REGIONAL SDC 25

BY Developers FOR Developers

Regional SDC Denver
April 30, 2025

Post-Quantum Cryptography Update

Paul Suhler
KIOXIA Corporation
Chair, IEEE Security In Storage Working Group

SNIA

Introduction

- This presentation describes the upcoming transition from cryptographic algorithms currently in use to algorithms that are resistant to attacks by quantum computers.
- The listener should take away a high-level understanding of the changes that will take place in storage devices, hosts, and communication protocols.
- This presentation provides links to the relevant standards.

Overview

- Background: Uses of Cryptography
- The Quantum Cryptography Problem
- Threats and Solutions
- Post-Quantum Cryptography (PQC) Transition
- Other Standards
- Summary of Standardization Activities
- Calls to Action

Background: Uses of Cryptography

- Data encryption is at the heart of online communication and data protection.
  - Identity is proven, data is encrypted, encryption keys are encrypted.
- Data is typically encrypted with “symmetric” encryption algorithms (the same key is used for encryption and decryption).
  - Example: Advanced Encryption Standard (AES) algorithm for stored data (IEEE 1619 XTS-AES) and transmitted data (TLS).
- Encryption keys are encrypted (wrapped) for sharing using a public key infrastructure (PKI); these are “asymmetric” encryption algorithms.
  - Example: Rivest-Shamir-Adelman (RSA) algorithm.
- PKI is also used to prove the identities of people sharing information.
- These are used to protect data from breaches that can reveal critical information and incur financial penalties.

REGIONAL SDC

The Quantum Cryptography Problem

- Cryptographically-relevant quantum computers are being developed.
- Quantum algorithms that break classical encryption already exist.
- Quantum-resilient algorithms (post-quantum cryptography – PQC) have been developed to protect against attacks using quantum computers.
- Computer security systems must transition from classical algorithms to quantum-resilient algorithms.

- The transition must happen before Q-Day.

REGIONAL SDC

Threats and Solutions

- Harvest now, decrypt later:
  - Encrypted data and wrapped keys can be copied in flight and encrypted disks can be lost or stolen.
  - Later, encrypted keys will be unwrapped and encrypted data decrypted.
- Asymmetric encryption (e.g., RSA) is the most vulnerable (Shor's Algorithm).
  - Solution: Transition to post-quantum cryptographic (PQC) algorithms.
- Symmetric algorithms (e.g., AES) are less vulnerable.
  - Solution: Transition to using the longest existing key length (256 bits).

Post-Quantum Cryptography (PQC) Transition

- US government has set deadlines for support by products used in national security systems (NSS).
- Commercial National Security Algorithm (CNSA) Suite 2.0 specifies PCQ algorithms to use.
- European Union Agency for Cybersecurity (ENISA) timeline is roughly aligned.
- PQC algorithms are defined in other standards.

PQC Adoption Timeline for National Security Systems

- Committee on National Security Systems Policy 15 (CNSSP 15):
  - By 1 January 2027, all new acquisitions must be CNSA 2.0 compliant.
  - By 31 December 2030, equipment & services not supporting CNSA 2.0 must be phased out.
  - By 31 December 2031, CNSA algorithms must be used.
  - Transition to QR algorithms for NSS to be complete by 2035.

  Cryptographic agility: Equipment pre-dating the required support date must be able to run new algorithms and to be updated to future algorithms.
- For details see:
  - NIST IR 8547 (Initial Public Draft) Transition to Post-Quantum Cryptography Standards , Nov. 2024
  - The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ, Dec. 2024, Ver. 2.1.

REGIONAL SDC

CNSA 2.0 Requirements

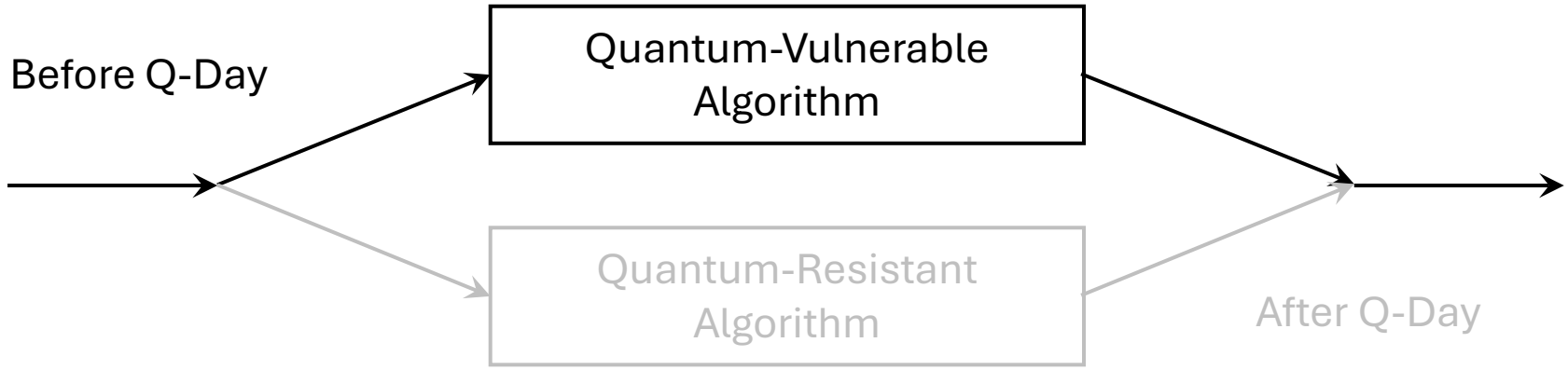
- Applies to National Security System (NSS) owners and operators (and vendors).
- Includes algorithms resistant to attacks by cryptographically relevant quantum computers.
  - RSA, finite-field Diffie-Hellman (DH), and elliptic curve cryptography (ECDH and ECDSA) are deprecated.
  - FIPS 197 – Advanced Encryption Standard is constrained: 256-bit keys required (128-bit and 192-bit keys deprecated)
  - FIPS 202 - SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions: For hardware integrity checks only.
  - FIPS 203 – Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM).
  - FIPS 204 – Module-Lattice-Based Digital Signature Standard (ML-DSA).
  - FIPS 180-4 – Secure Hash Standard (SHS): SHA-384 and SHA-512 are allowed.
  - SP 800-208 - Layton-Micali Signature (LMS) and Xtended Merkel Signature Scheme (XMSS) for signing firmware and software. (HSS and XMSSMT are not allowed.)
- Original candidate algorithms went by the names CRYSTALS-Kyber and CRYSTALS-Dilithium. The standardized algorithms differ. Use the FIPSes above for implementation.

REGIONAL SDC

Transitioning to Quantum-Resistant Algorithms

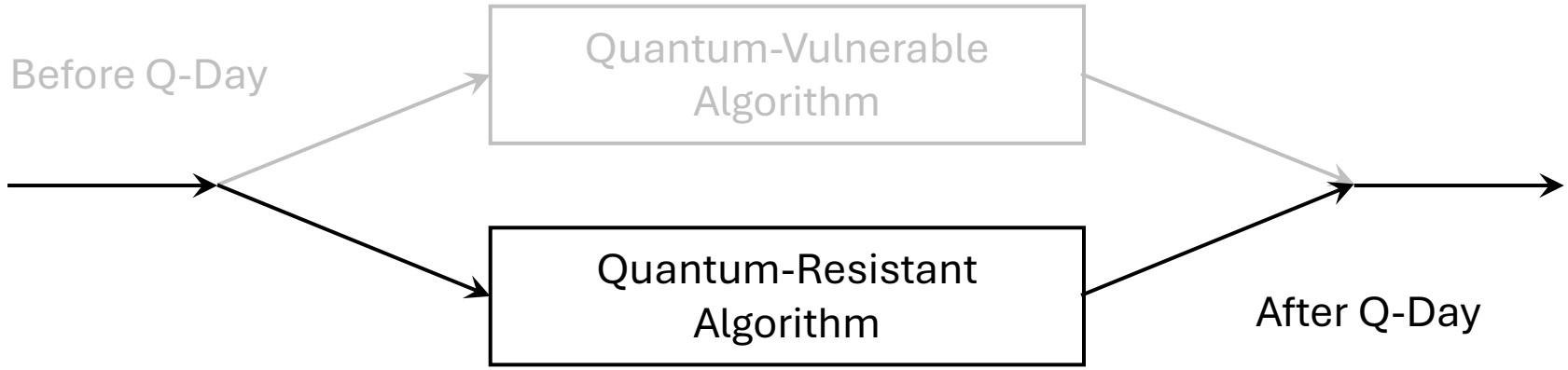
- PCQ keys are large and will be integrated into certificates and protocols, for example:
  - Certificate signing
  - TLS key exchange
- How to allow PQC and non-PQC devices to interoperate during the transition period? Two schemes:
  - Switch deployed products from quantum-vulnerable algorithms to quantum-resistant algorithms before Q-Day.
  - Deploy products with hybrid algorithms.

Transition: Switch Algorithms in the Field



- Implement both vulnerable and resistant algorithms.
- Change to quantum-resistant algorithms before the deadline, and do not return to vulnerable algorithms.
- But if a QR algorithm is broken, returning to a vulnerable algorithm would at least protect against non-quantum cryptographic attacks.
- No standard API exists to perform switching.

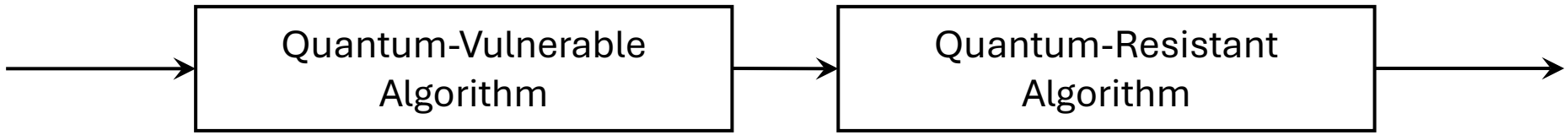
Transition: Switch Algorithms in the Field



- Implement both vulnerable and resistant algorithms.
- Change to quantum-resistant algorithms, and do not return to vulnerable algorithms.
- But if a QR algorithm is broken, returning to a vulnerable algorithm would at least protect against non-quantum cryptographic attacks.
- No standard API exists to perform switching.

REGIONAL SDC

Transition: Implement Hybrid Algorithms



This is not a literal representation of how the algorithms are applied.

- Data is encrypted with both a vulnerable algorithm and a resistant algorithm.
- If either algorithm is broken, then data retains the protection of the other algorithm.
- Cost and performance penalties apply.

REGIONAL SDC

Hybrid Algorithms

- NIST is not yet standardizing hybrid algorithms.
- NIST Cryptographic Algorithm Validation Program (CAVP) will validate individual algorithms, not hybrid algorithms.
- Expect guidance from the NIST Cryptographic Module Validation Program (CMVP) and from validation labs.
- Most work is being done by the Internet Engineering Task Force (IETF).
  - Post-Quantum Cryptography Recommendations for TLS-based Applications
  - Hybrid key exchange in TLS 1.3
  - Enhancing Security in EAP-AKA' with Hybrid Post-Quantum Cryptography
  - Terminology for Post-Quantum Traditional Hybrid Schemes

Other Standards

- DMTF (formerly the Distributed Management Task Force)
  - Security Protocols and Data Models (SPDM) 1.4.0 will probably add FIPS 203 ML-KEM and FIPS 204 ML-DSA by mid-2025. (DSP0274)
- Trusted Computing Group (TCG)
  - Device Identifier Composition Engine (DICE)
  - Core architecture
  - Opal family of standards
  - Enterprise SSC
  - Key Per I/O

Cryptographic Module Validation Program FIPS 140

- NIST CMVP certification to FIPS 140:
  - FIPS 140-3 is based on ISO/IEC 19790:2012.
  - ISO/IEC 19790:2025 was published in February 2025
  - FIPS 140-4 may modify some requirements of 19790:2025.

Summary of Standardization Activities

- A sufficient set of PQC algorithms has been standardized.
  - Work on future algorithms continues.
- The focus is on updating protocols to use PQC algorithms (TLS, SPDM, DICE, etc.)
  - Also: Secure Shell (SSH), Internet Protocol Security (IPsec), and Cryptographic Message Syntax (CMS).
- Libraries will be updated:
  - OpenSSL, BoringSSL, Libsodium, Java Cryptography Architecture (JCA), etc.

Call to Action – Consumers

- Understand how your providers will meet PQC requirements.
- Understand their plans to transition from quantum-vulnerable to quantum-resistant (PQC) algorithms.
- Monitor execution of the plan.

Call to Action – Providers

- Understand the standards that affect your products.
- Develop a plan to transition from quantum-vulnerable to quantum-resistant (PQC) algorithms.
- Align vendor and customer requirements.
- Execute the plan to meet the timelines.

Thank You