Post-Quantum Cryptography (PQC)

1

Post-Quantum Crypto (PQC): What, Why, How ?

What is PQC?

The development and implementation of cryptographic algorithms that are considered to be secure against a cryptanalytic attack by a quantum computer.

PQC is also known as "quantum-proof," "quantum-safe" or "quantum-resistant" cryptography

Why do I care about PQC?

When large-scale quantum computers (QC) become available, they will be able to break many of the public-key cryptosystems currently in use. This will seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere. Compliance deadlines in place or imminent.

How does PQC protect against QC attacks?

PQC is a collection of standardized algorithms that are believed to be resistant to quantum computer attacks. These algorithms have been vetted by U.S. NIST as part of its "PQC standardization process" that started in 2016.

2

2

The Quantum Computer (QC) Threat to Cryptography

Quantum Computers (QC): *NEW* Computing Paradigm
- (*Some*) Algorithms Exploit the "Quantum Advantage"

Quantum Advantage
- *Information Parallelism*: Qubits are both "0" and "1" at the same time
- *Entanglement*: Value of One Qubit is "Coupled" to Another Qubit

Algorithms that Threaten Modern Cryptography
- Shor's Factoring Method: Quickly Factor Semiprimes
  (824,095,473,731,380,783 = 997,991,983 × 825,753,601)
  Used to Quickly Find the Key in Public Key Encryption (PKE)
- Grover's Search Method: Find Value in List of N, with $\sqrt{N}$ Steps
  (Can Find Jack of Hearts in Shuffled Deck with $8 = \lfloor\sqrt{52}\rfloor$ Tries)
  Used to Quickly Find the Key in Shared Key Encryption (SKE)

CRQC: "Cryptoanalytically Relevant Quantum Computer"

3

3

Quantum Technology: A Clear and Present Danger ????

Quantum computing is *not a future threat*, but *a present and urgent challenge* that organizations must address immediately.

Specifically:
- Quantum readiness is a "now" problem, not a future concern (HNDL & PQC Dev. time)
- Nearly half of businesses are not prepared for quantum computing threats
- Companies need to develop comprehensive quantum-safe roadmaps now
- Waiting or delaying action could lead to significant cybersecurity risks
- Organizations must:
  - Conduct strategic assessments: "Discovery" Migration Phase should Start Now
  - Gain cryptographic visibility: Create "Cryptographic Bill of Materials" (CBoM)
  - Build cryptographic resilience: Especially for Crypto-Hybrid Implementations
  - Prepare for future cryptographic migrations: This WILL Happen Again "Quantum Crypto" is Coming

Corporations should proactively prepare for quantum threats, viewing this as an opportunity to strengthen their overall cybersecurity posture, rather than waiting for a crisis to force action.

*Some content from Michele Mosca, Global Risk Institute

4

4

How Important is PQC, Should I be Concerned?

- Modern Public Key Cryptography (PKE) Systems and Infrastructure Required About 20 Years to Deploy
- While Debatable, Many Experts Believe CRQC Will Become Available Within a 20 Year Timeframe – many predict 3 to 10 years – "Y2Q" day
- In 2024, NIST Standardized Three (3) PQC Standards, More Coming
- PQC Standards are Not Drop-in Replacements:
  - Larger-sized keys will generally be needed
  - New PQC Codes Require Support (*eg.*, high-quality & high-throughput RNG/RBG Entropy Sources)
- Migrating to PQC Requires Planning and Time (Adopt/Implement/Deploy)
  - Organizations Urged to Begin the Transition Process Now
  - CRQC Not Yet Available, but a Matter of Engineering and the Race is On, Risk is Feasible by 2035
  - "Harvest Now, Decrypt Later" is Already Occurring so the CRQC Threat may be Relevant Now

5

5

Y2Q & Harvest Now, Decrypt Later: Is it all Hype?

- Y2Q is the Date that a CRQC becomes available, the date that classically encrypted data is vulnerable to a QC attack: the "Quantpocalypse"
- Y2Q will happen, it is a matter of when
- Encrypted private data is still vulnerable due to "Harvest Now, Decrypt Later"
  - Nation States are Harvesting Data – Even the US
  - Massive Amount, High-value Targets Most Likely to be Decrypted
  - Some Criminals may have a Bad Day in the Future
- Y2Q and HNDL are Probably not Reasons to Panic, but they are Reason to Start Planning for PQC Migration Now Rather than Later

6

6

QC Crypto Threat: CRQC Requirements

- Defeating RSA-2048 (Public Key) Requires ~1,000,000 Physical Qubits
  - CRQC Executing Semiprime Factoring Algorithm (Shor's)
  - ~1,730 Logical Qubits (500 to 5,000 Physical Qubits per Logical Qubit)
  - Requires ~40 Runs (Algorithm* Comprises 2^{36} Toffoli Gates)

- Defeating AES-128 (Symmetric) Requires ~200,000 Physical Qubits
  - CRQC Executing Shared Key Search (Grover's)
  - ~264 Logical Qubits for Grover Oracle (Reversible AES-128 circuit)
  - Requires 2^{64} AES Runs (Compared to 2^{128} Runs for Exhaustive Key Search)

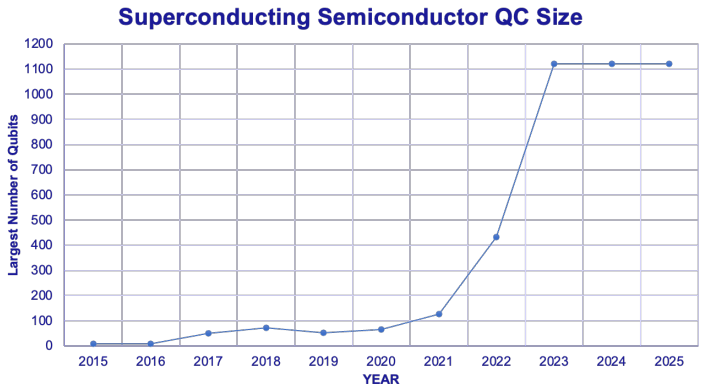
- Defeating AES-256 (Symmetric) Requires ~1,000,000 Physical Qubits
  - CRQC Executing Shared Key Search (Grover's)
  - ~1,300 Logical Qubits for Grover Oracle (Reversible AES-256 circuit)
  - Requires 2^{128} AES Runs (Compared to 2^{256} AES Runs For Exhaustive Key Search)

*Chevignard, C., Fouque, P. A., and Schrottenloher, A.,"Reducing the Number of Qubits in Quantum Factoring," In *Annual International Cryptology Conference* (CRYPTO), August 2025, pp. 384-415, Springer Nature Cham, Switzerland.

7

7

Semiconductor QC Size since 2015

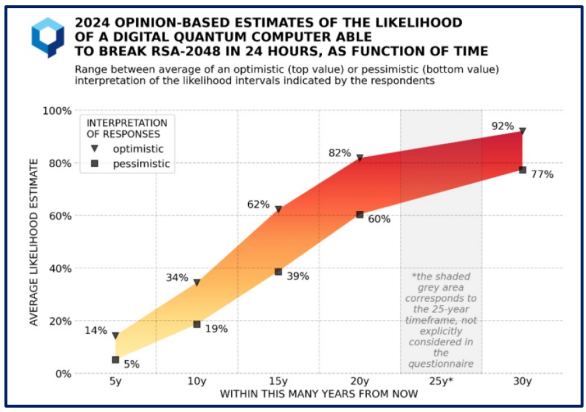


~1,000 Qubit Monolithic QPU "Limit" Reached in 2023 – Industry Focusing on Modular/3D/Chiplet Approaches
Engineering Breakthrough is Imminent – The 1,000 Qubit Barrier Will be Broken Through

8

8

When will Y2Q Day Occur?



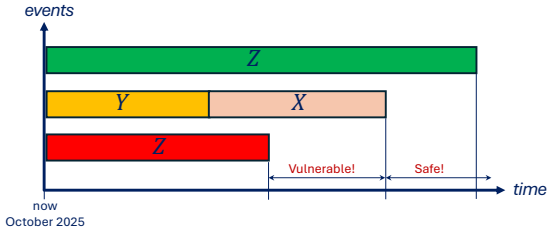
Annual Report from the Global Risk Institute

9

9

Mosca's Theorem*

- X is the length of time that your encrypted data must remain secure
- Y is the length of time to transition/deploy to operational PQC
- Z is the length of time until a CRQC is created/used to run Shor's algorithm
- Theorem: If $X + Y > Z$, then your data is no longer protected

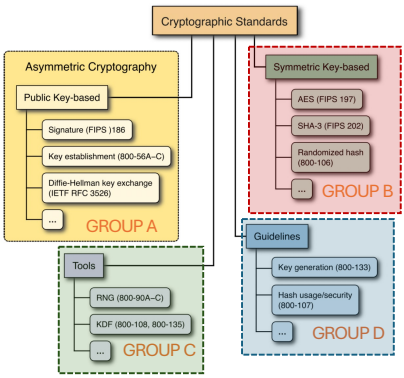


*Mosca, oral presentation, Setting the scene for the ETSI quantum-safe cryptography workshop, in e-proceedings of 1st Quantum-Safe-Crypto Workshop, Sophia Antipolis 2013 Sept. 26, 2013, pp. 26-27.

10

10

NIST Standardized Classical Cryptographic Methods



- **GROUP A**: Vulnerable, Need to be Replaced
- **GROUP B**: Somewhat Vulnerable, Double Key Sizes (at least)
- **GROUP C**: Will Need to be Updated or Replaced
- **GROUP D**: Will be Updated in Accordance with Transition Changes

- *Group A*: Asymmetric: RSA-2048, **Requires ~1M Qubits**
  - CRQC Executing Semiprime Factoring Algorithm (Shor's)
  - ~1,730 Logical Qubits (500 to 5,000 Physical Qubits per Logical Qubit)
  - **Algorithm Requires ~40 Runs** (Comprises 2^{36} Toffoli Gates)
- *Group B*: Symmetric: AES-128, **Requires ~200k Qubits**
  - CRQC Executing Shared Key Search (Grover's)
  - ~264 Logical Qubits for Grover Oracle (Reversible AES-128 circuit)
  - **Algorithm Requires 2^{64} AES Runs** (halves security; 2^{128} For Exhaustive Search)
- *Group B*: Symmetric: AES-256, **Requires ~1M Qubits**
  - CRQC Executing Shared Key Search (Grover's)
  - ~1,300 Logical Qubits for Grover Oracle (Reversible AES-256 circuit)
  - **Algorithm Requires 2^{128} AES Runs** (halves security; 2^{256} For Exhaustive Search)

*NIST, "Migration to Post-Quantum Cryptography Quantum Readiness: Cryptographic Discovery, Volume B: Approach, Architecture, and Security Characteristics of Public Key Application Discovery Tools," NIST SP 1800-38B, December 2023, (with annotations by M. Thornton).

11

11

Asymmetric Public Key Overview: RSA-2048

- **Public Modulus** is n (Large Semiprime Integer)
  - Modulus, n, Product of Two Large Secret Primes, (p, q) as $n = p \times q$
  - Modulus, n, is 2,048 bits in length or 617 decimal digits
- **Public Key** is (n, e) (where e is usually the value 65,537 or $64 \times 2^{10} + 1$)
  - Bitstring representing the pair comprised of the Public Modulus and the Public Exponent
- **Private Key** is Secret Exponent, d,
  - Derived from p and q via "Euler's totient function*" $\varphi(n) = (p-1)(q-1)$ where $ed \equiv 1 \pmod{\varphi(n)}$

- Factoring Modulus n to Recover p and q Allows Adversary to Compute Secret d
  - *Exponential* Worst-case Temporal Complexity to Factor n on Conventional Electronic Computer

$$O(n) = e^{\left\lfloor (1+o(1))\sqrt{(\ln n)(\ln \ln n)} \right\rfloor}$$

  - *Polynomial* Worst-case Temporal Complexity to Factor n on Quantum Computer: *Polynomial*

$$O(n) = (\log n)^3$$

*Euler's totient function, $\varphi(n)$, (or Euler's phi function) counts the integers $1 \leq k \leq n$ that are coprime to n. Rivest-Shamir-Adleman (RSA) encryption uses an Open/Public Exponent e with $GCD(e, \varphi(n)) = 1$ and computes the Secret/Private Exponent d as the modular multiplicative inverse of e modulo $\varphi(n)$ as $d \equiv e^{-1} \pmod{\varphi(n)}$.

12

12

Quantum-vulnerable Cryptography

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer	QC Threat
AES	Symmetric key	Encryption	Larger key sizes needed	Grover's Search
SHA-2, SHA-3	----------	Hash functions	Larger output needed	Grover's Search
RSA	Public key	Signatures, key establishment	No longer secure	Shor's Factoring
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure	Shor's Factoring
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure	Shor's Factoring

*U.S. NIST Report, "Report on Post-Quantum Cryptography," NISTIR 8105, April 2016, http://dx.doi.org/10.6028/NIST.IR.8105 .

13

13

Widely Deployed (Classical) Vulnerable Methods

Algorithm	Function	Specification
Elliptic Curve Diffie Hellman (ECDH) Key Exchange	Asymmetric algorithm for digital signatures/key exchange	NIST SP 800-56A/B/C
Menezes Qu Vanstone (MQV) Key Exchange	Asymmetric algorithm for key exchange	NIST SP 800-56A/B/C
Elliptic Curve Digital Signature Algorithm (ECDSA)	Asymmetric algorithms for digital signatures/key exchange	FIPS PUB 186-5
Diffie Hellman (DH) Key Exchange	Asymmetric algorithms for digital signatures	IETF RFC 3526
RSA Encryption Algorithm	Asymmetric algorithms for digital signatures/key establishment	SP 800-56B Rev. 2
RSA Signature Algorithm	Asymmetric algorithms for digital signatures/key exchange	FIPS PUB 186-5
Digital Signature Algorithm	Asymmetric algorithms for digital signatures/key exchange	FIPS PUB 186-5
Edwards-curve Digital Signature Algorithm (EdDSA)	Asymmetric algorithms for digital signatures	FIPS PUB 186-5

*NIST, "Migration to Post-Quantum Cryptography Quantum Readiness: Cryptographic Discovery, Volume B: Approach, Architecture, and Security Characteristics of Public Key Application Discovery Tools," NIST SP 1800-38B, December 2023, (with annotations by M. Thornton).

14

14

The NIST PQC Competition* – Recap of "Rounds"

NIST Publishes PQC Report (NISTIR 8105), April 2016

Round 1 Standardization Process Announced, December 2016

- 82 Received, 69 Accepted, 43 Eliminated, 26 Algorithms move to Round 2 Evaluation

Round 2, January 2019 through July 2020

- 26 Entries, 11 Eliminated, 15 Algorithms move to Round 3 Evaluation (7 "Finalists" & 8 "Alternatives")

Round 3, July 2020 – July 2022,

- 15 Entries, 11 Eliminated, 4 Finalists &◄/3 Alternates for Round 4 Evaluation
  - CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, SPHINCS+
  - Standards: CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, SPHINCS+ (Digital Signatures)
  - Alternates: BIKE, Classic McEliece, HQC and SIKE
  - (SIKE Broken in August 2022 using 1997 theorem on 10-year-old PC.)

Round 4, July 2022-present (still waiting for FIPS 206 standard), 11 Eliminated

Standards Announced, August 2024

- Standards: Crystals-Kyber (FIPS 203,ML-KEM), CRYSTALS-Dilithium (FIPS 204, ML-DSA), SPHINCS+ (FIPS 205, SLH-DSA), FALCON (FIPS 206, FN-DSA, yet to be released, *was planned to release in 2024*)
- Alternates: HQC (3/11/25, std in ~1 year), BIKE and Classic McEliece (still under consideration)

*NIST prefers the words "standardization process" instead of "competition"

15

15

Migrating to PQC is a MASSIVE Undertaking – Affects Everyone!

- Anything that Requires a Password (all but simplest electronic devices)
- Most Forms of Wired/Wireless Electronic Communication (Cell Phones, TXT, TV, Internet, Bluetooth, WiFi, Key Fobs, IoT & "Smart" devices)
- Most devices with Embedded CPUs (passwords, storage, *etc.*)
- Infrastructure: Telecommunications, Finance, Utilities
- Secure Communications (Military, Government, Industry/e-Commerce, Social Media)
- Automobiles (key fobs, SW/FW updates, OBD-II ports, *etc.*)
- Personal Devices (passwords, storage, Internet/https, email, WiFi, pay-TV, home security, voice assistants, *etc.*)
- *many others*

16

16

Making OT Quantum-safe: May be Harder than IT PQC Migration

- OT/ICS/CI/Cyberphysical Systems Rely on Cryptography for the "AIC Triad" (Availability/Integrity/Confidentiality)
  - May not Support Computation-heavy PQC and Larger Keys (lack of CryptoAgility; Obsolete Legacy Devices)
  - DS-signed Commands & FW Updates Forgery (Integrity concerns - TNFL)
  - Critical Infrastructure (CI) Affects Public Safety/Health/Welfare (Cyberkinetic concerns - People can be Injured or Worse)
  - Safety Certs./Regulatory Approvals/Extensive Testing Protocols (Government/Vendor/3rd-Party Test Coordination for PQC Migration)
  - Patching Time Windows (Availability concerns - Plant Shutdowns, Maintenance Outages)
  - CBOM Compilation is Complicated for OT (Deploying Monitoring Agents or NW Sniffers)
  - Other Issues (Out-of-Band Devices, Embedded Crypto. Primitives, Lack of Documentation, *etc.*)

17

17

How does migration to PQC affect my organization?

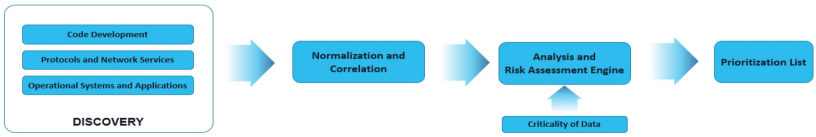
- Requires Assessment of Current Cryptographic Dependencies – "Discovery"
- Must Engage with Vendors & IT Staff to Implement New Algorithms
- May Involve Significant Investment and Infrastructure Upgrades
- PQC Standards are Not Drop-in Replacements:
  - Larger-sized keys will generally be needed
  - New PQC Codes Require Support (*eg.*, high-quality & high-throughput RNG/RBG Entropy Sources)
- May Affect Other Systems:
  - Disaster recovery
  - Interfaces with other organizations
  - Dual-support (classical/PQC) during transition within outside entities

18

18

NIST PQC Migration Project*: Discovery, Interoperability, Performance

- **Discovery**: Use of tools to detect/report presence/use of quantum vulnerable cryptography to inform risk and remediation



- **Interoperability**: Identifying interoperability/performance challenges that applied cryptographers face when implementing NIST standardized PQC algorithms
- **Performance**: Compare algorithms (not the implementation) by independent testing. Document relative costs of using pure or hybrid PQC algorithms with classic algorithms as baseline across various implementations.
- NIST Collaborating with 26 Technology Vendors under a CRADA in Response to Open Call in the Federal Register

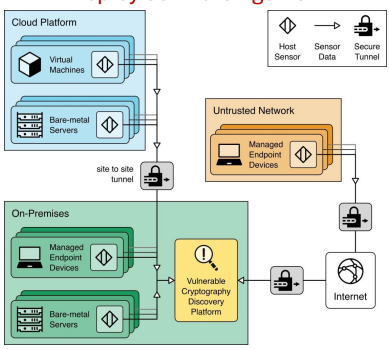
*NIST, "Migration to Post-Quantum Cryptography," https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms, (last accessed, March 18, 2025.

19

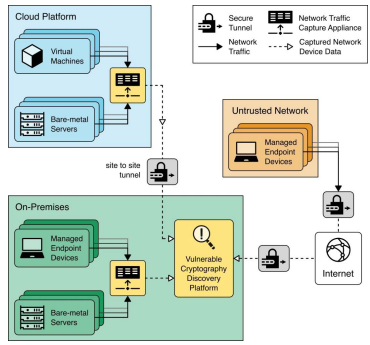
19

Discovery Approaches

Deploy Software Agents



Network Monitors



*NIST, "Migration to Post-Quantum Cryptography Quantum Readiness: Cryptographic Discovery, Volume B: Approach, Architecture, and Security Characteristics of Pulic Key Application Discovery Tools," NIST SP 1800-38B, December 2023, (with annotations by M. Thornton).

20

20

Discovery: Cryptographic Bill of Materials (CBOM)

- *More than a "List*:" CBOM is Collection of DB Records Containing Cryptographic SW Component Details Needed for Migration
- *CBOM Creation Challenges*: API Variability, Data Flow Complexity, API Modeling Scope, Abstraction Unification, *etc*.
  Example "Data Flow Complexity:"
  - Need to Trace Data Source Paths to Data Sinks in Configuration
  - Configuration Could Be Root-of-Trust, Initialization Vector, Key Size, Algorithm Specification, *etc*.
  - These Challenges Could Require Inter-procedure Analysis in Large Systems

21

21

PQC Migration Approach – Global Risk Institute

- **Phase 1** - Identify and document information assets, and their current cryptographic protection.
- **Phase 2** - Research the state of emerging quantum computers and quantum-safe cryptography. Estimate the timelines for availability of these technologies. Influence the development and validation of quantum-safe cryptography.
- **Phase 3** - Identify threat actors and estimate their time to access quantum technology, Z.
- **Phase 4** - Identify the lifetime of your asset's X, and the time required to transform the organization's technical infrastructure to a quantum-safe state, Y.
- **Phase 5** - Determine quantum risk by calculating whether business assets will become vulnerable before the organization can move to protect them, ($X + Y > Z$?)

*Mosca, *et. al*., oral presentation, "A Methodology for Quantum Risk Assessment," Global Risk Institute, 2021.

22

22

PQC Migration Approach – US Dept. Homeland Security

1) Is the system a high-value asset based on organizational requirements?
2) What is the system protecting (e.g., key stores, passwords, root keys, signing keys, personally identifiable information, sensitive personally identifiable information)?
3) What other systems does the system communicate with?
4) To what extent does the system share information with federal entities?
5) To what extent does the system share information with other entities outside of your organization?
6) Does the system support a critical infrastructure sector?
7) How long does the data need to be protected?

*U.S. Dept. Homeland Security, Preparing for Post-Quantum Cryptography, October 202, https://www.dhs.gov/sites/default/files/publications/post-quantum_cryptography_infographic_october_2021_508.pdf.

23

23

"Crypto-Agility" and Hybrid Approaches

- "Crypto-agility" is the Ability to Easily Replace One Cryptographic Method with Another
- The Defeat of SIKE Soon After it was Chosen by NIST Underscores this Need
  - May Decide to Incorporate Crypto-Agility in your PQC Transition Process
- Lack of Current Crypto-Agility Underscores the Need to Start PQC Transition Process Now
  - Consider Implementing Crypto-Agility in the PQC Migration Process
- Hybrid Approaches Use Classical and PQC Methods Together to Reduce Risk if One is Broken
- Interoperability and Connectivity will be Challenging During the PQC Transition
  - Inadvertent Cyber Security Vulnerabilities Could Surface During PQC Transition
- NIST Plans to Provide Transition Guidance

24

24

Quantum Technology be Leveraged to Improve Security

- PQC Requires Enhanced Security Infrastructure: Not Just an "Algorithm Swap"
  - Enhanced Entropy Generators (RNG/RBG)
  - Alternative Roots-of-Trust (Photonic PUF)
- Current SMU/DDI Projects Relevant to PQC and Quantum Security
  - Post-Quantum Secure/Crypto Agile "Zero-Knowledge Proofs" (ZKP) Enhance Conventional/PQC Digital Signatures
  - PQC Attack Surface Investigations (Degraded Entropy analysis for SLH-DSA (SPHINCS+))
  - Single-chip Solutions: QRNG (Patented/Licensed) & Photonic PUF (Patented/Licensed)
  - Reconfigurable Quantum Photonic Integrated Circuits (QPIC) – High-Dimensional Sponsored by DARPA+Industry
  - PQC ML-KEM (CRYSTALS-Kyber) Ported to FPGA ARM64 core and Performance Profiled
  - QPIC Design Automation Tools Sponsored by Industry
  - Quantum Key Distribution (QKD): Current Investigation & Recent Past Performance Sponsored by DARPA+Industry
    - QKD Supports Legacy Crypto + PQC with your existing fiber networks
  - *Numerous Other Past Projects*

25

25

5 Reasons that PQC Migration is Urgent

1) **HNDL** (*harvest now, decrypt later*) –This Happening Right Now!
   - Confidentiality threat!!! Sensitive data encrypted-at-rest (health, gov. secrets, IP, PII, …)
2) **TNFL** (*trust now, forge later*) – Digital Signature Version of HNDL
   - DS use RSA/ECDSA for SW/FW updates, Identity, Financial transactions
   - CRQC Enables Adversaries to Forge all these Signed Documents

Exemplary Large Datacenter

3) **Compliance Deadlines** (*PQC Migration*)
   - 2030 for National Security Systems (CNSA 2.0)
   - 2035 Recom. for Federal Civilian Agencies; Crypto Inventory Now (annually per OMB memo M-23-02)
   - No Blanket Federal Mandate for Critical Infrastructure/Private Sector (*yet*), but DHS is Asking for PQC Migration Planning Now (CISA PR 6/6/22 PQC Initiative)
4) **Hybrid Cryptography** (*Deploy PQC+Classical Crypto. Support*)
   - Private/Gov/Comm Entities will NOT all Migrate to PQC Simultaneously – Matter of Business Continuity
5) **CryptoAgility** (*Ability to Easily/Quickly Swap Crypto. Algorithms and Infrastructure*)
   - Crypto. Migration Almost Certain to Occur Again (*eg*. SIKE KEM NIST endorsed 7/22 – classically broken 8/22)
   - True Quantum Cryptography widely Predicted to Replace new PQC Standards

26

26