Securing Critical Infrastructure with Quantum-Resistant Cryptography

Getting Ready for the Post Quantum Cryptography Threat? You Should be.

The U.S. National Institutes of Science and Technology (NIST) initiated a Post Quantum Cryptography (PQC) program in 2016. The U.S. government is mandating their agencies to harden critical networks against quantum-computer vulnerabilities before 2027. Industry also will need to be doing this migration. The migration is not going to be easy or pain free. There isn't a consensus amongst security professionals on the size of the threat, but NIST estimates that perhaps 20 billion devices within the U.S. will need to be updated with Post-Quantum Cryptography (PQC), safeguarding.

The goal of PQC, also called quantum-resistant cryptography (QRC), is to develop cryptographic systems that are secure against both quantum and classical computers and can interoperate with existing communications protocols and networks.

The term 'quantum computer' means a computer utilizing the collective properties of quantum states, such as superposition, interference, and entanglement, to perform calculations. The foundations in quantum physics give a quantum computer the ability to solve a subset of hard mathematical problems at a much faster rate than a classical (i.e., non-quantum) computer.

Today, it is understood that Advanced Persistent Threat (APT) actors are actively collecting, or "scraping," as much encrypted data as they can in hopes that the future availability of quantum computers will enable them to read all gathered encrypted data later. This "Harvest Now, Decrypt Later" (HNDL) activity isn't just a concern for secret government networks. For example, a Cryptanalytically Relevant Quantum Computer (CRQC) will essentially break HTTPS, impacting all communication and commerce across the Internet.

Contents

> “This advisory notifies NSS (National Security Systems) owners, operators, and vendors of future requirements for quantum-resistant (QR) algorithms for NSS. These algorithms (also referred to as post-quantum algorithms) are analyzed as being secure against both classical and quantum computers. They are an update to those in the Commercial National Security Algorithm Suite (referred to as CNSA 1.0, the algorithms currently listed in CNSSP 15, Annex B). The National Security Agency (NSA) will reference this update as CNSA Suite 2.0, and any future updates will modify the version number.”

The goal of PQC, also called quantum-resistant cryptography (QRC), both referring to the same concept: cryptographic algorithms designed to remain secure even when facing attacks from powerful quantum computers; essentially, they are methods for encryption that can withstand the potential decryption capabilities of future quantum computing technology., secure against both quantum and classical computers and facilitate transition of existing communications protocols and networks

Commercial National Security Algorithms (CNSA) Suite 2.0

For the protection of TOP SECRET data-at-rest (DAR), the National Security Agency (NSA’s) Commercial Solutions for Classified (CSfC) program specifies the Commercial National Security Algorithm (CNSA) Suite. The CNSA Suite is a set of commercial algorithms that includes cryptographic algorithms for confidentiality, key exchange, digital signature, and hashing capable of protecting data through the TOP SECRET level. Currently, CNSA Suite 1.0 from DAR Capability Package, Version 5.0, November 2020, Section 4.4, Page 12 specifies the following CNSA 1.0 algorithms:

Algorithm	Function	Specifications	Parameters
Advanced Dncryption Standard (AES)	Summetric block cipher for information protection	FIPS PUB 197	Use 256-bit keys for all classification levels
Elliptic Curve Diffie-Hellman (ECDH) Key Exchange	Asymmetric algorithm for key establishment	NIST SP 800-56A	Use Curve P384 for all classification levels
Elliptic Curve Digital Signature Algorithm (ECDSA)	Asymmetric algorithm for digital signatures	FIPS PUB 186-4	Use Curve P384 for all classification levels
Secure Hash Algorithm (SHA)	Algorithm for computing a condensed representation of information	FIPS PUB 180-4	Use SHA-384 for all Classification levels
Diffie-Hellman (DH) Key Exchange	Asymmectric algorithm for key establishment	IETF RFC 3526	Minimum 3072-bit modulus for all classification levels
RSA	Asymmectric algorithm for key establishment	FIPS SP 800-56B	Minimum 3072-bit modulus for all classification levels
RSA	Asymmectric algorithm for key establishment	FIPS PUB 186-4	Minimum 3072-bit modulus for all classification levels

Moreover, the NSA has released the CNSA 2.0 detailing future Quantum Resistant (QR) algorithm requirements for National Security Systems (NSS). CNSA 1.0 was published in 2016 to replace NSA Suite B and standardized the use of the AES, SHA, RSA, DH, ECDH, and ECDSA algorithms and mandated minimum key/curve sizes and uses. CSNA 2.0 adds quantum resistant algorithms with an eye to deprecating the algorithms under threat from practical quantum computing before such platforms are generally available.

These new QR algorithms replaces the RSA and ECC-based algorithms currently used by most products in Common Criteria evaluations. When Automated Cryptography Validation Test System (ACVTS) tests are implemented for these new algorithms, they will be added as selections in NIAP-approved Protection Profiles. Products to be evaluated must implement these new algorithms by the time they are made mandatory, and their counterparts deprecated.

Symmetric algorithms are not considered to be at risk, so they are largely unchanged from CNSA 1.0. CNSA 2.0 specifies AES-256, SHA-384, and adds SHA-512. Asymmetric algorithms specified in CNSA 1.0 are threatened by quantum computing and therefore are replaced by new QR asymmetric algorithms in CNSA 2.0.

Note this will effectively deprecate the use of RSA, Diffie-Hellman (DH), and elliptic curve cryptography (ECDH and ECDSA) when mandated. NSA urges NSS owners and operators to pay special attention to these requirements. In the interim, CNSA 1.0 compliance continues to be required. Below are CNSA 2.0 Algorithms for Digital Signatures.

Algorithm	Function	Specification	Parameters
CRYSTALS-Kyber	Asymmetric algorithm for key establishment	TBD	Use level V parameters for all classification levels
CRYSTALS-Dilithium	Asymmetric algorithm for digital signatures	TBD	Use level V parameters for all classification levels

Public-key Algorithms

Public Key Infrastructure (PKI) is foundational to securing digital communications, relying on cryptographic algorithms like RSA and ECC to establish trust and confidentiality. However, the advent of quantum computing introduces significant vulnerabilities to these systems. Quantum computers, leveraging algorithms such as Shor's, can efficiently solve the mathematical problems underpinning RSA and ECC, rendering them susceptible to rapid decryption. This capability threatens the integrity of PKI, as encrypted data and digital signatures could be compromised, undermining the security of sensitive communications and transactions.

The potential for quantum computers to break current cryptographic algorithms poses a critical risk to PKI-dependent systems. Adversaries could exploit quantum capabilities to decrypt intercepted communications, forge digital signatures, and impersonate legitimate entities, leading to breaches in confidentiality, authentication, and data integrity. This vulnerability extends to various sectors, including finance, healthcare, and national security, where PKI is integral to protecting sensitive information and ensuring secure operations.

Traditional PKI systems rely on algorithms like RSA and ECC, which are vulnerable to quantum attacks capable of compromising key exchanges and digital signatures. Isidore Quantum mitigates these risks by implementing a CNSA 2.0-compliant framework that leverages quantum-resistant algorithms, such as CRYSTALS-Kyber for key management and AES-256 for encryption. This approach ensures that even with the advent of quantum computing, the cryptographic integrity of communications remains intact.

Intersection with Zero Trust

While CNSA 2.0 equips critical infrastructure with the necessary cryptographic tools to defend against quantum computing threats, the integration of Zero Trust principles ensures that these tools are deployed within a secure and resilient framework. This combined approach addresses both the cryptographic and architectural aspects of security, providing a comprehensive defense strategy against the multifaceted challenges posed by quantum computing advancements.

Zero Trust is a cybersecurity paradigm that operates on the principle of "never trust, always verify." Unlike traditional security models that assume trustworthiness for users and devices within a network perimeter, Zero Trust requires continuous authentication and authorization for every access request, regardless of the user's location or device. This approach ensures that no implicit trust is granted based solely on network location or asset ownership, thereby enhancing security across the entire network infrastructure.

A key component of Zero Trust is the principle of least privilege access, which limits users' access rights to only what is necessary for their roles. In the context of critical infrastructure, this means that operators and systems have access only to the specific functions they need to perform their duties, minimizing the potential impact of compromised credentials. By enforcing strict access controls, Zero Trust helps prevent lateral movement within the network, thereby containing potential breaches and protecting sensitive operational technology (OT) environments.

Moreover, Zero Trust emphasizes continuous monitoring and validation of user and device identities. In critical infrastructure sectors, this continuous verification is crucial for detecting and responding to anomalies or unauthorized activities in real-time. By requiring continuous validation of user and device identities, Zero Trust ensures that even if quantum-resistant algorithms are in place, access to critical infrastructure remains tightly controlled and monitored.

Isidore Quantum® makes transition to post-quantum security effortless with an elegant, scalable, plug-and-play design that is 75% faster to implement, and 60% more cost-effective to own and operate than traditional solutions that are not quantum-ready.

Challenges and Considerations in Post-Quantum Cryptography for Data-in-Transit

After the September 2022 NIST announcement, a second batch of four algorithms were under consideration for NIST approval, including the Supersingular Isogeny Key Encapsulation (SIKE). SIKE is a family of post quantum key encapsulation mechanisms based on the Supersingular Isogeny Diffie-Hellman (SIDH) key exchange protocol.

Using only a single-core personal computer, SIKE was easily broken just one hour after its release. The fact that SIKE was solved so quickly raises a general concern that CRYSTALS-Dilithium, one of three algorithms believed to be cryptographically sound, along with Falcon and SPHINCS+, that NIST has selected for use in digital signatures, has not yet faced first contact with APT actors.

Today's best understanding of the threat to data security, combined with mathematical analysis, clearly shows that the pre-shared key (PSK) symmetric encryption approach is quantum-resistant, and the NSA's current guidance is to use a PSK system. According to the NSA, using pre-shared symmetric keys in a standards- compliant fashion provides a better near-term post- quantum solution than implementing experimental post-quantum asymmetric algorithms possibly incompatible with NIST standards. Eventually, the NSA will provide capability packages that coincide with commercial technological development to implement CNSA 2.0 algorithms.

Transition to Quantum-Resistant Cryptography for Data-in-Transit

Isidore Quantum® was invented by the NSA and licensed to Forward Edge-AI to improve and manufacture. The Isidore Quantum® device is compliant with CNSA 2.0 and offers a robust solution to the challenges discussed here.

Isidore Quantum incorporates CNSA 2.0-approved algorithms, such as CRYSTALS-Kyber for key encapsulation and CRYSTALS-Dilithium for digital signatures. A notable feature of Isidore Quantum is its autonomous key and channel management system. This system facilitates periodic rekeying, key recovery, and zeroization without manual intervention, ensuring continuous security and reducing the risk of key compromise. Such automation is crucial for maintaining secure communications in dynamic and high-risk environments.

Isidore Quantum also operates on a zero-trust model, meaning it does not inherently trust any device or user, regardless of their location within the network. This approach ensures that every access request is authenticated and authorized, minimizing the risk of unauthorized access and lateral movement by potential adversaries.

Designed to be protocol, device, and network agnostic, Isidore Quantum can be integrated into existing critical infrastructure without significant modifications. Its plug-and-play design allows for rapid deployment, enabling organizations to enhance their security posture promptly in response to evolving quantum threats.

Isidore Quantum® also incorporates a highly performant Rules Engine to detect and address known threats, and Machine Learning algorithms to learn the patterns of daily life, detect anomalies that may signal a novel attack, execute a cyber-immune response, and recover stronger because it has learned from the previous attack.

By deploying Isidore Quantum devices, organizations can proactively, and cost effectively harden their critical infrastructure against the anticipated capabilities of quantum computers. This forward-looking approach addresses current security challenges while ensuring resilience against future quantum advancements, safeguarding essential services and national security interests.

Isidore Quantum® Advantages

Criteria	Classic/Legacy Solutions	Isidore Quantum®
Confidentiality, Integrity, Availability (CIA)	Does not obscure traffic or geolocation, not quantum-resistant, does not autonomously respond to attacks	Quantum resistant (CNSA2.0), artificially intelligent. Proposed DP2 adaptations will obscure traffic and geolocation
Architecture	(IP specific) suited when dynamic security associations is required	(Protocol agnostic) designed for moderate topologies. Capable of mesh, hub and spoke, point to point/multi-point
Keying Methodology	PKI, certificate authority required, and not adequate against quantum attacks	PKI/KMI and certificate authorities not required. Ephemeral keying algorithms
Operational Security	Easy to detect and geolocate devices	No forensic footprint
Power/Throughput	30 Watts/1GB/s	3 Watts/1GB/s
Form Factor	Half brick sized, 4.4 pounds	Credit card sized, 0.2 pounds
Ease of use	Controlled item (crisis if lost), requires skill to integrate, operate and maintain	Non-CCI, set and forget, as easy as an ATM machine to use, no integration
Price	**$7,600 - $75,000**	**$1,600**

Originally invented by the NSA, Isidore Quantum® offers a comprehensive solution by integrating advanced cryptographic techniques and robust security architectures tailored for edge environments.\

Beyond its cryptographic strengths, Isidore Quantum adheres to Zero Trust principles, enforcing continuous authentication and authorization for all access requests. This approach mitigates risks associated with classical cybersecurity threats, such as unauthorized access and lateral movement within networks. Additionally, Isidore Quantum's autonomous key and channel management system facilitates periodic rekeying and key recovery without manual intervention, enhancing operational security and reducing the likelihood of key compromise. These features collectively make Isidore Quantum a robust and adaptable solution for securing edge devices in the face of evolving cyber threats. Technological and operational advantages include:

> **"There is nothing in our portfolio that is high assurance, low cost, easy to own, future proof, easy to certify, scalable to multiple form factors, and non-Controlled Cryptographic Item (CCI)"**
>
> Andy White
>
> National Security Agency, June 2022

Technology Advantages:

- Self isolating/zero trust by default
- Protocol, network, and end user hardware agnostic
- Learns the patterns of daily life, detects attacks, executes a cyber-immune response, and recovers stronger using machine learning and rules engine

Operational Advantages:

- Affordable/low cost
- Eliminates the need for PKI/KMI and certificates, reduces cognitive load and labor
- Deployable and disposable crypto, does not require key loaders
- Light touch, easy to set up, easy to own, and future proof

Appendix A

Acronyms

AES	Advanced Encryption Standard CQTS
	Cross-Quantum Technology Systems
CRQC	Cryptoanalytically-Relevant Quantum Computer CSfC
	Commercial Solutions for Classified
HiPS	High-Performance Superconducting Qubit Systems HNDL
	Harvest Now, Decrypt Later
LPS	Laboratory for Physical Sciences LWE
	learning-with-errors
NEQST	New & Emerging Qubit Science & Technology NIST
	National Institute of Science and Technology NQCO
	National Quantum Coordination Office
NSA	National Security Agency NSS
	National Security Systems
PKI	Public-key Infrastructure, asymmetric encryption scheme, two different keys are used to encrypt/decrypt PQC
	Post-Quantum Cryptography
PSK	Pre-shared key, symmetric encryption scheme, same key is used to encrypt/decrypt QC
	Quantum Computer
QCISS	Quantum Characterization of Intermediate-Scale Systems QIS
	Quantum Information Science
QiS	Qubits in Silicon Program
QR	Quantum-Resistant (algorithms)
QRC	Quantum-Resistant Cryptography
SHiFT	Stable High Fidelity Trapped Ion Systems SIS
	short integer solution

.