Eric Heflin
Heflin Consultancy LLC

HL7® FHIR® Security

Education Event

Quantum Computing and Healthcare Cybersecurity: A Pragmatic Perspective

HL7 International | ASTP Assistant Secretary for Technology Policy | ONC Office of the National Coordinator for Health Information Technology

® Health Level Seven and HL7 are registered trademarks of Health Level Seven International, registered with the United States Patent and Trademark Office.

Quantum Computing and Cybersecurity

- Definition and Context
- New Algorithmic Attacks
- Three Tracks
- Risks
- Defenses
- Opportunities
- Suggested Approach
- Further Reading

HL7® International

ASTP Assistant Secretary for Technology Policy

ONC Office of the National Coordinator for Health Information Technology

® Health Level Seven and HL7 are registered trademarks of Health Level Seven International, registered with the United States Patent and Trademark Office.

Copyright© Eric Heflin

Quantum Computers

- Require exotic cooling (-450 degrees F)
- High vacuum
- Electromagnetic shielding
- Requires special instruction language
- Reason for these measures: Noise reduction
- Disclosure: I'm a former IBM consultant

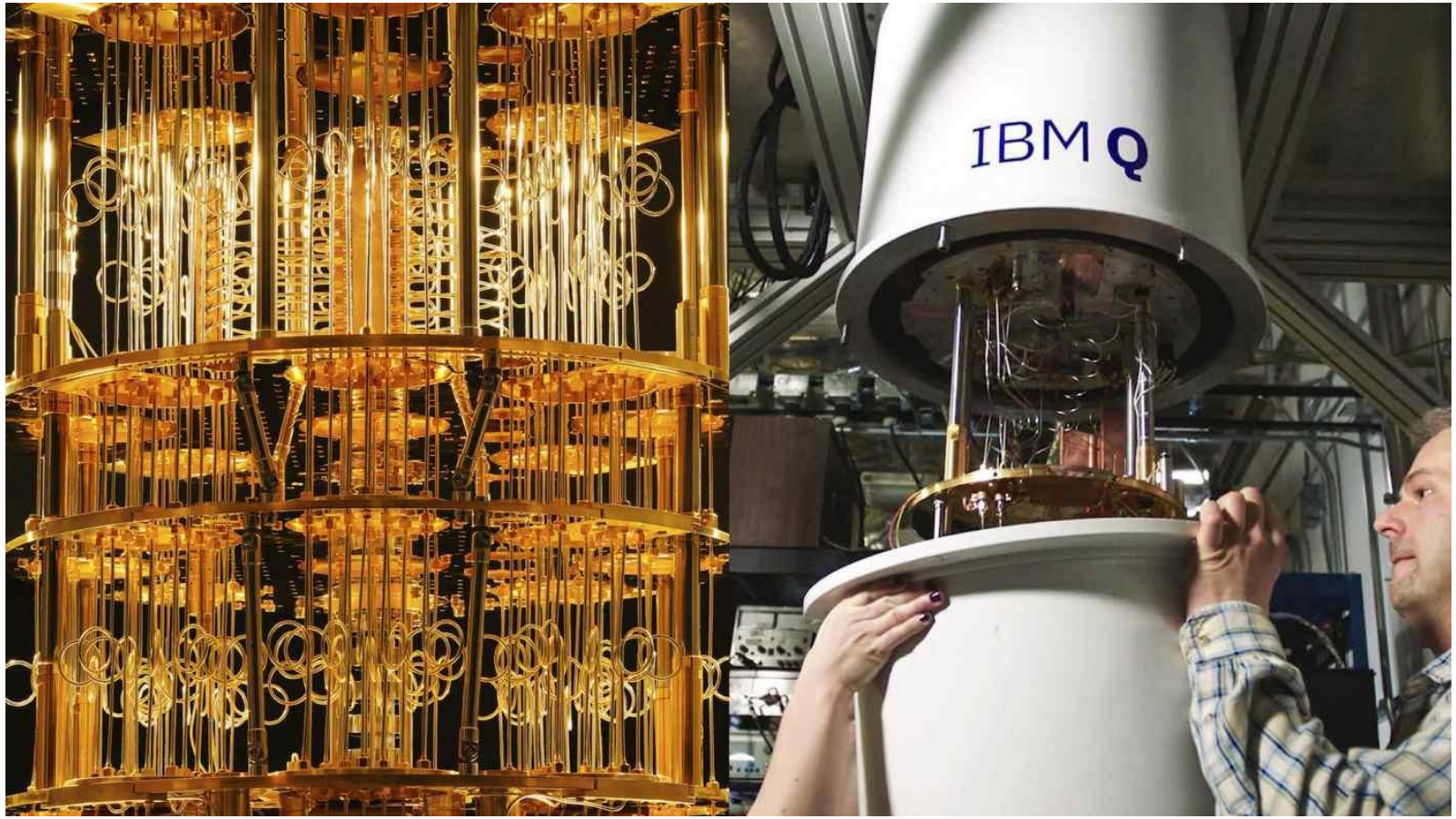
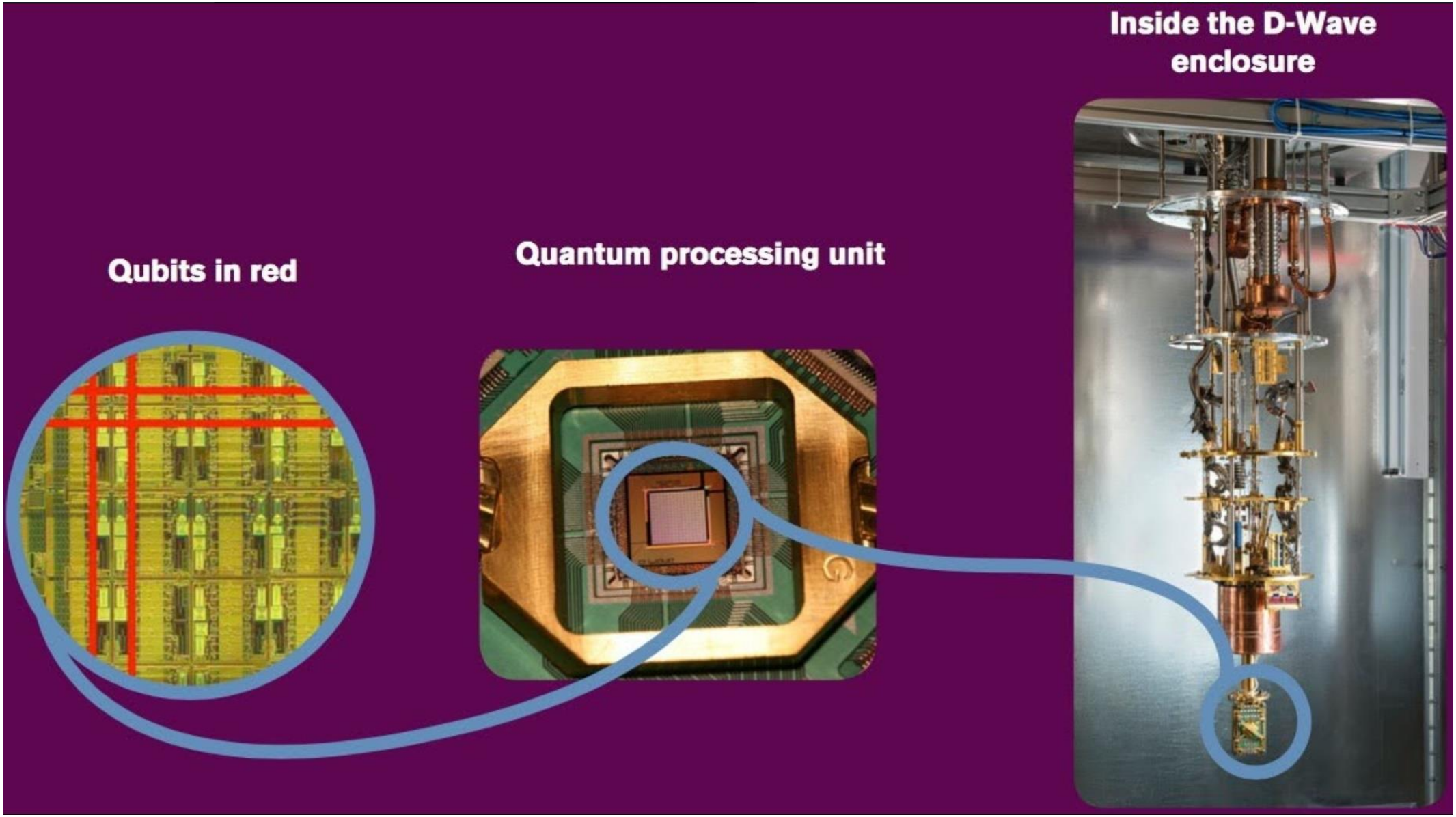


Image credit: IBM.com

Copyright© Eric Heflin


Inside the D-Wave enclosure
Qubits in red
Quantum processing unit

“Classic” Public Key Security Mechanisms

Why is Public Key Infrastructure (PKI) Secure …

(Currently)?

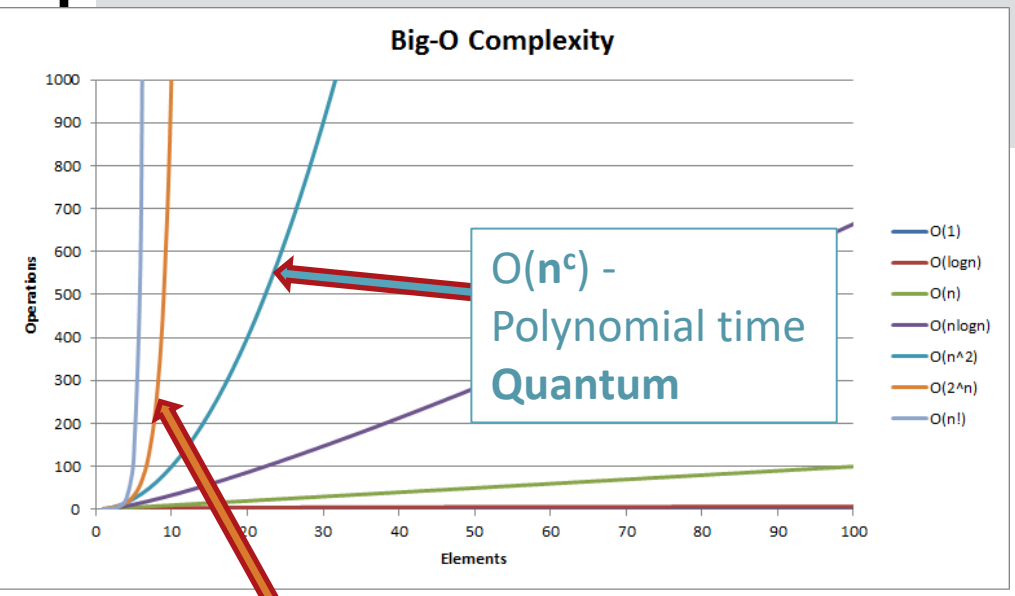
PKI depends on mathematically linked public and private keys

RSA’s security depends on difficulty of factorization of the private key

ECC’s security depends on discrete logarithm problem solving of the private key

Copyright© Eric Heflin

Quantum Computing



n = size of input, c = some constant

Example: n = 1,000 c = 4
Classic effort: 4^1,000 = 1 followed by 602 zeros!
Quantum: 1,000^4 = 1 followed by 12 zeros!

- Uses quantum mechanics to process data
- Classical computing uses bits of 0 or 1
- In quantum computing, information is stored in quantum bits, or qubits, which can exist in a superposition of both 0 and 1 at the same time
- Qubits allows quantum computers to be exponentially faster for some operations
  - Can factor large numbers in polynomial time
  - Classical computers do so in exponential time
- Quantum computing is still in its early stages
  - Not stable; noise is a significant issue
  - Small number of qbits
  - Algorithms are still actively being researched

HL7 International | ASTP Assistant Secretary for Technology Policy | ONC Office of the National Coordinator for Health Information Technology

Image credit: https://i.stack.imgur.com/ia6VB.png

Copyright© Eric Heflin

Video: https://youtu.be/OWJCfOvochA?t=206

® Health Level Seven and HL7 are registered trademarks of Health Level Seven International, registered with the United States Patent and Trademark Office.

Rapid Advances

Google… announced [in 2020] … they had assembled a machine that performed a test calculation in 200 seconds, that would have taken conventional supercomputers thousands of years to accomplish.

…commercial quantum computers… cost … $10 million [for] 50 qubits.

SpinQ machine [is $5,000] for 2 qubits

Image credit: https://swarajyamag.com/tech/honey-ive-shrunk-the-quantum-computer-worlds-first-portable-desktop-sized-quantum-machines-announced
https://www.discovermagazine.com/technology/a-desktop-quantum-computer-for-just-usd5-000

TECH

Honey, I've Shrunk The Quantum Computer! World's First Portable, Desktop-Sized Quantum Machines Announced

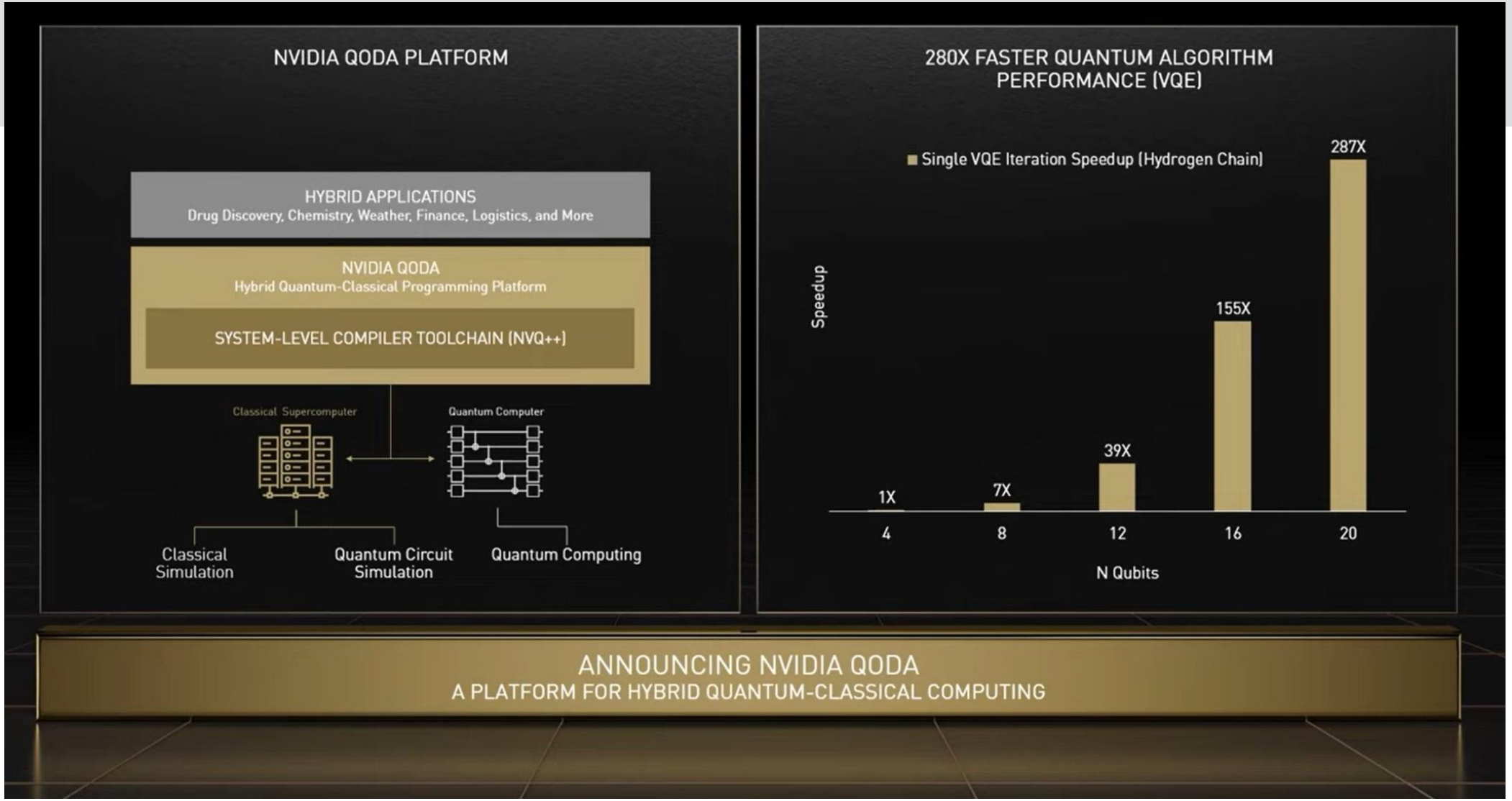
by *Anand Parthasarathy* -
Dec 21, 2022 05:01 PM +05:30 IST

A vision of the future: A classroom equipped with a quantum computer for every student, just as today's smart classrooms have laptops

Snapshot

- *In a pathbreaking development, a dramatic lurch towards affordable quantum computing platforms has occurred.*
- *Three portable quantum computing platforms have been put on sale online by China based SpinQ Technology and Japan's Switch Science.*

Copyright© Eric Heflin



Copyright© Eric Heflin

- Definition and Context
- New Algorithmic Attacks
- Three Tracks
- Risks
- Defenses
- Opportunities
- Suggested Approach
- Further Reading

HL7® International

ASTP Assistant Secretary for Technology Policy

ONC Office of the National Coordinator for Health Information Technology

® Health Level Seven and HL7 are registered trademarks of Health Level Seven International, registered with the United States Patent and Trademark Office.

Copyright© Eric Heflin

Quantum-Based Attacks

- Enables New Algorithmic Attacks:
- Factorization
- Brute Force

- Quantum algorithms leverage the new physics allowing multiple simultaneous states to exist; can allow for high degree of parallel problem solving
- Shor's Algorithm (Peter Shor, MIT)
  - Solves cryptographic factorization much faster (polynomial time)
- Grover's Algorithm (Lov Grover, Cornell University)
  - Database queries
  - Brute force attacks

® Health Level Seven and HL7 are registered trademarks of Health Level Seven International, registered with the United States Patent and Trademark Office.
Copyright© Eric Heflin

Known Quantum Computing Vulnerable Algorithims

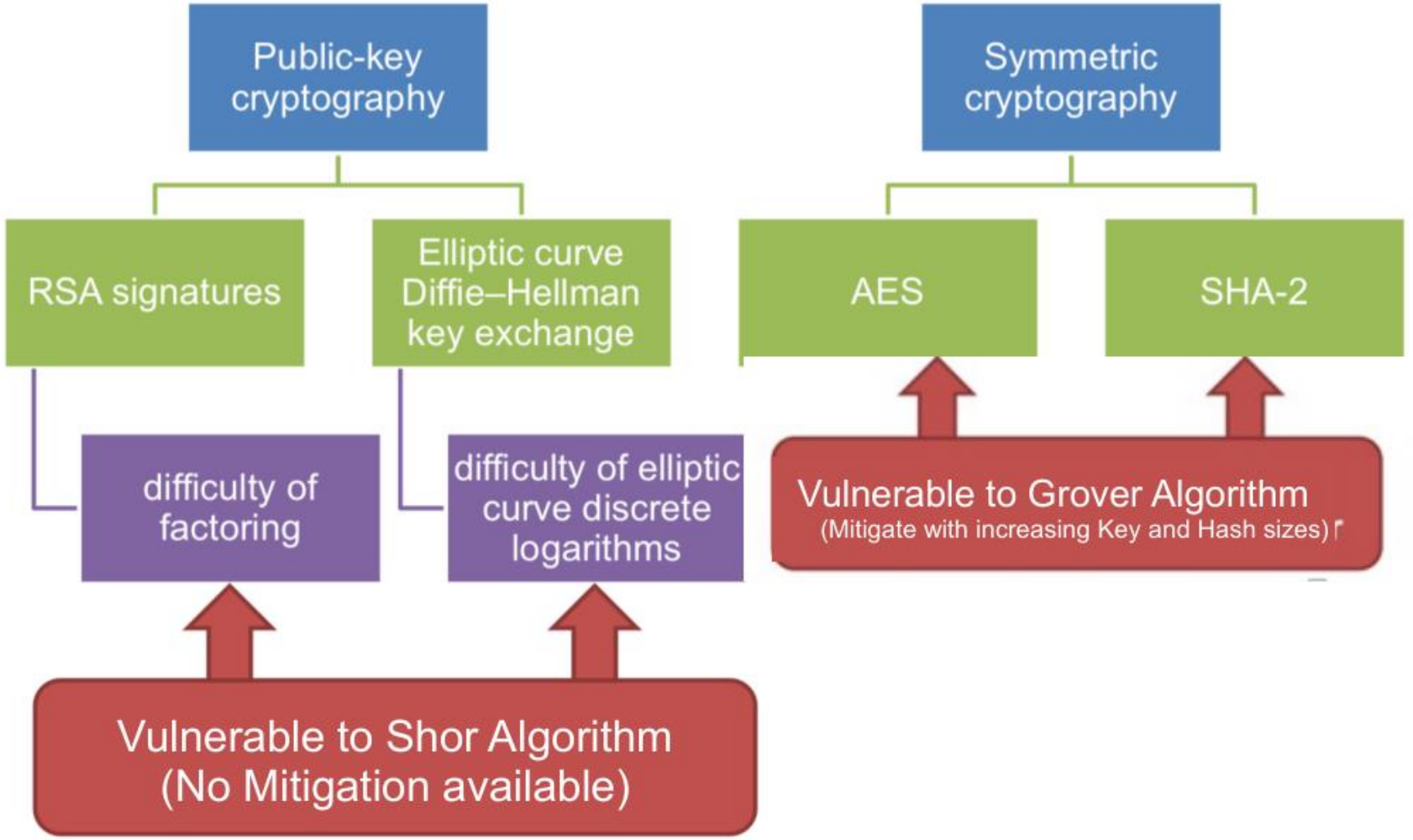


Image and text credit: Ramesh Nagapan, Harvard University

HL7 International | ASTP Assistant Secretary for Technology Policy | ONC Office of the National Coordinator for Health Information Technology
® Health Level Seven and HL7 are registered trademarks of Health Level Seven International, registered with the United States Patent and Trademark Office.
Copyright© Eric Heflin

Quantum Computing: New Risks to PKI, Symmetric, Hashing

Classic asymmetric key cryptosystems are vulnerable to Quantum computers running Shore's Algorithm

- RSA, ECC, etc. can likely be broken
- One attack is called "store-now decrypt later"
- Larger key sizes are not a viable defense against quantum computing

Classic symmetric key cryptosystems are likely vulnerable to Grover's Algorithm

- Allows much faster brute force searching (square root smaller effort) for inputs that match a given hash value
- Using larger key sizes is anticipated to be a viable mitigation

Copyright© Eric Heflin

Comparison of Traditional v Quantum Security

- Effective Key Strength in a Quantum Computing Environment

Algorithm	Key Length	Effective Strength	
		Traditional	Quantum Computing
RSA 1024	1024 bits	80 bits	0 bits
RSA 2048	2048 bits	112 bits	0 bits
ECC-256	256 bits	128 bits	0 bits
ECC-384	384 bits	256 bits	0 bits
AES-128	128 bits	128 bits	64 bits
AES-256	256 bits	256 bits	128 bits

Image and text credit: Ramesh Nagapan, Harvard University

HL7 International | ASTP Assistant Secretary for Technology Policy | ONC Office of the National Coordinator for Health Information Technology
® Health Level Seven and HL7 are registered trademarks of Health Level Seven International, registered with the United States Patent and Trademark Office. Copyright© Eric Heflin

- Definition and Context
- New Algorithmic Attacks
- Three Tracks
- Risks
- Defenses
- Opportunities
- Suggested Approach
- Further Reading

HL7® International

ASTP Assistant Secretary for Technology Policy

ONC Office of the National Coordinator for Health Information Technology

® Health Level Seven and HL7 are registered trademarks of Health Level Seven International, registered with the United States Patent and Trademark Office.

Copyright© Eric Heflin

Three Tracks

1. Classic Quantum Computing
2. Noise-Tolerant Quantum Computing
3. Breakthroughs

Copyright© Eric Heflin

Image: Licensed from iStockPhoto

® Health Level Seven and HL7 are registered trademarks of Health Level Seven International, registered with the United States Patent and Trademark Office.

Track 1: Traditional (Noiseless) Quantum Computing

- At this time, from the perspective of traditional noiseless quantum attacks against PKI purely theoretical.
- Current biggest challenge: Building a large computer that's noise-free and remains coherent.
- Most progress reports assume use of noise-free quantum computers
- As of the IBM roadmap, they currently have released a 433 qbit chip and are targeting 5,000 qubits by the end of 2024.
- According to Bruce Schneier it would take approximately 1,000,000 qbits to crack the ECC used for Bitcoin

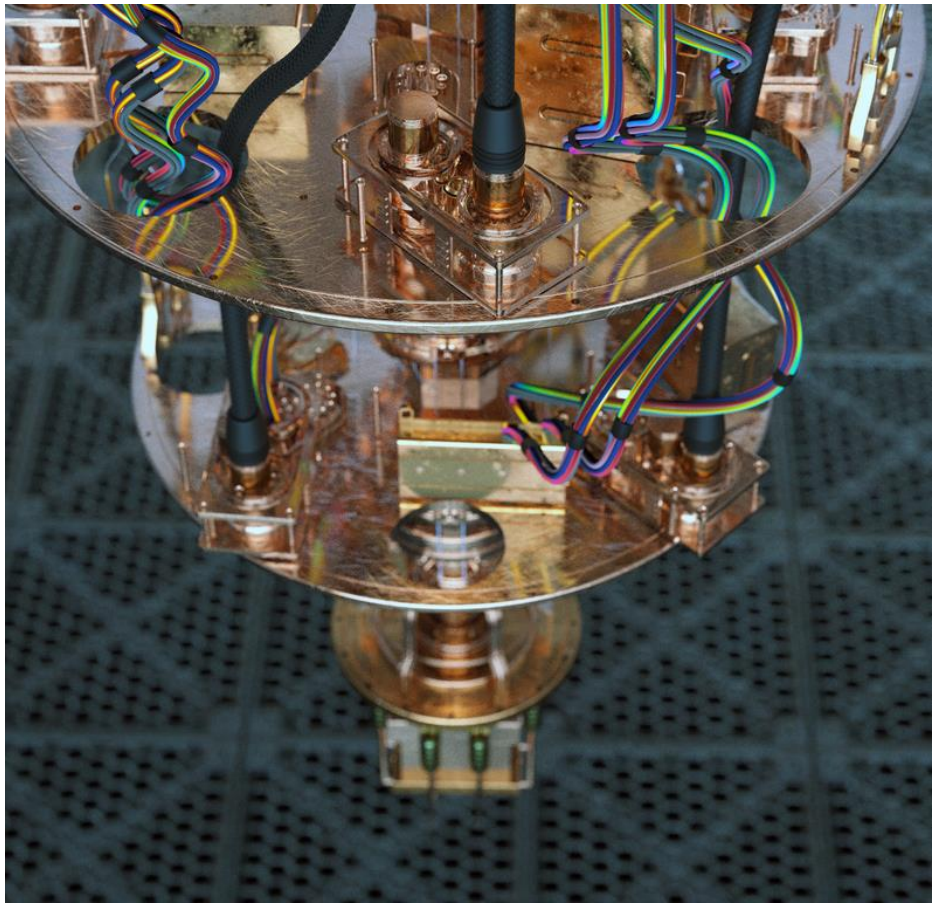


Image: Licensed from iStockPhoto

Source: https://www.ibm.com/roadmaps/quantum/

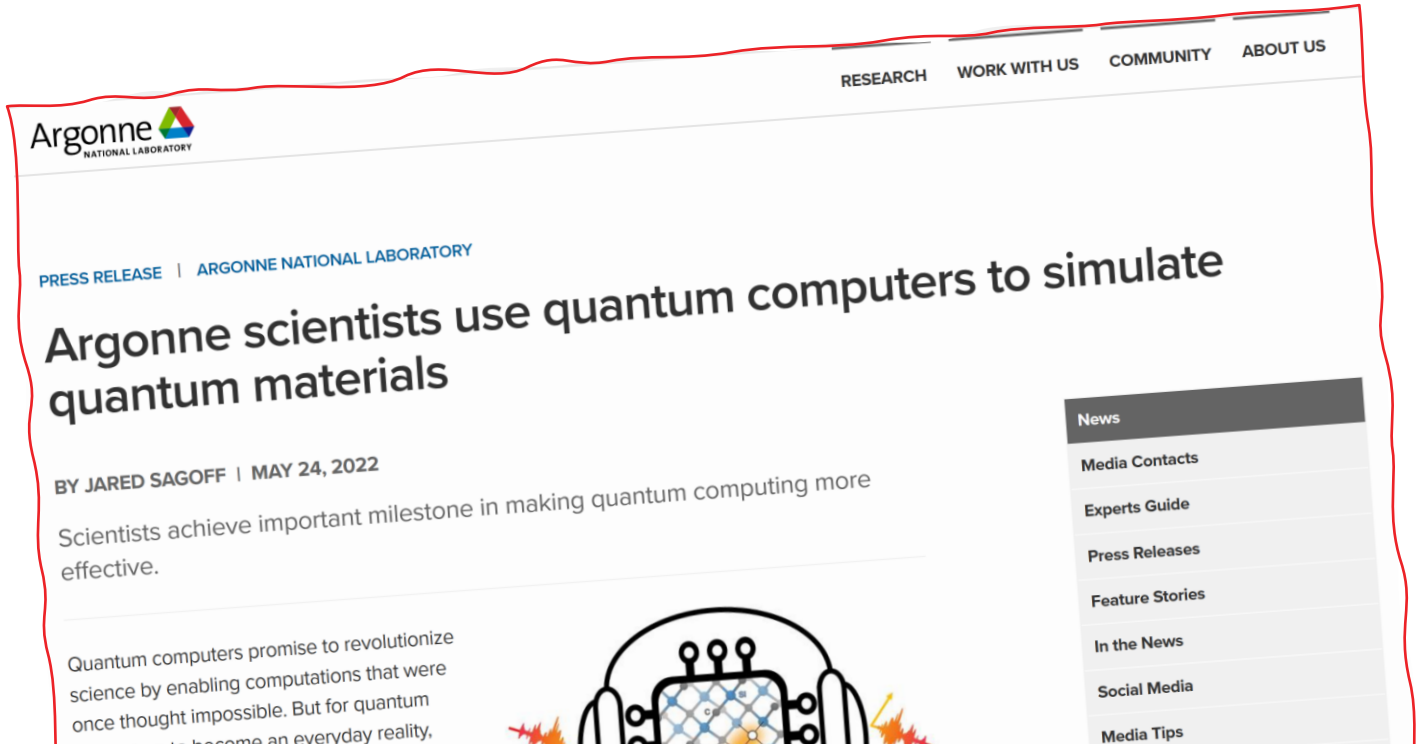
Copyright© Eric Heflin

Track 2: Noise-Tolerant Quantum Computing

- HOWEVER: In May 2022 Argonne National Lab simulated correction and use of a noisy quantum computer using Quantum Defect Embedding Theory (QDET). This, if practical, may indicate we are much closer to practical PKI attacks.

"The study improved the accuracy of calculations on quantum computers by correcting for noise introduced by quantum hardware."

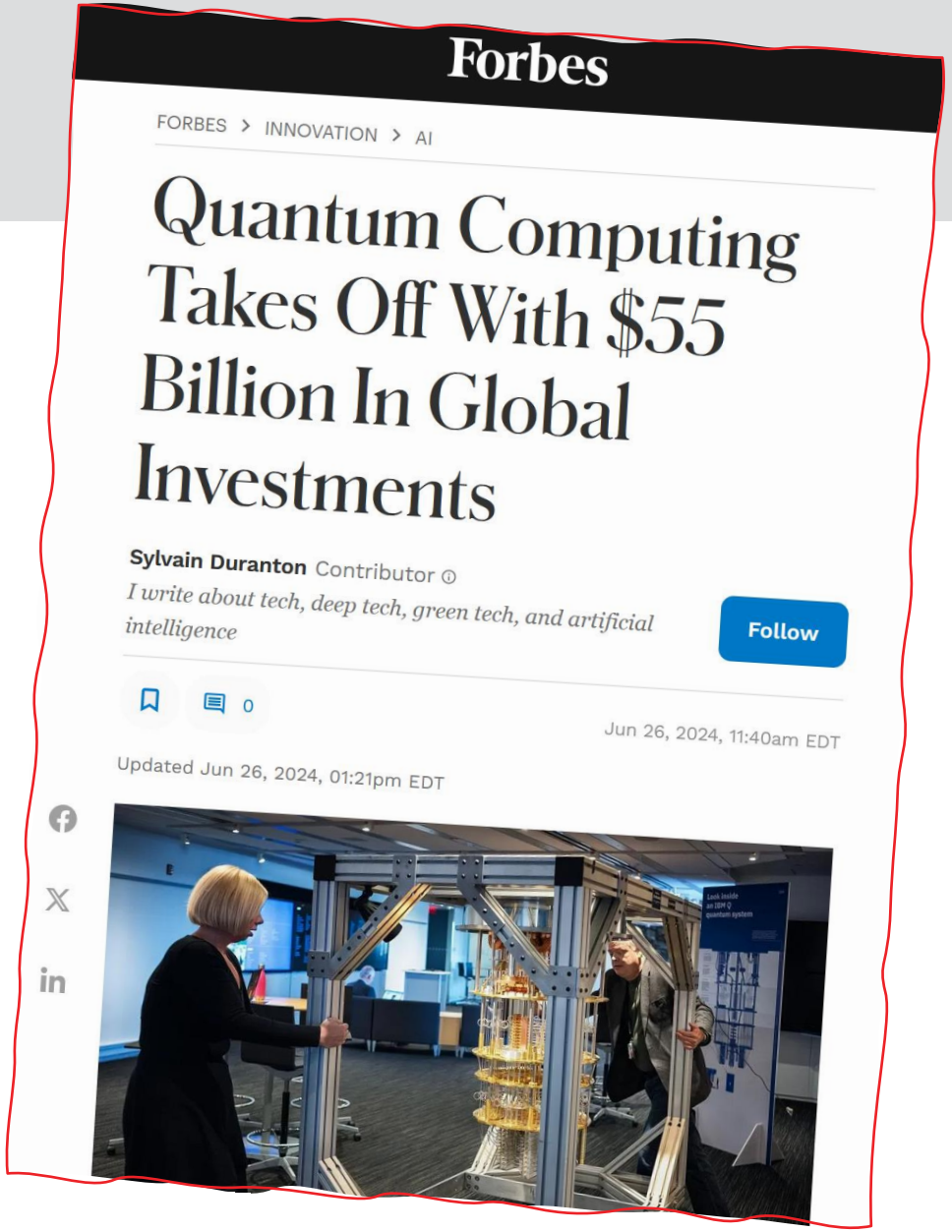
https://www.anl.gov/article/argonne-scientists-use-quantum-computers-to-simulate-quantum-materials



Copyright© Eric Heflin

Track 3: Breakthroughs

- Unpredictable breakthroughs
- Example: Argon National Labs breakthrough work on noise-tolerant quantum computing
- Global investment in quantum computing is estimated to have been $55 billion in 2023



Forbes

FORBES > INNOVATION > AI

Quantum Computing Takes Off With $55 Billion In Global Investments

Sylvain Duranton Contributor

I write about tech, deep tech, green tech, and artificial intelligence

Follow

0

Jun 26, 2024, 11:40am EDT

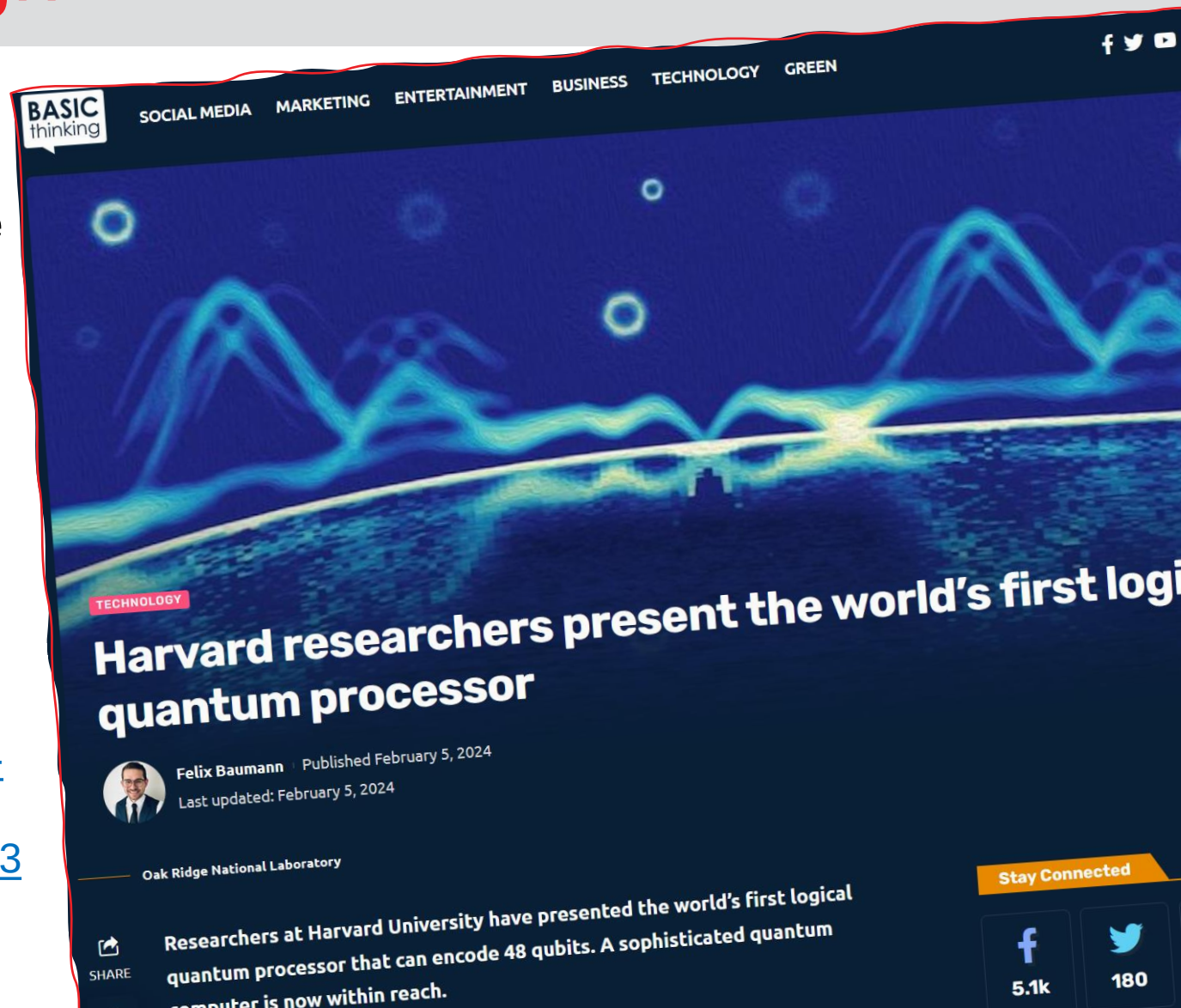
Updated Jun 26, 2024, 01:21pm EDT

https://www.forbes.com/sites/sylvainduranton/2024/06/26/quantum-now/

Copyright© Eric Heflin

Track 3: First Working Logical Quantum Processor Breakthrough

- Supports 48 qbits
- … a potential turning point in the development of quantum processors.
- It demonstrates the first large-scale execution of algorithms on an error-corrected quantum computer.



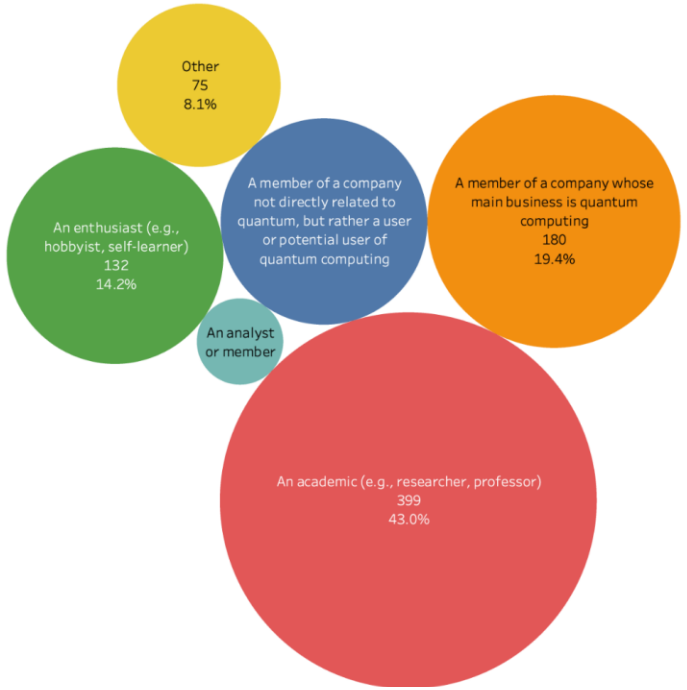
Sources:

- https://www.basicthinking.com/harvard-researchers-present-the-worlds-first-logical-quantum-processor/
- https://www.nature.com/articles/s41586-023-06927-3

HL7 International | ASTP Assistant Secretary for Technology Policy | ONC Office of the National Coordinator for Health Information Technology

Copyright© Eric Heflin

The pace of development relative to expectations



- Academics: 43.0%
- Quantum Computing Companies: 19.4%
- Non-Quantum Companies: 13.0%
- Analysts/Press: 2.3%
- Enthusiasts: 14.2%
- Others: 8.1% (e.g., researchers in non-profits, consultants, students)

July 2024 Survey of 927 Quantum Professionals

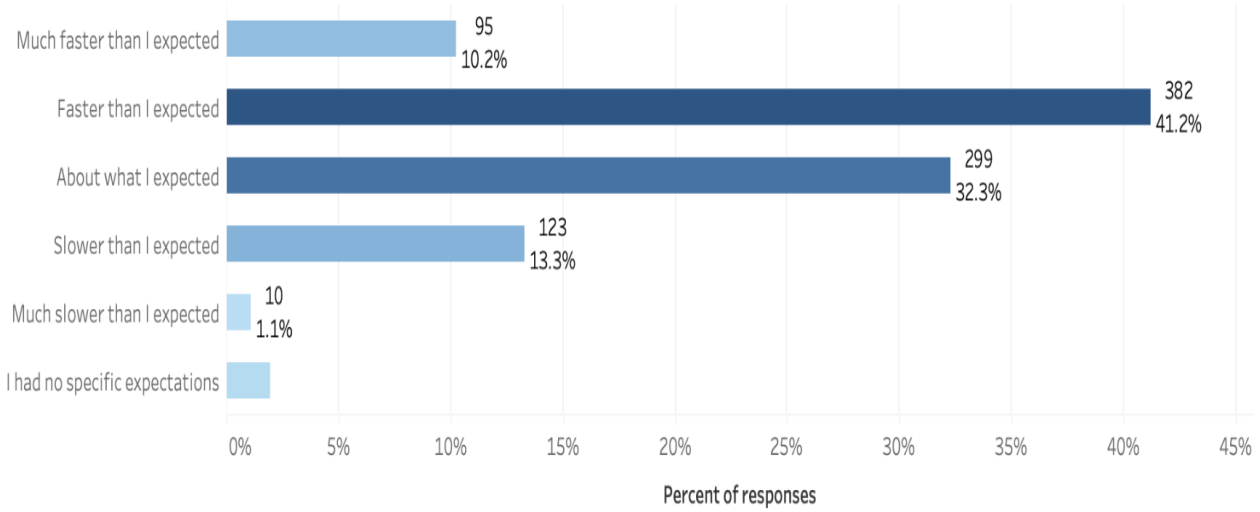


Figure 9 - How does the pace of development compare to your expectations from a few years ago?

Source: https://www.quera.com/blog-posts/current-and-future-state-of-quantum-computing

® Health Level Seven and HL7 are registered trademarks of Health Level Seven International, registered with the United States Patent and Trademark Office. Copyright© Eric Heflin

When would Quantum be Superior to Classical Computing?

We asked "When do you expect quantum to be a superior alternative to classical computing for certain workloads?":

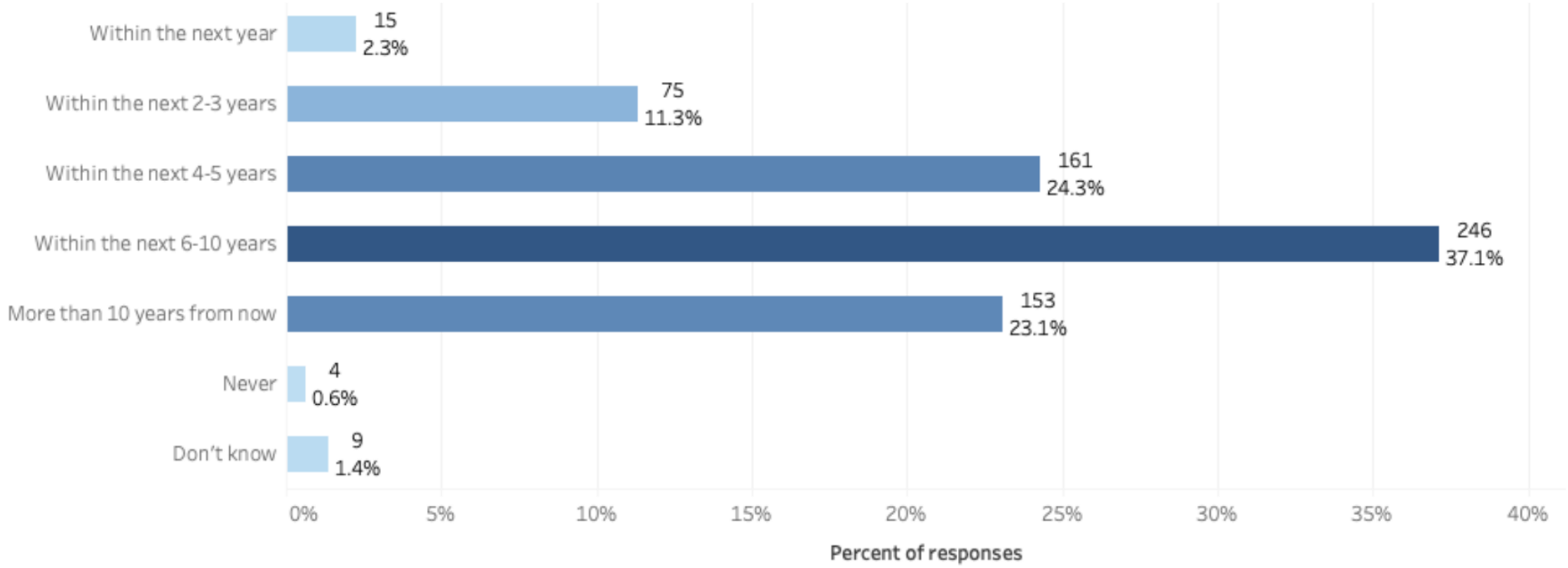


Figure 29 - When do you expect quantum to be a superior alternative to classical computing for certain workloads?

Most respondents felt that it would be 6-10 years from today.

Source: https://www.quera.com/blog-posts/current-and-future-state-of-quantum-computing

Copyright© Eric Heflin

Definition and Context

New Algorithmic Attacks

Three Tracks

Risks

Defenses

Opportunities

Suggested Approach

Further Reading

HL7® International

ASTP Assistant Secretary for Technology Policy

ONC Office of the National Coordinator for Health Information Technology

® Health Level Seven and HL7 are registered trademarks of Health Level Seven International, registered with the United States Patent and Trademark Office.

Copyright© Eric Heflin

Impact of Quantum Computing on Healthcare IT

Assumptions:
1) We take no action
2) We are using RSA and ECC encryption
3) Quantum computing become practical
4) Reminder: Symmetric encryption can be quantum resistant

- If we take no action (continue to use current algorithms) then…
- PKI based network communications: Become insecure
- VPN using Pre Shared Key: Likely OK
- VPN using X.509: Becomes insecure
- Encrypted e-mail: Becomes readable and untrustworthy
- Classic RSA/ECC PKI: Not trustworthy
- Digital Signatures: No longer trustworthy
- Software and Mobile App distribution: No longer trustworthy
- Cryptocurrencies: Fundamentally broken in many cases (including Bitcoin)

Copyright© Eric Heflin

Image: Licensed from iStockPhoto

Definition and Context

New Algorithmic Attacks

Three Tracks

Risks

Defenses

Opportunities

Suggested Approach

Further Reading

HL7® International

ASTP Assistant Secretary for Technology Policy

ONC Office of the National Coordinator for Health Information Technology

® Health Level Seven and HL7 are registered trademarks of Health Level Seven International, registered with the United States Patent and Trademark Office.

Copyright© Eric Heflin

Quantum Computing Defenses
Post-Quantum Cryptography

- Post-Quantum or “quantum resistant” algorithms are already available for testing for free
- NIST has been driving an international competition that is nearing likely completion (genesis in the year 2015)
- Goal is to create algorithms and approaches so that classic computers can resist quantum attacks
- One promising technique is to employ multiple containers, such as multiple quantum resistant algorithms, or to use large bit size asymmetric inside quantum resistant.

Image: Licensed from iStockPhoto

Copyright© Eric Heflin

Analogy: A Pipe within a Pipe

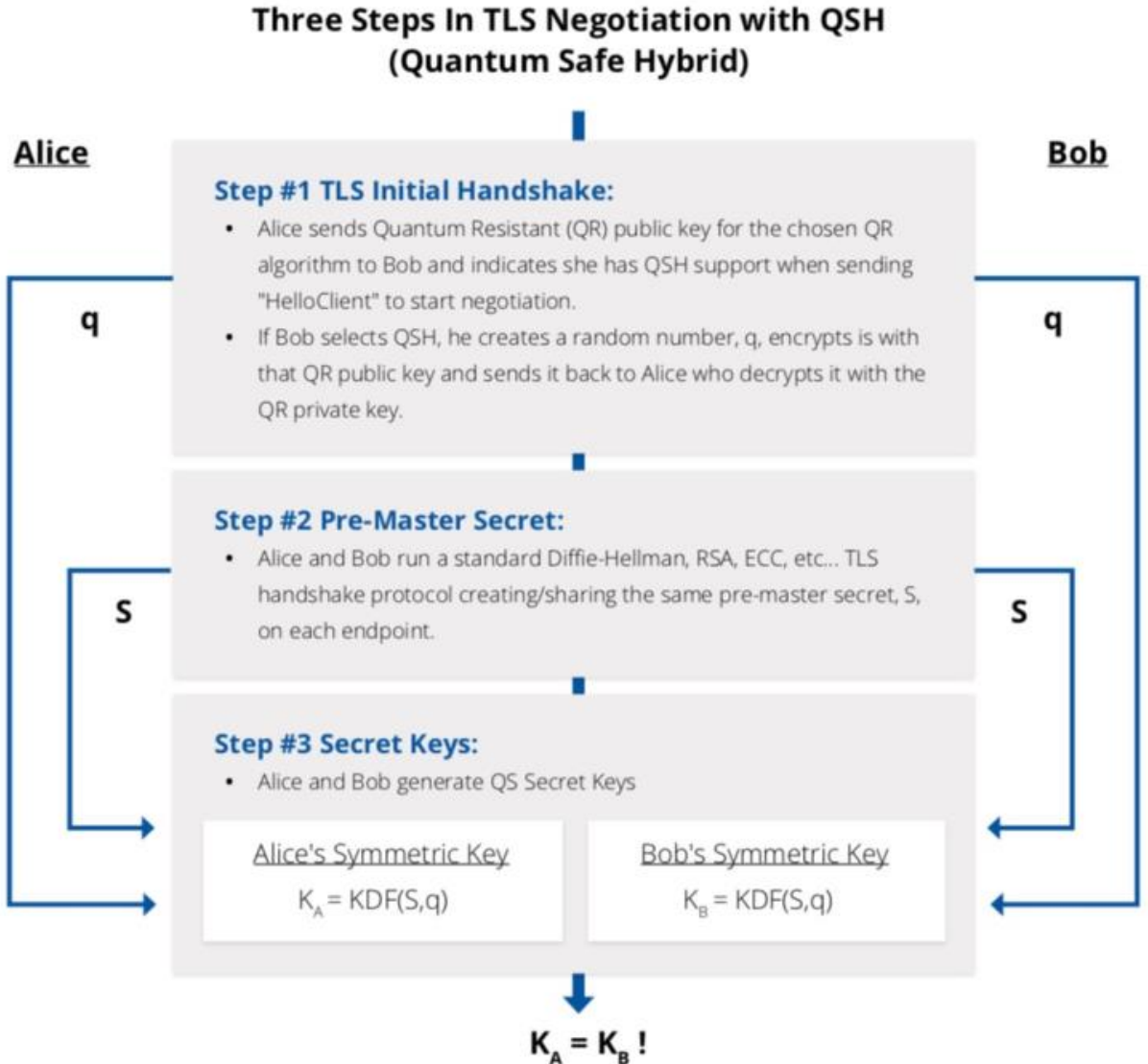
Quantum Safe Encryption Tunnel

Traditional Encryption Tunnel

Image: Licensed from iStockPhoto

Copyright© Eric Heflin

Exploring One Solution: Post Quantum Computing Hybrid Approach for TLS



- Enable TLS Key Negotiation with two algorithms (PQC algorithm and traditional)
- Used to transport Quantum safe component (TLS session key) between two communicating parties
- Adopting PQC algorithm as part of initial TLS handshake may thwart the exposure of TLS Session Key

Image and text credit: Ramesh Nagapan, Harvard University

Definition and Context

New Algorithmic Attacks

Three Tracks

Risks

Defenses

Opportunities

Suggested Approach

Further Reading

HL7® International

ASTP Assistant Secretary for Technology Policy

ONC Office of the National Coordinator for Health Information Technology

® Health Level Seven and HL7 are registered trademarks of Health Level Seven International, registered with the United States Patent and Trademark Office.

Copyright© Eric Heflin

Image: Licensed from iStockPhoto

New Opportunities

- Stronger encryption methods
- Quantum key distribution protocols
- Faster cryptanalyses
- Improved authentication methods
- Enhanced machine learning algorithms, leading to better fraud detection, malware identification, and intrusion detection
- Truly random number generation
- Tamper detection observation

Copyright© Eric Heflin

Definition and Context

New Algorithmic Attacks

Three Tracks

Risks

Defenses

Opportunities

Suggested Approach

Further Reading

HL7® International

ASTP Assistant Secretary for Technology Policy

ONC Office of the National Coordinator for Health Information Technology

® Health Level Seven and HL7 are registered trademarks of Health Level Seven International, registered with the United States Patent and Trademark Office.

Copyright© Eric Heflin

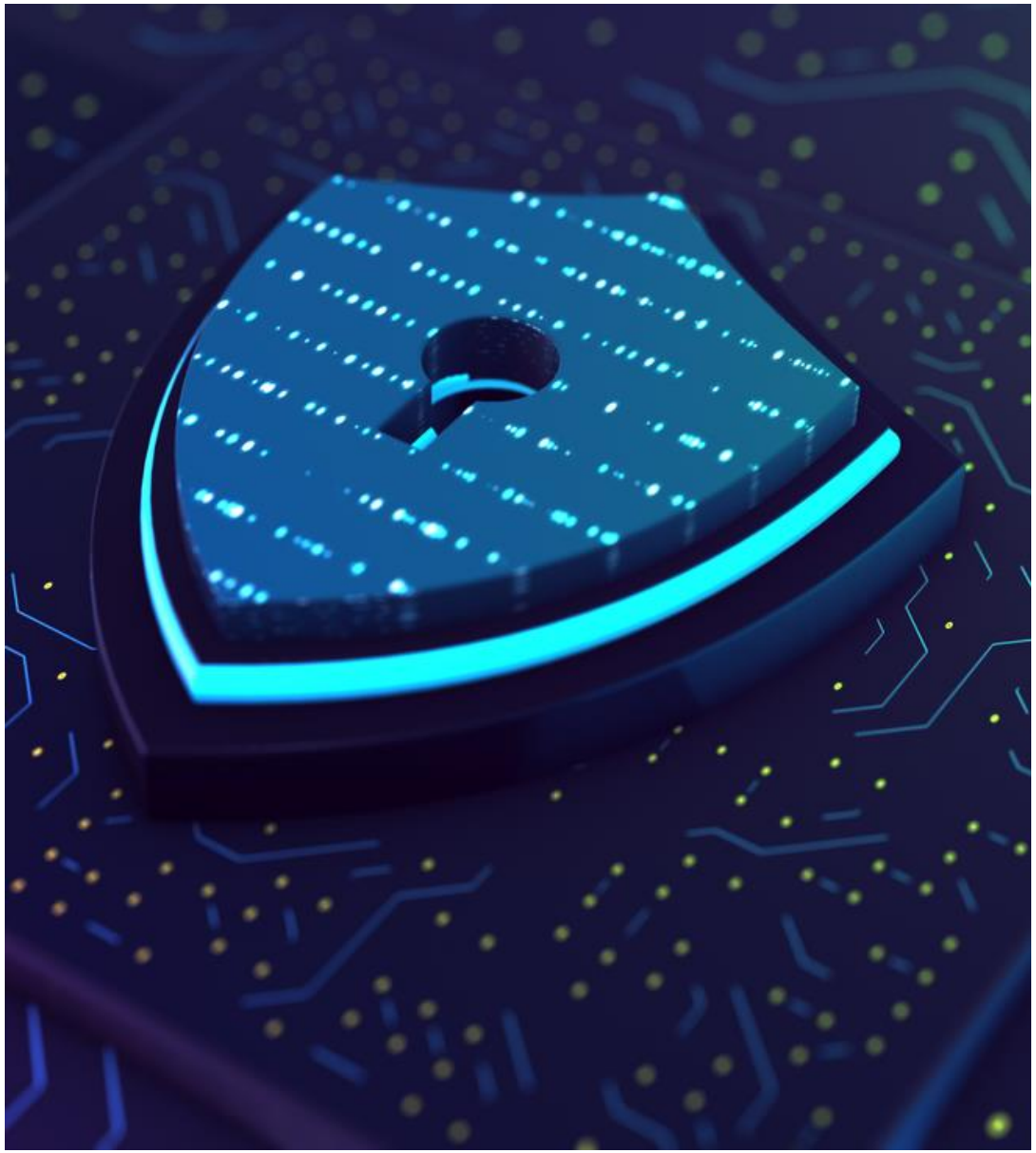


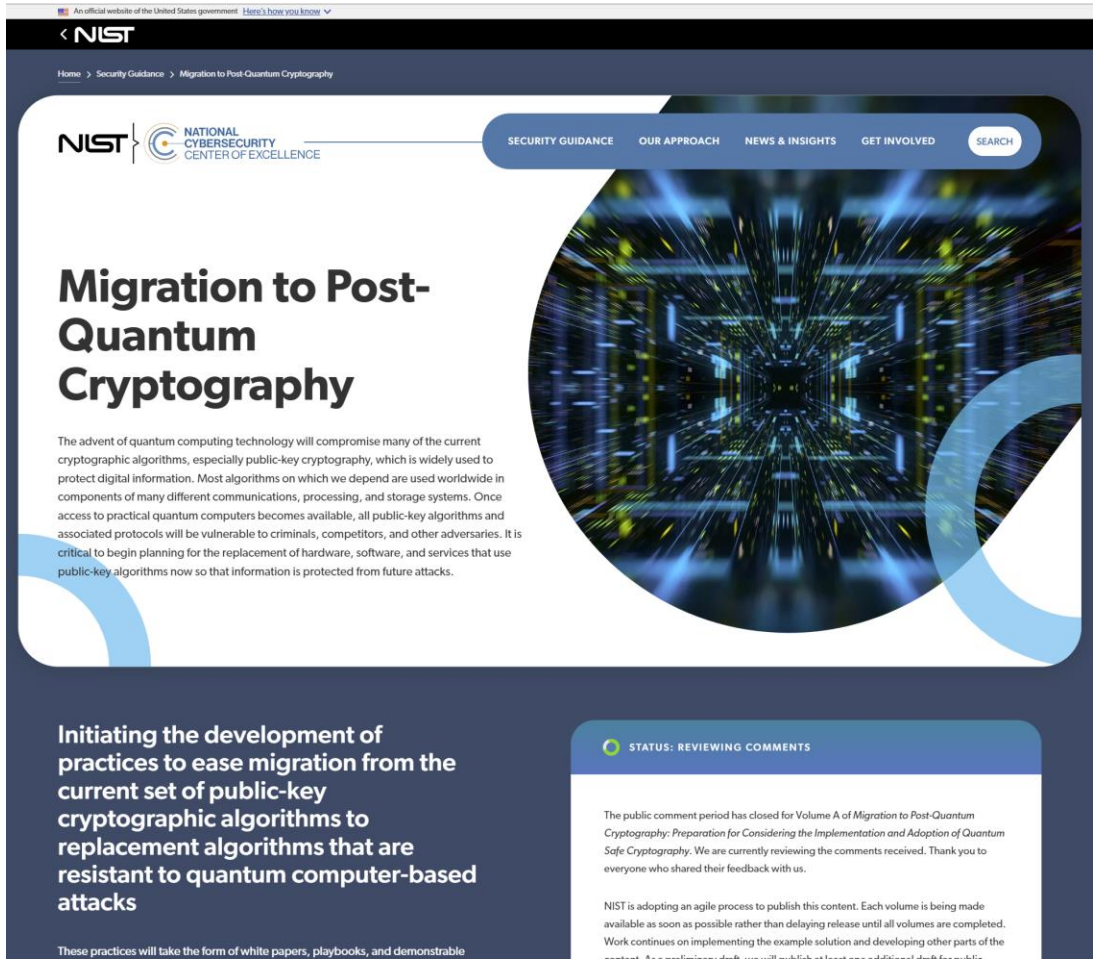
Image: Licensed from iStockPhoto

When Should We Start Planning For Post Quantum?

- Michele Mosca:
- X = amount of time that we wish our data to be secure
- Y = time it will take for our computer systems to transition from classical to postquantum
- Z = time it will take for quantum computers to start breaking existing quantum-susceptible encryption protocols
  - X + Y > Z
  - 10 years + 5 years perhaps?

Copyright© Eric Heflin

Copyright© Eric Heflin

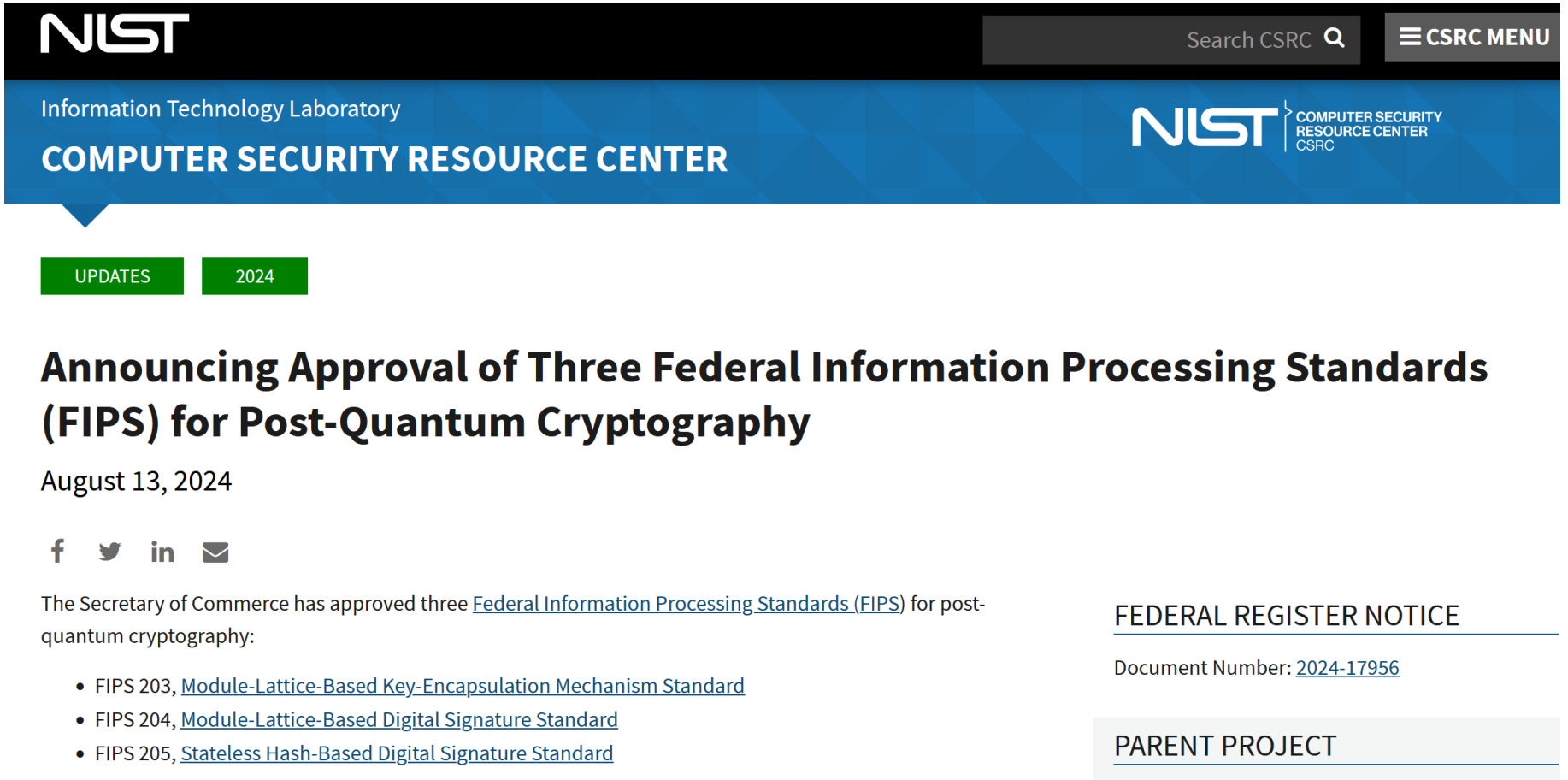


NIST Challenge

- Announced in 2015
- International competition to create viable Post Quantum crypto systems
- Initial winners announced August 2024
- Initially had 59 encryption schemes and 23 signature schemes
- Public Key Encryption finalists:
  - CRYSTALS-Kyber
  - ~~NTRU~~
  - ~~SABER~~
- Three signature finalists:
  - CRYSTALS-Dilithium
  - FALCON
  - ~~Rainbow~~
- Work still on-going, and is very dynamic

Copyright© Eric Heflin

New: NIST Has Now Approved Post-Quantum Cryptography Standards FIPS 203, 204, 205



NIST

Search CSRC

CSRC MENU

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

UPDATES 2024

Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography

August 13, 2024

The Secretary of Commerce has approved three Federal Information Processing Standards (FIPS) for post-quantum cryptography:

- FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard
- FIPS 204, Module-Lattice-Based Digital Signature Standard
- FIPS 205, Stateless Hash-Based Digital Signature Standard

FEDERAL REGISTER NOTICE

Document Number: 2024-17956

PARENT PROJECT

Source: https://csrc.nist.gov/News/2024/postquantum-cryptography-fips-approved

Copyright© Eric Heflin

Quantum Safe Project

The Open Quantum Safe (OQS) project is an open-source project that aims to support the development and prototyping of quantum-resistant cryptography.

OQS consists of two main lines of work: liboqs, an open source C library for quantum-resistant cryptographic algorithms, and prototype integrations into protocols and applications, including the widely used OpenSSL library. These tools support research by ourselves and others.

All of our development takes place on our Github repositories. We welcome new contributors interested in joining our team. We are grateful to our financial sponsors and the companies who contribute in-kind developer time.

Recent updates

- July 7, 2023: Release of OQS-OpenSSL 1.1.1 snapshot 2023-07; note that this is the final release of OQS-OpenSSL 1.1.1
- July 5, 2023: Releases of liboqs-cpp 0.8.0, liboqs-go 0.8.0, and liboqs-python 0.8.0
- July 4, 2023: Release of OQS-BoringSSL snapshot 2023-06
- June 26, 2023: OQS-OpenSSH snapshot 2023-06
- June 9, 2023: Release of oqs-provider 0.5.0
- **June 7, 2023: Release of liboqs version 0.8.0**
- **August 21, 2022: Release of liboqs version 0.7.2**

- https://openquantumsafe.org/
- Prototypes of quantum safe:
  - OpenSSL
  - BoringSSL
  - Linux liboqa
  - TLS
  - SSH
  - X.509 certificates
  - CMS and S/MIME

HL7 International | ASTP Assistant Secretary for Technology Policy | ONC Office of the National Coordinator for Health Information Technology

Copyright© Eric Heflin

Definition and Context

New Algorithmic Attacks

Three Tracks

Risks

Defenses

Opportunities

Suggested Approach

Further Reading

HL7® International

ASTP Assistant Secretary for Technology Policy

ONC Office of the National Coordinator for Health Information Technology

® Health Level Seven and HL7 are registered trademarks of Health Level Seven International, registered with the United States Patent and Trademark Office.

Copyright© Eric Heflin

Suggested Approaches

1

Monitor NIST Quantum challenge results

Inventory the healthcare IT cybersecurity standards your organization relies upon

2

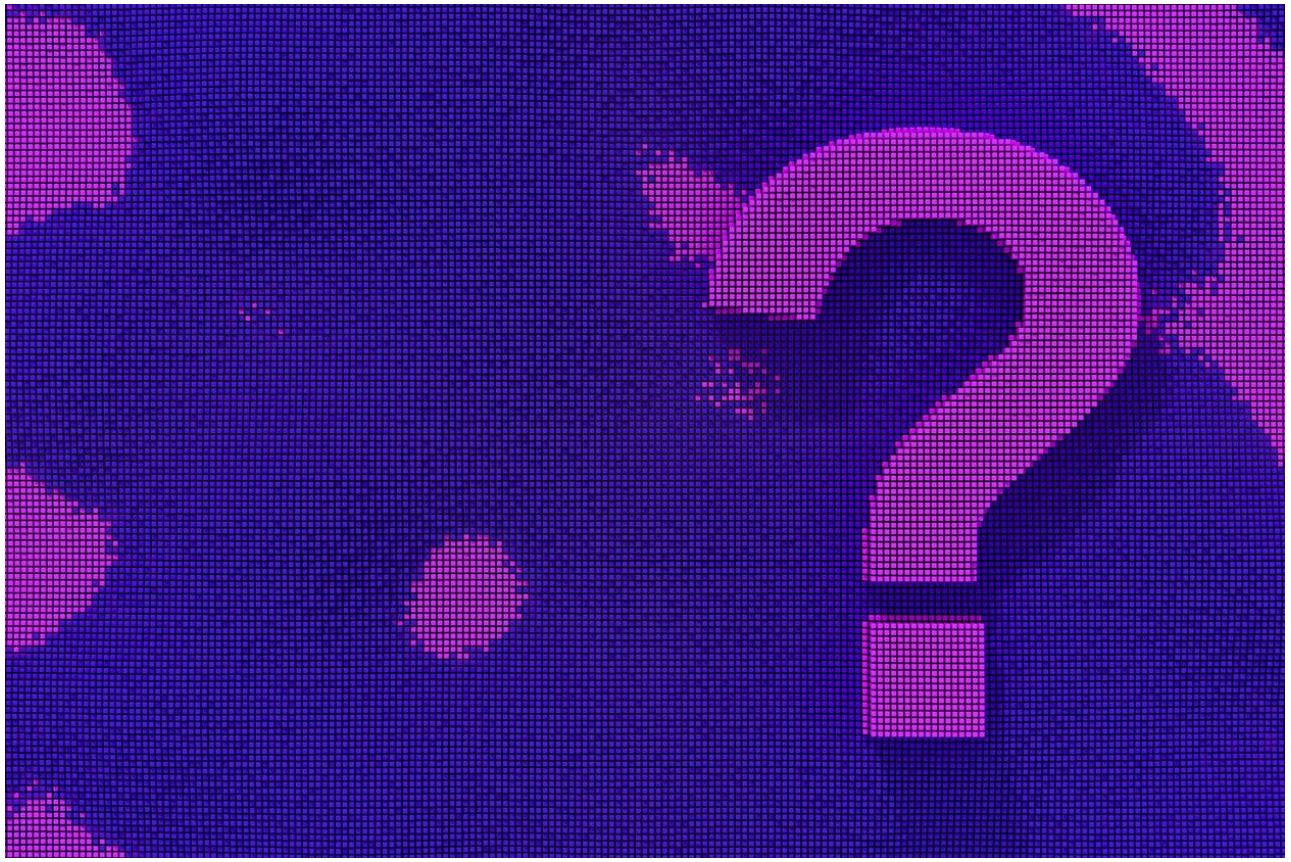
Monitor practical computing progress esp. breakthroughs and noise-tolerant implementations (Quantum Safe Project)

3

Identify a point where the standards you use (HL7, IHE, ANSI, NIST, etc.) are viable to update to quantum safe and then take an active role such as requesting working group support

Updated security considerations sections of business processes

Copyright© Eric Heflin



Questions?

Image: Licensed from iStockPhoto

Copyright© Eric Heflin

- Definition and Context
- New Algorithmic Attacks
- Three Tracks
- Risks
- Defenses
- Opportunities
- Suggested HL7 Approach
- Further Reading

HL7® International

ASTP Assistant Secretary for Technology Policy

ONC Office of the National Coordinator for Health Information Technology

® Health Level Seven and HL7 are registered trademarks of Health Level Seven International, registered with the United States Patent and Trademark Office.

Copyright© Eric Heflin

Further (Optional) Reading

- https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms
- https://www.schneier.com/blog/archives/2023/05/nist-draft-document-on-post-quantum-cryptography-guidance.html
- https://csrc.nist.gov/pubs/sp/1800/38/iprd
- https://openquantumsafe.org/
- https://www.sciencedaily.com/news/computers_math/quantum_computers/

Image credit: Licensed from iStockPhoto

® Health Level Seven and HL7 are registered trademarks of Health Level Seven International, registered with the United States Patent and Trademark Office.

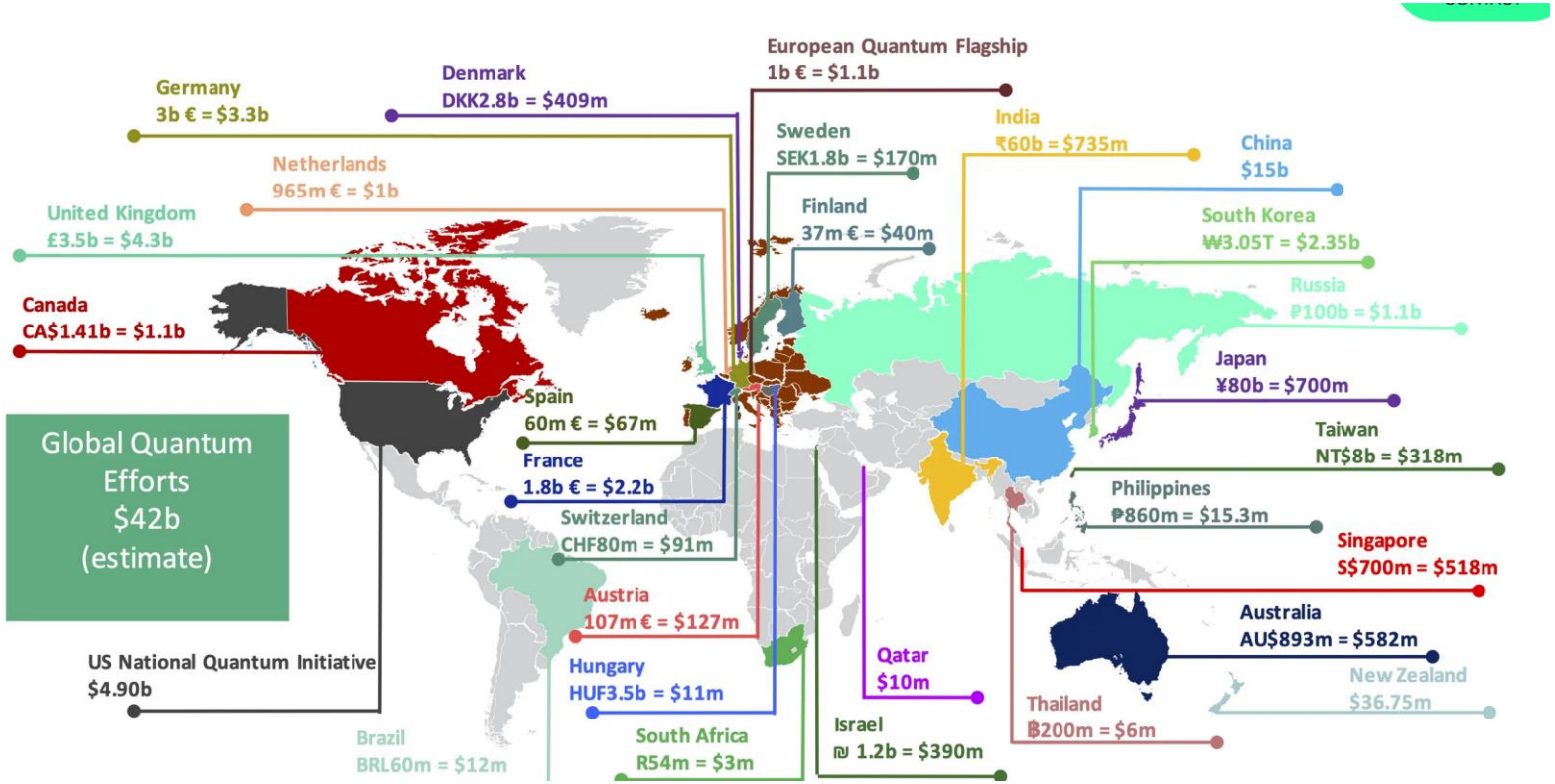
Copyright© Eric Heflin

My Contact Information

- https://www.linkedin.com/in/eric-heflin/
- https://EricHeflin.com
- Email: Eric @ Heflin.io
- Mobile: 512.897.0748 (text before calling please)
- Signal: 5128970748

® Health Level Seven and HL7 are registered trademarks of Health Level Seven International, registered with the United States Patent and Trademark Office.

Total National Quantum Computing Investments



Estimated cumulative quantum computing investment per nation

Source: https://www.qureca.com/quantum-initiatives-worldwide/