Accenture Federal Services

Post-Quantum Security

Quantum Computing & the Threat to Cybersecurity

Garland Garris, Global Quantum Security Lead

Quantum Timeline: Background

The quantum computing journey has spanned a century, and advancement is escalating:

1900s – 1990s
Quantum
Theory Work

1990s – 2000s
First Derived
Technical Devices

2010s – 2010s
Quantum
Processor
Development

2015 >
Quantum
Computer
Development

2020 >
Production
of Quantum
Computers

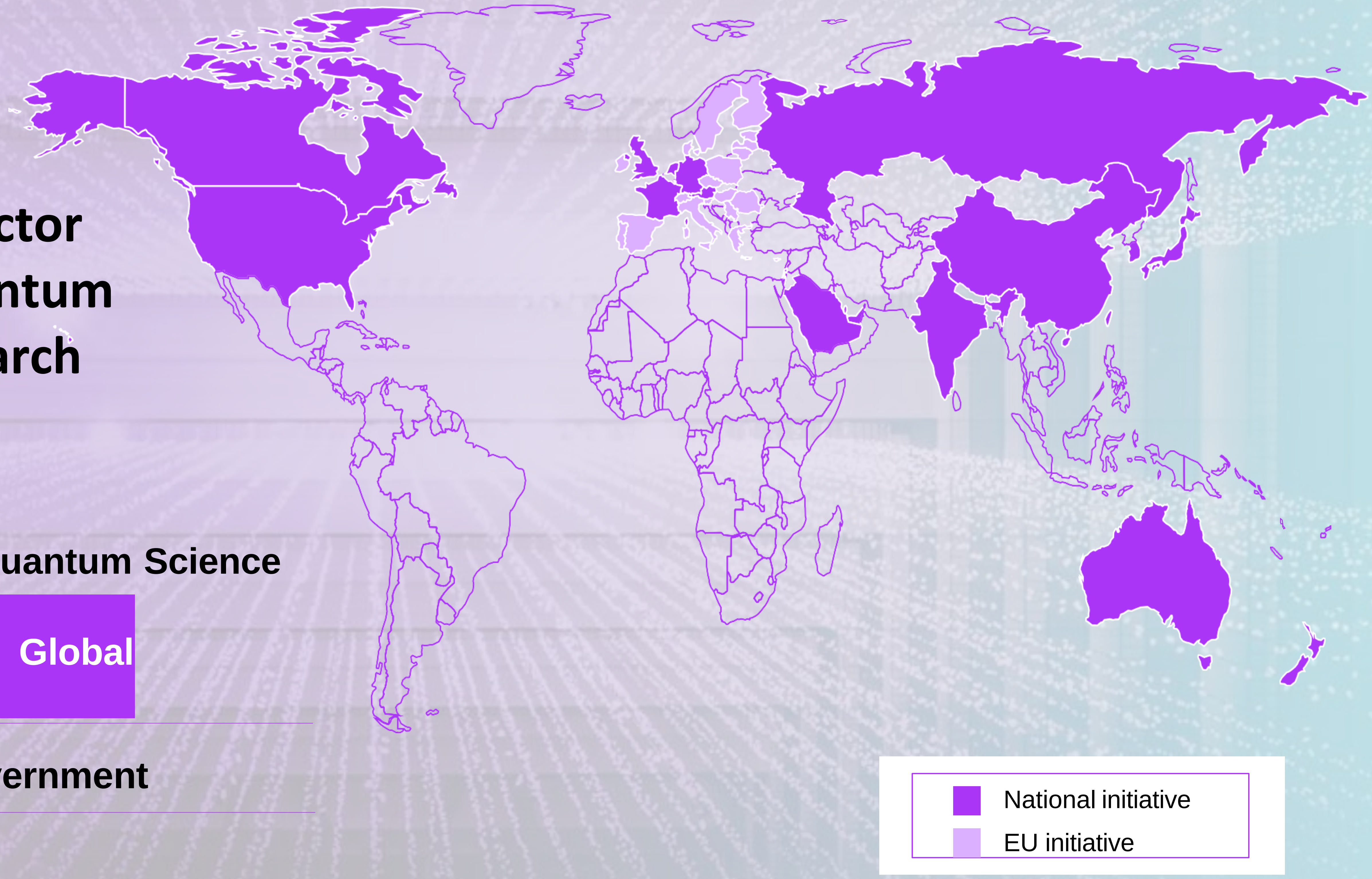
2020 >
Cloud Computing

- **Simulation & Optimization –** molecular & atomic interaction
- **Sensing –** magnetic & gravitational fields
- **Artificial Intelligence –** new opportunities in faster AI
- **Materials Science – materials engineering**
- **Financial Services –** stock options pricing

intel
IBM
Google
amazon
Microsoft
Tencent Cloud
Alibaba Cloud

Government Investment in Quantum

Global public sector investing in quantum computing research



2021 Investment in Quantum Science

$24B Global

$1B U.S. government

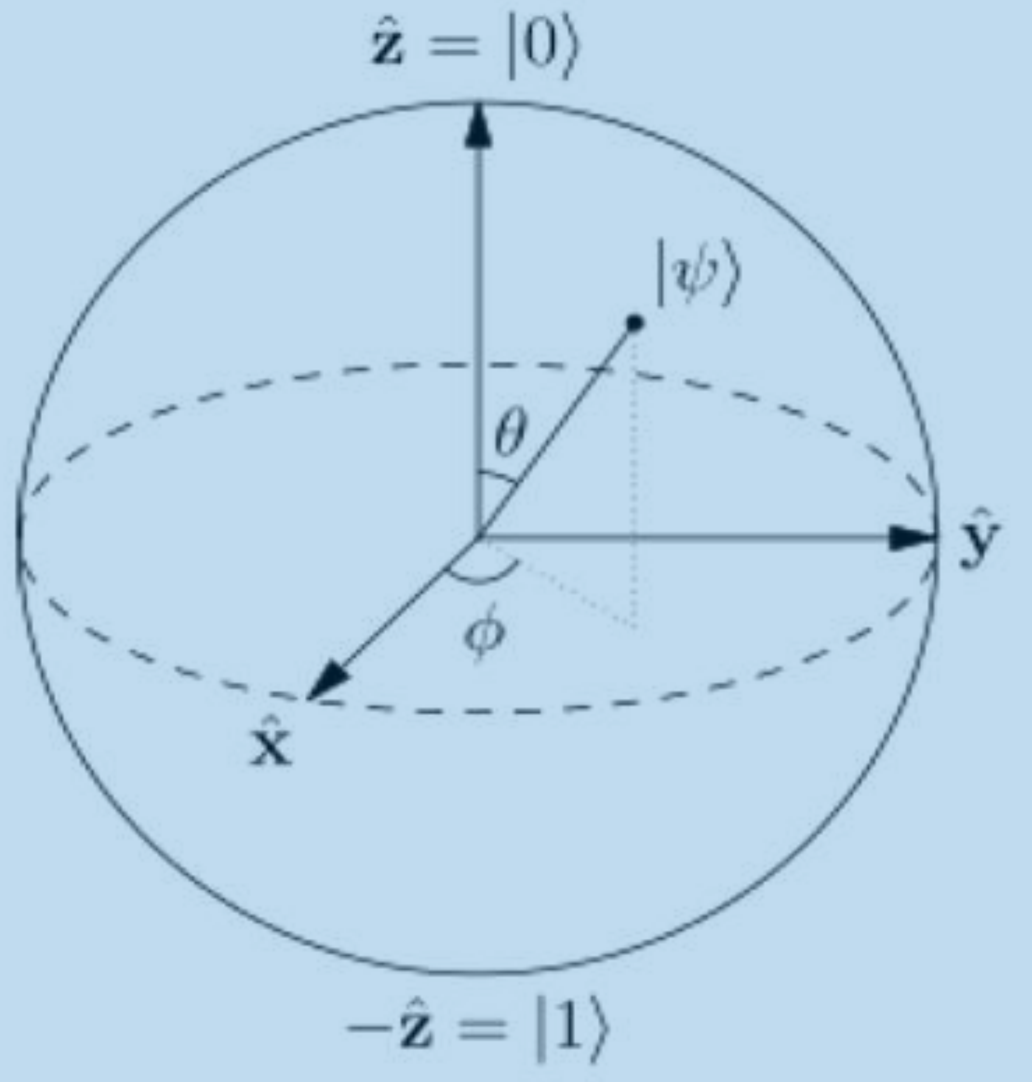
How Is Quantum Computing Different?

A classical computer **BIT** is a **ZERO** or a **ONE**, arranged in logical order that makes sense when mapped to a natural language.

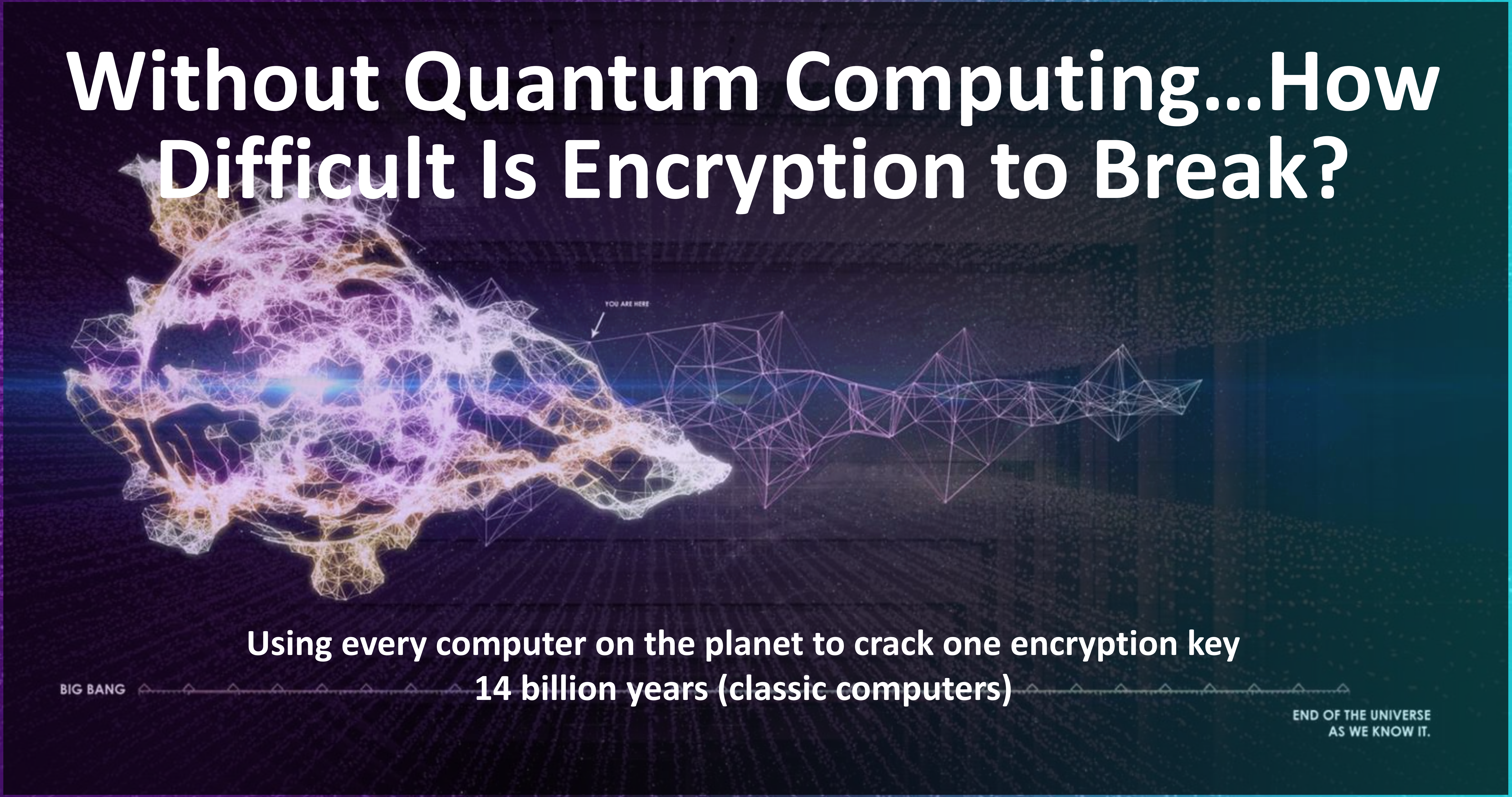
QUANTUM COMPUTERS

- A **QBIT** can be zero and one at the same time and in any number of **superpositions** in between.
- Also, quantum particles can become **entangled** such that if you change one particle, it changes the other one.

Using these properties, quantum computers have been built that can solve **specific types** of problems exponentially faster than traditional computers.

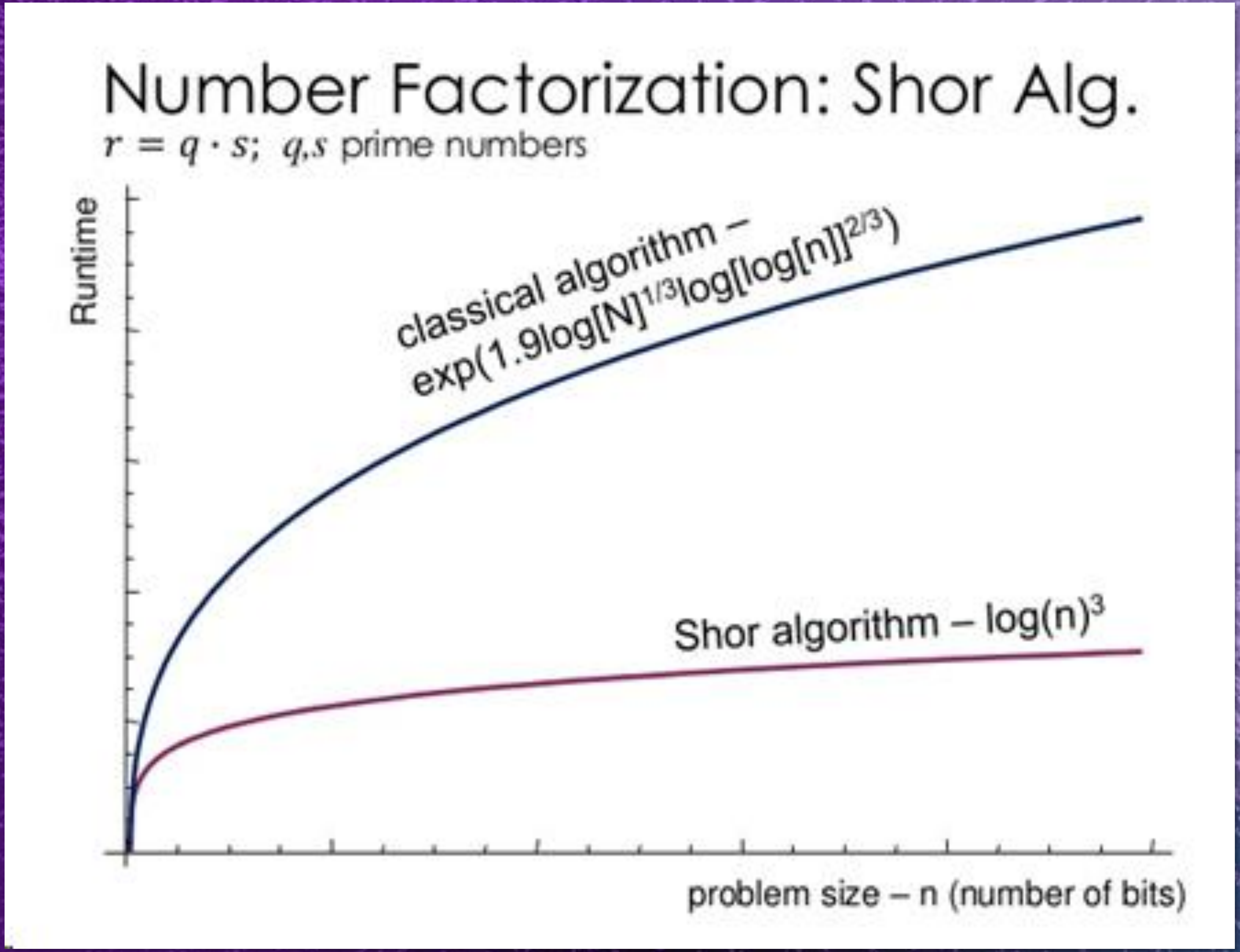


Without Quantum Computing…How Difficult Is Encryption to Break?



Using every computer on the planet to crack one encryption key
14 billion years (classic computers)

How Vulnerable Are We?



Advances in quantum computing will render multiple cryptosystems—all previously deemed impenetrable—vulnerable to brute force attacks.

Key Standard	Qubits	Time to Break
RSA-1024	2050	**3.58 hours**
RSA-2048	4098	**28.63 hours**
NIST P-256	2300	**10.5 hours**
NIST P-521	4098	**55 hours**
AES-128	2953	2.6×10^{12} years
AES-256	2953	2.29×10^{32} years

🟪 Employing Shor’s algorithm

⬜ Employing Grover’s algorithm

The Question of When (Y2Q)

Today’s quantum computers:
50-100 Qubits a piece

Quantum computers of 2000+
Qubits will pose a crypto threat

Truly clutch quantum
computing: (10-20 yrs)

$ Billions of private and public
sector R&D: shorten estimates

Why This Is a NOW Problem

“Hack Now, Crack Later”
Adversaries steal sensitive data today, with the intent of decrypting it when quantum computers mature.

20+ billion devices must be upgraded to quantum-safe cryptography.

Daunting but Doable: Y2Q Scale

Level of effort: comparable to efforts undertaken to address Y2K bug

As veterans of government know, government system transitions can take years.

Common Misconceptions About PQC

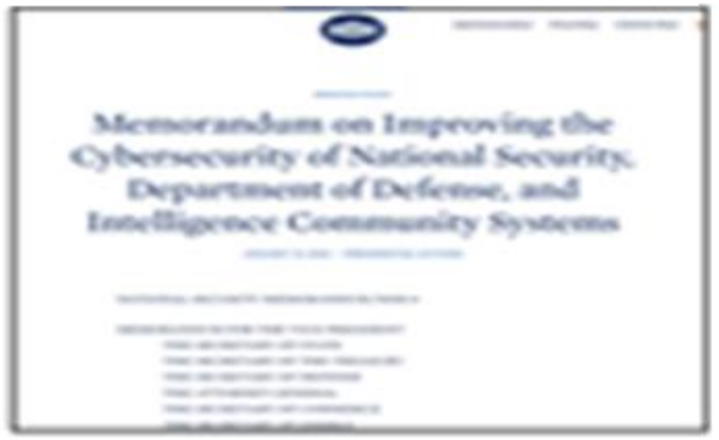
- ⊗ Agency leaders must understand quantum science to prepare for PQC.
- ⊗ Achieving quantum-resilient cryptography requires quantum computers.
- ⊗ There’s nothing we can do today to protect data against quantum-enabled decryption.
- ⊗ It is the responsibility of CSPs to secure my GovCloud environment from quantum threats.

White House Mandates Agency Action

May 12th 2021 – EO 14028

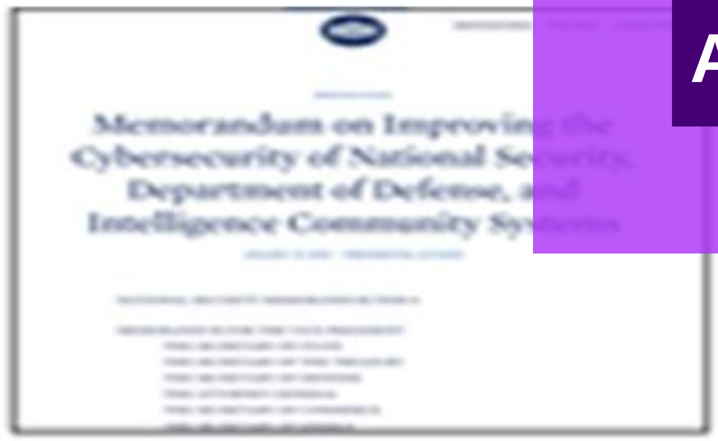
Executive Order on Improving the Nation's Cybersecurity

Jan 19th 2022 – NSM-8



Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems

May 4th 2022 NSM-10



Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems

Nov 22nd 2022 – M-23-02

Dec, 21 2022 – HB7535

117th CONGRESS
2d Session

S. ____

To encourage the migration of Federal Government information technology systems to quantum-resistant cryptography, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Ms. Hassan (for herself and Mr. Portman) introduced the following bill, which was read twice and referred to the Committee on ____

A BILL

To encourage the migration of Federal Government informa-

Deadline to inventory and report on quantum vulnerabilities

Agencies operating NSS	July 2022
All other agencies	May 2023

Images of documents referenced are taken from https://whitehouse.gov

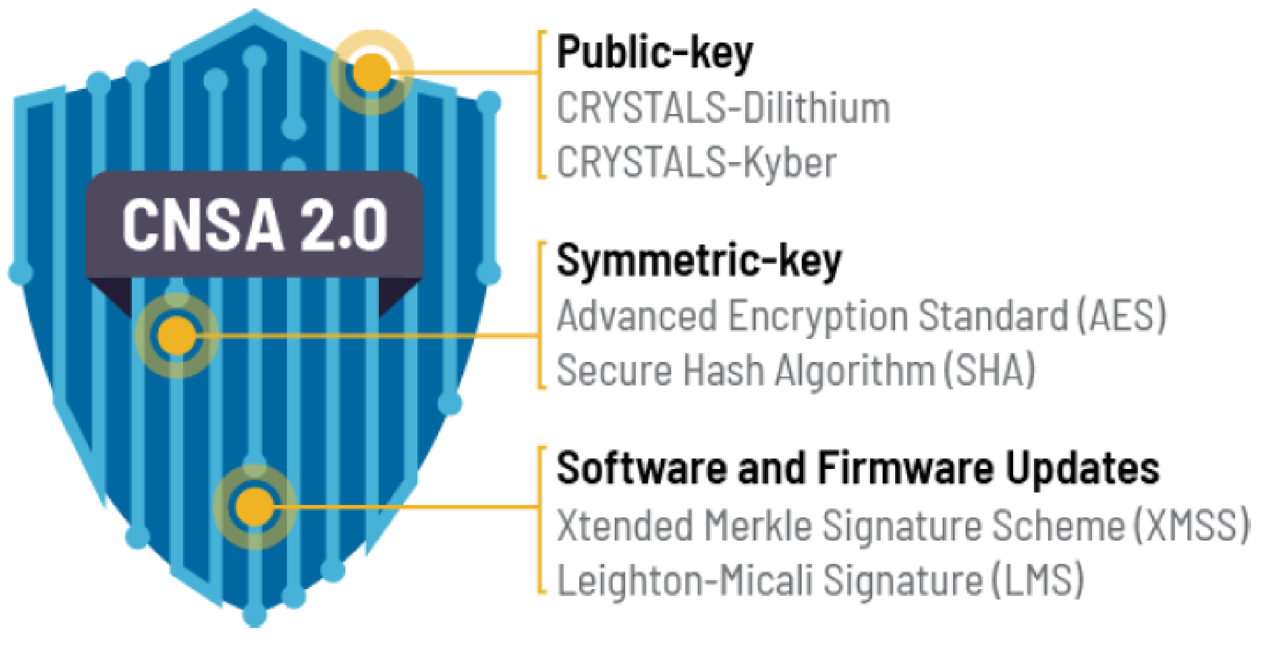
NIST-NSA Post-Quantum Standards and Guidance

Announcing the Commercial National Security Algorithm Suite 2.0

CNSA 2.0 Timeline

NIST Post-Quantum Cryptography Standardization

Year	Round	Candidates	Accepted
2017	Round 1	82	**69**
2019	Round 2	69	**26**
2020	Round 3	26	**15**
2022	**First Four PQC Algorithms Selected**		



Public-key
CRYSTALS-Dilithium
CRYSTALS-Kyber

Symmetric-key
Advanced Encryption Standard (AES)
Secure Hash Algorithm (SHA)

Software and Firmware Updates
Xtended Merkle Signature Scheme (XMSS)
Leighton-Micali Signature (LMS)

Images of referenced are taken from https://media.defense.gov

CRYPTOGRAPHY SOLUTIONS

QUANTUM – BREAKABLE

RSA Encryption

A message is encrypted using the intended recipient's public key, which the recipient then decrypts with a private key. The difficulty of computing the private key from the public key is connected to the hardness of prime factorization.

Diffie-Hellman Key Exchange

Two parties jointly establish a shared secret key over an insecure channel that they can then use for encrypted communication. The security of the secret key relies on the hardness of the discrete logarithm problem.

Elliptic Curve Cryptography

Mathematical properties of elliptic curves are used to generate public and private keys. The difficulty of recovering the private key from the public key is related to the hardness of the elliptic-curve discrete logarithm problem.

QUANTUM – SECURE

Lattice-Based Cryptography

Security is related to the difficulty of finding the nearest point in a lattice with hundreds of spatial dimensions, where the lattice point is associated with the private key, given an arbitrary location in space associated with the public key.

Code-Based Cryptography

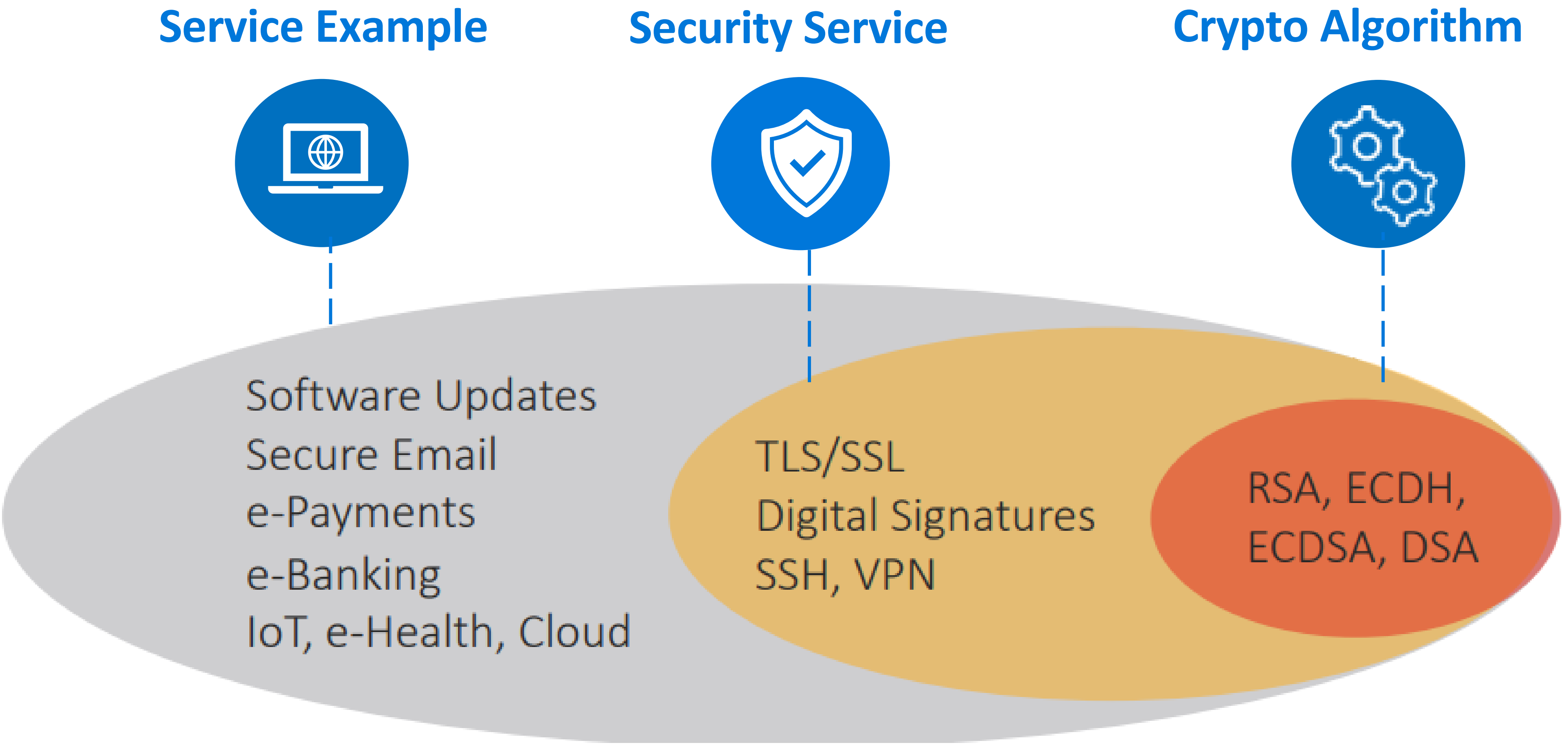
The private key is associated with an error-correcting code and the public key with a scrambled and erroneous version of the code. Security is based on the hardness of decoding a general linear code.

Multivariate Cryptography

These schemes rely on the hardness of solving systems of multivariate polynomial equations.

Study – Post-Quantum Authentication in TLS 1.3 – A Performance Study*

TLS certificates are used to encrypt all comms between client and server.



Service Example

Security Service

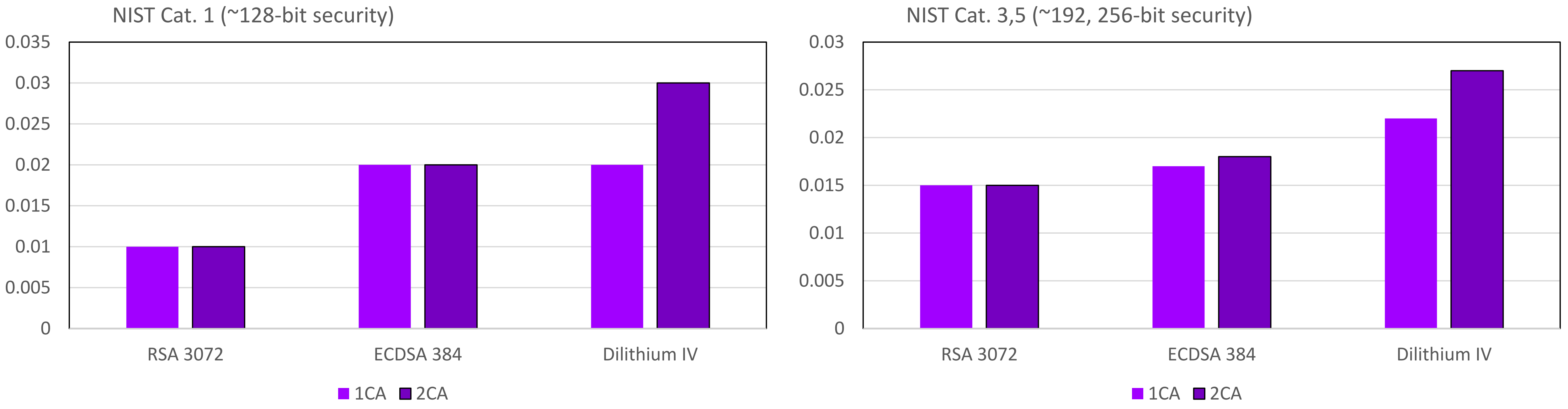
Crypto Algorithm

Software Updates
Secure Email
e-Payments
e-Banking
IoT, e-Health, Cloud

TLS/SSL
Digital Signatures
SSH, VPN

RSA, ECDH,
ECDSA, DSA

PQ Handshake Time vs. Classic Algorithms – TLS Handshake Time in Seconds



Perf. of Sign/Verify Operations

Signature Algorithm	Sign	Verify
RSA 3072	3.19	0.06
ECDSA 384	1.32	1.05
Dilithium II	0.82	0.16
Dilithium IV	1.25	0.30

Certificate Chain Sizes

	Cert. Chain Size KB		
Signature Algorithm	1CA	2CA	Verify
RSA 3072	1.63	2.44	0.38
ECDSA 384	1.34	2.15	.0.05
Dilithium II	6.90	10.42	2.04
Dilithium IV	10.70	16.11	3.37

Performance Takeaways

- Dilithium NIST Level 1 performed sufficiently but at <128 bit of classical security – 15% performance hit.
- Web connections will be most effected, short-lived small amounts of data per connections.
- Increase TCP congestion window parameter to >34 MSS to accommodate all PW algorithms round trip.
- Increased certificate size can cause connection issues.

---

*Dimitrios Sikeridis, Panos Kampanakis, Michael Devetsikiotis, Dept. of Electrical and Computer Engineering, The University of New Mexico, USA

Crypto-agility: The Key to Compliance and Enduring Security

Crypto-agility enables an organization to quickly switch between algorithms, cryptographic primitives, and other encryption mechanisms.

Support for multiple algorithms is needed.

(Kyber, Dillithium, Falcon, ….)

Advantages of Crypto-agility

Crypto-agility simultaneously solves for current and future threats. Key advantages include:

- Support legacy and PQC algorithms.
- Determine which assets can be protected with conventional cryptography while others require PQC.
- Agencies can maintain continuous compliance.
- Advanced threat detection enabling agencies to detect previously unknown cryptography on their networks.

Agile vs. Hasty: Avoiding the Risks of Unproven Cryptosystems

Crypto-agility does not equal hasty adoption of PQC technologies.

A quantum-safe cypher created by a threat actor could be used to hold ransom or permanently deleted by employing cryptographic erasure.

First Steps: Launching the Journey Toward Crypto-agility

Agencies can begin the work of inventorying and auditing their current cryptographic posture without committing significant personnel or budgetary resources.

Empowered with an inventory of cryptography, advise agency effort to achieve quantum-safe cryptography by advising agency planning and implementation efforts by:

Providing **inputs to budgetary requests** to provision crypto-agile platform and operating model

Identifying **systems with legacy cryptographic** standards and other priority security updates

Prioritizing **updates to protect HVAs with quantum-resistant algorithms**

Many factors go in to understanding an agency's vulnerability to a QC-enabled threat actor:

- ✓ Custom systems with embedded algorithms
- ✓ Legacy systems, which may contain legacy cryptography
- ✓ Disconnected or island networks
- ✓ The maturity of the agency's current cybersecurity and information assurance program

Enduring Cyber-Resilience for the American People

1. DHS-NIST Quantum Roadmap
2. Inventory & Assessment of Crypto
3. Identify Public Key Crypto Use
4. Prioritize HVAs
5. Choose a Crypto-Agility Platform
6. Develop a Transition Plan
7. Integrate Post-Quantum Plan Into ZT Strategy

Counter Imminent Post-Quantum Threats

Timeline: Policy, Compliance, and Action on Quantum Computing

The Path to Crypto-agility for Federal Agencies

2-3 Months
Preparation & Assessment

6 Months
Define Crypto-agile Strategy – Targeted Scanning

1-3 Years
Define and Implement Crypto-agility Platform

Ongoing
Maintain Crypto-agile Posture; Continuous Monitoring

Y2Q–Traditional encryption becomes crackable

2030 ⟶

Classical Computing Era

Quantum Computing Era

Policy and Compliance Milestones

- **Dec 2016** NIST launches search for PQC standard
- **Dec 2018** Congress passes National Quantum Initiative Act
- **Jan 2022** NSM-08 mandates action for IC and defense agencies
- **May 2022** NSM-10 mandates action for civilian agencies
- **July 2022** NIST selects 4 algorithms for future PQC standard
- **December 2022** HB7535 - Quantum Computing Cybersecurity Preparedness Act
- **2024** NIST announces additional PQC algorithms (anticipated)
- **2024-2026+** All agencies must implement NIST standard (anticipated)

Critical Agency Deadlines

- **July 2022** NSS agencies must report on quantum vulnerabilities
- **May 2023** Non-NSS agencies must report on quantum vulnerabilities
- **Sep 2024** All agencies must achieve Zero Trust

Accenture Federal Services

Thank you

Garland Garris, Global Quantum Security Lead
Garland.garris@accenturefederal.com