-Agility is a key here

- ML-KEM — a Key Establishment algorithm (NIST FIPS 203)
- ML-DSA — a lattice-based Digital Signature Algorithm (NIST FIPS 204)
- SLH-DSA — a stateless hash-based Digital Signature Algorithm (NIST FIPS 205)

HOU·NET

What is Crypto-Agility?

Cryptographic Agility refers to the ability of systems, platforms, applications or organizations to rapidly adapt its cryptographic mechanisms and algorithms in response to changing threats without the need to rewrite application or deploy new hardware systems

1- Crypto-agility requires modularity and abstraction

2- Crypto-agility requires automation

3- Crypto-agility requires governance

HOU·NET

The Roadmap
Quantum Computing Preparedness Act

July 2024, Public Law No: 117-260

3. Prioritize systems and data for PQC migration

The Dilemma: Can't do it all at once, yet we need to have interoperability

High impact information systems

High value assets

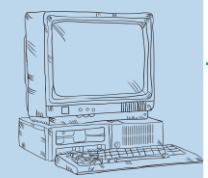
Data expected to remain mission-sensitive in 2035

Any access control based on asymmetric encryption

HOU·NET

The Roadmap
Quantum Computing Preparedness Act

July 2024, Public Law No: 117-260

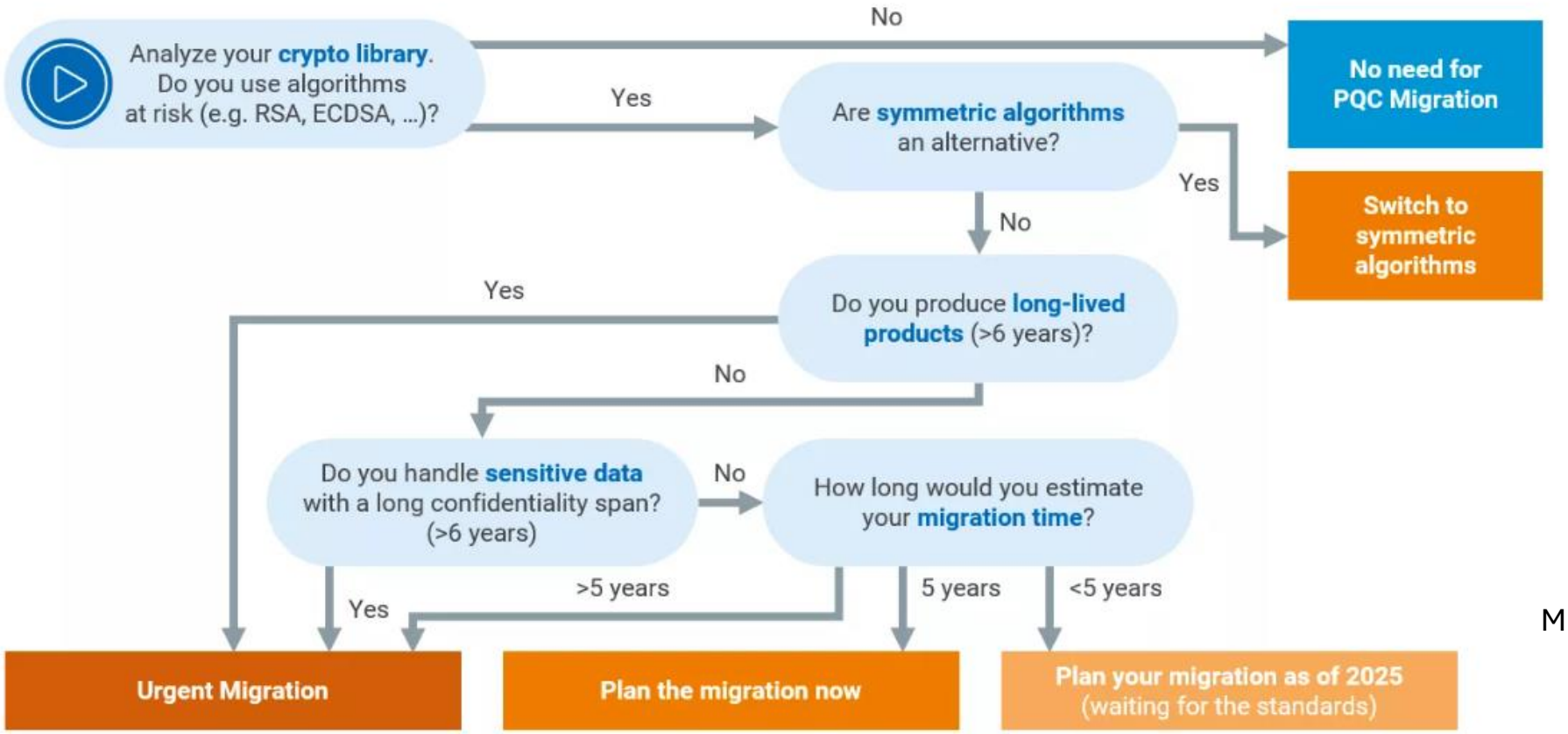


4. Identify the systems that will not be able to support PQC algorithms

Why would these systems even exist?

Incorporate the modernization and digital transformation timelines into the PQC migration plans

A PQC Migration Strategy: Urgent vs. Regular Adopters



by Utimaco: Ensuring Resilience post quantum cryptography

Migration is time-consuming

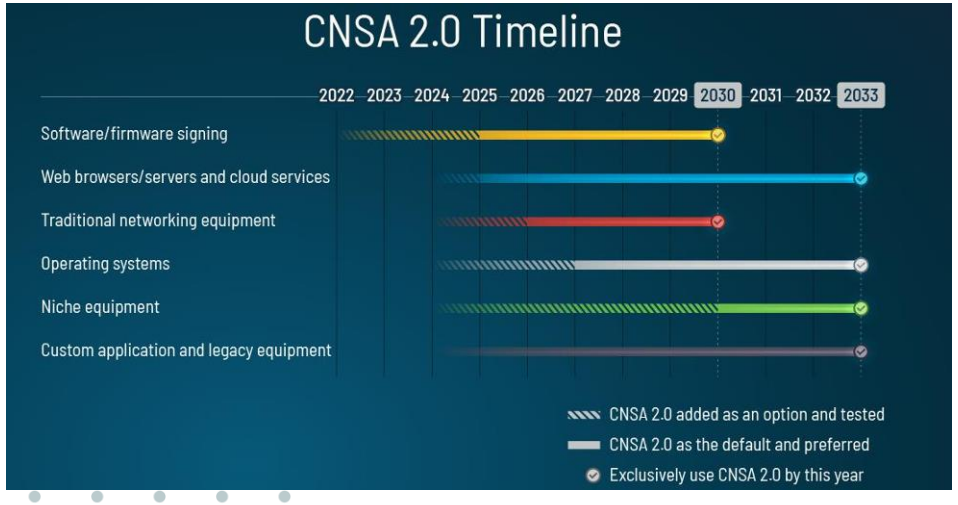
HOU·NET

What's happening in the scenes now?

working on updating the widely-used security protocols (TLS and IPSec) to be resistant against a quantum computer

Published next steps preparation white paper

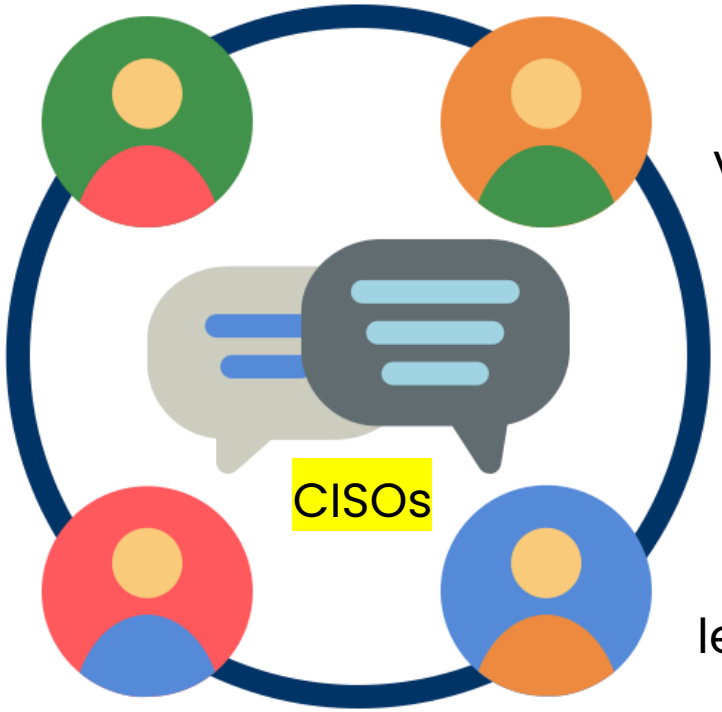
Guidelines to the adoption of PQC/T hybrid schemes for key establishment (TLS 1.3 and IKE RFC 9370) and PKI



Start the conversations .. Don’t wait!

Now is the perfect time to build your Crypto-Agility

Start communicating with your developers, IT/OT support teams, security architects to define the organizational needs for cyber-agility, crypto inventory and migration plans



Start communicating with technology procurement specialists to identify hw/sw vendors plans for supporting PQC in their products

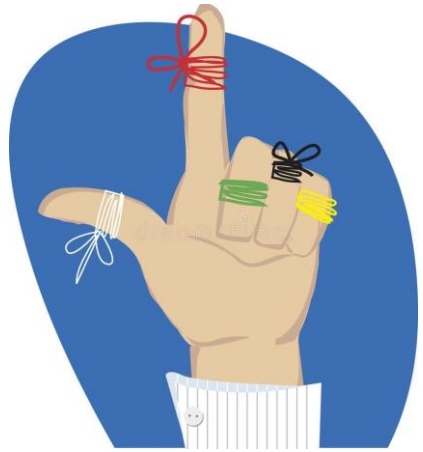
Start communicating with CEOs and CFOs on the financial plans for updating the enterprise systems

Start communicating with legal and compliance teams

HOU·NET

Key Takeaway points for today

- The global state of Quantum Computing is accelerating with capital investments in research and production
- Most PKC algorithms in use today will be vulnerable to a CRQC. The best mitigation against the threat of quantum computers to traditional PKC is PQC.
- The security of symmetric cryptography is not significantly impacted by quantum computers, and existing symmetric algorithms with appropriate key sizes can continue to be used.
- Migration to PQC is a long and tedious process – start assets identification, data sensitivity analysis, and build your crypto agility plan to migrate to hybrid and/or PQC
- If relying on a PQC/T hybrid scheme, it's recommended to be used as an interim measure. A flexible framework should allow for complete migration to PQC.
- Follow Standards Bodies – Monitor and engage with NIST, CISA ..etc.



HOU·NET

THANK YOU

Questions?

Marian Zaki

Ph.D. Assistant Professor | Computer Science | CyberSecurity | External Partnerships Coordinator fo...