Post-Quantum Cryptography and Self-Encrypting Drives

Post-Quantum Cryptography (PQC) – also known as quantum resistant cryptography – is an effort to define new cryptographic primitives and algorithms that can withstand attacks using quantum computers. Currently it is unclear when quantum computers can weaken or break current data security implementations as a practical attack implementation requires a quantum computer with many stable qubits. Although the fundamentals are understood, the engineering challenge is still significant. Both the uncertainty of when practical quantum computers are available and the time it takes to update deployed crypto systems requires risk mitigation. This was clearly understood in 2016 when the National Institute of Standards (NIST) started the official process to define new PQC standards.

The threat is that data protected with classical cryptography is stored off-line until large quantum computers are available, compromising the security of that data over time. High-level, two algorithms optimized for quantum computers can put classical cryptography at risk: an implementation of Shor's algorithm to break asymmetric key cryptography and – to a lesser degree – the use of Grover's algorithm to lower the security of symmetric key encryption.

“Shor’s Algorithm” can factor complex numbers and solve discrete logarithm problems, thereby putting existing asymmetric key cryptography, e.g., RSA and ECC, at risk. As such, these asymmetric key schemes are considered insecure against quantum attacks. On the other hand, Grover's quantum search algorithm provides a fast search mechanism that likely threatens symmetric key cryptography and cryptographic hash functions. By estimation, it halves the strength of AES cryptography, thereby dropping AES-128 bits encryption to about 64-bits of security. For symmetric key encryption, AES-128 is considered insecure against quantum attacks (yet still secure from attacks using classical computers), whereas AES-256 is considered secure and quantum resistant. Similarly, the hash algorithms SHA-384 and SHA-512 are considered quantum resistant.

PQC Standardization Process

NIST’s standardization process for PQC aims to develop new cryptography that is secure against attacks that use both quantum and classical computers. The effort officially started in 2016 when NIST published a request for proposals of new PQC algorithms. Due to the theoretical nature of quantum computers at that time, NIST wanted to mitigate the risk by looking for a broad set of different PQC techniques. The call for proposals started the first round of – what is known as – the PQC competition and by November 2017 NIST had accepted 69 candidate submissions. In July 2020 second-round candidate algorithms were announced and in July of 2022 the finalists for standardization were selected. Alongside the finalists, a set of alternate algorithms were advancing to a fourth round for ongoing evaluation, with the intend to add to the PQC standards over time.

In August 2023 NIST published three draft standards for public comment and almost exactly one year later, on August 13, 2024, NIST released the official standards. The newly created standards are: FIPS 204 “Module-Lattice-Based Digital Signature Standard” and FIPS 205 “Stateless Hash-Based Digital Signature Standard” for signatures, and FIPS 203 “Module-Lattice-Based Key-Encapsulation Mechanism Standard” for key exchange. Two of the three FIPS standards define a PQC resilient version for digital signatures (based on the CRYSTALS-Dilithium and SPHINCS+ candidate

algorithms), with the third FIPS standard providing a PQC resilient shared secret key establishment scheme over a public channel (based on the CRYSTALS-Kyber candidate).

Implications for Data Security and Self-Encrypting Drives

On September 7, 2022, NSA released the "Commercial National Security Algorithm Suite 2.0" (CNSA 2.0) Cybersecurity Advisory*). It provides a first clear guidance on the timing for implementing quantum resistant cryptography in the context of US national security systems. The advisory recognizes that – at the time of publishing – NIST was still working on finalizing PQC standards. Nevertheless, it put manufacturers of computer systems and components on notice to start planning for the PQC transition.

For manufacturers of Self-Encrypting Drives (SEDs), the overall CNSA 2.0 guidance applies to three areas of the device's security implementation:

1. It requires AES-256 for data confidentiality;
2. The need to transition to NIST FIPS 204 for integrity protection (e.g., digital signatures used for firmware integrity and secure boot);
3. The use of SHA-384 or SHA-512 for cryptographic hashes per NIST FIPS PUB180-4.

Additionally, when applicable, use FIPS 203 key exchange in secure messaging channels.

Interesting side note: at the time of publication CNSA 2.0 recommended the LMS or XMSS algorithms defined in NIST SP 800-208 "Stateful Hash-Based Signature Schemes" for firmware and software signing. Reasons given: the NIST standard was already published, the algorithms had "… the most substantial history of cryptanalysis in a use case where their potential performance issues have minimal impact.", and the use case was considered more urgent. This guidance opens the door for either NIST SP 800-208 or FIPS 204 when protecting the integrity of the device's firmware. It should be noted that the SHA-3 or SHAKE hash algorithms are generally not allowed under CNSA 2.0 (with minor exceptions).

The transition timeline applicable to SEDs as outlined in the September 2022 Advisory is brisk: "Software and firmware signing: begin transitioning immediately, support and prefer CNSA 2.0 by 2025, and exclusively use CNSA 2.0 by 2030." And the National Information Assurance Partnership (NIAP) plans to update the "collaborative Protection Profile for Full Drive Encryption" to reflect CNSA 2.0 guidelines. This Protection Profile is used by NIAP in the Common Criteria evaluation of SEDs. The expectation (or - for now - speculation) is that SEDs listed on NSA's CSfC approved products list must meet the CNSA 2.0 compliant selection criteria of the updated Protection Profile.

*) https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF