



# Post-Quantum Trust Anchors

Security and trust in a post-quantum computing world



## Introduction

The potential for the first large-scale quantum computers to appear on the scene has many in the industry concerned about the impact this will have on current cryptography standards. A cryptographically relevant quantum computer ([CROC](#)) could break essentially all the public key cryptography standards in use today: ECC, RSA, DSA, and DH.

Someone could store a captured TLS negotiation and decrypt the encrypted data within a quantum computer sometime in the future, thus breaking the confidentiality of the protected data. In another scenario, if a digital signature used to validate file integrity is embedded in software or burned into a piece of hardware, a quantum computer could be used to forge a new signature of an arbitrary software or data. The potentially malicious forgery would then appear as if it were an authentic asset loaded from a known, trusted entity.

Despite the hype, viable quantum computers are not right around the corner. But extensive, critical efforts continue in academia, standards bodies, and within the industry to devise quantum-resilient algorithms that will continue to keep us secure in the post-quantum (PQ) world. Several quantum-safe algorithms have already been approved, including: LMS (RFC 8554), XMSS (RFC 8391), ML-KEM (FIPS-203), ML-DSA (FIPS-204), and SLH-DSA (FIPS-205).

The remainder of this paper, first published in 2019, provides a 2024-updated overview of the potential solutions for designing quantum-resilient systems, and what Cisco is doing about it today.

## Security and trust in a post-quantum world

At Cisco, we take product trust seriously. Cisco Trust Anchor Technologies provide the foundation for trustworthy systems across Cisco. The Cisco Trust Anchor and a Secure Boot check of signed images help ensure that the code running on Cisco hardware platforms is authentic and unmodified, establishing a hardware-level root of trust and an immutable device identity. Subsequent validation of all levels of software running on the platform during startup establishes a chain of trust for the system anchored to the hardware root. Such boot-code-integrity procedures are mandated in the Cisco Secure Development Lifecycle for all Cisco platform-based products. Furthermore, Cisco Trust Anchor Technologies provide product assurance functionality as well as foundational security features: immutable identity, highly secure storage, a random bit generator, and secure key management.

It is natural to prepare Trust Anchor Technologies to be secure in a PQ world. Cisco has already started deploying quantum-secure signatures in a limited number of systems and is continuing to expand their usage.

## PQ signatures

Cryptographical signatures are fundamental to trust anchor technology. However, traditional signature methods rely on RSA or ECC (Elliptic Curve Cryptography), both of which could be vulnerable to a large-scale quantum computer. Even though such a large-scale quantum computer is not expected to be in existence for a while, trust anchors are built into Cisco devices and are deliberately hard to update. Fortunately, there are several signature algorithms that are secure even if the adversary has access to a quantum computer.

Due to their well-understood and analyzed primitives, Hash-Based Signature (HBS) schemes are widely accepted as good candidates for quantum-secure signatures that are as strong as the hash function itself. NIST has approved two stateful HBS schemes (LMS and XMSS) in SP 800-208 and one stateless scheme (SLH-DSA) in FIPS 205. The distinction is that, for a stateful scheme, the signer needs to securely record how many signatures it has generated, and that is difficult for a trust anchor module. The advantage of a stateful scheme for such resource constrained devices lies in the efficiency of signature verification. Thus, we use LMS to sign firmware generated at Cisco so that the device can detect modified or inauthentic binary images.

The post-quantum signature algorithm for general use is ML-DSA, which NIST has standardized in FIPS 204. It is based on the module lattice problem (which is what the “ML” stands for), and that problem is believed to be hard for a quantum computer to solve. This is the postquantum signature algorithm that would be used if the trust anchor needs to generate a signature itself.

To make our [Trust Anchor technologies](#) secure against a quantum computer, Cisco has already been employing quantum-secure key sizes and algorithms in some of our platforms for many years, and will continue to roll out additional quantum-safe capabilities in our products

## Hashes

We verify software integrity using hashes, so we want to ensure that the hashes we use are PQ secure. To be conservative against anticipated quantum attacks of the future, we chose to use 512-bit hashes with our software, which should provide PQ security for many years to come. Thus, we use SHA512 of the SHA2 hash family (Figure 1).

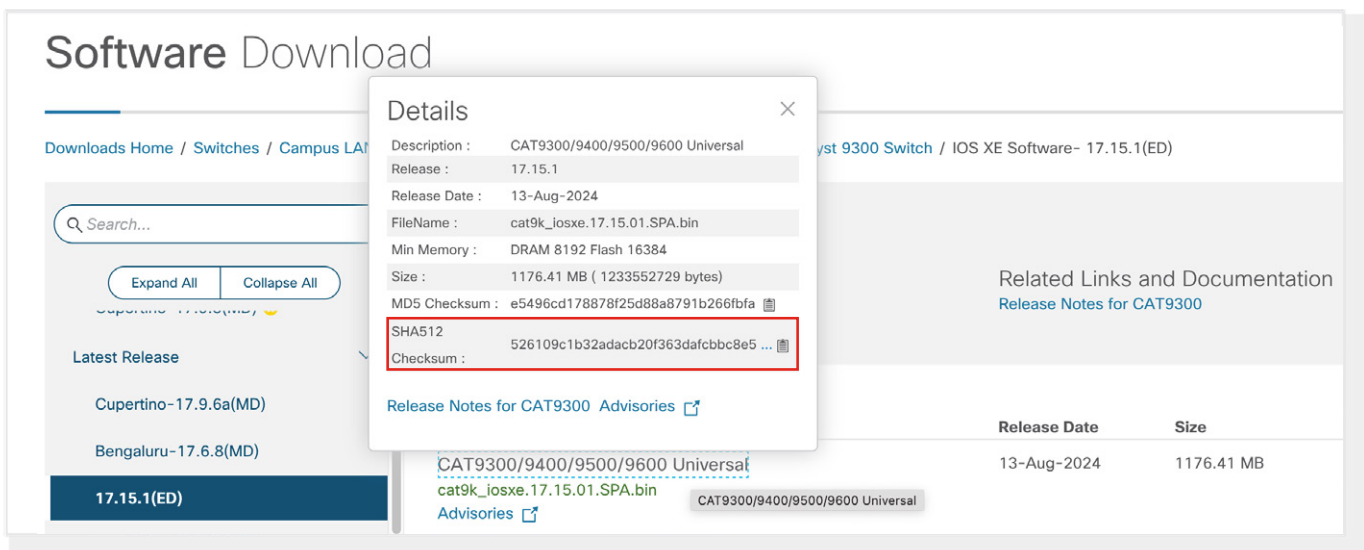


Figure 1: Snapshot of a software download from cisco.com that includes the SHA512 hash for manual integrity verification before loading the software on a virtual machine (VM). The Secure Boot feature provides automatic integrity and authenticity verification of the chain of loaded firmware and software on a device.

## Symmetric algorithms

We use constructs like FPGAs to achieve a variety of system functions. Often these FPGAs are used to implement system-critical security functions such as trust anchor designs as well as datapath crypto FPGAs. Where possible, we use 256-bit AES keys to encrypt the configuration bitstream of these devices.

## Signatures

We chose HBS for their straightforward implementation and minimal code size, their well-understood nature, and the simple primitives upon which they are based. Cisco employees David McGrew, Scott Fluhrer, and Michael Curcio co-authored the LMS standard (RFC 8554), a stateful HBS scheme that is the evolution of LDWM. LDWM is an HBS scheme based on research pioneered by Lamport, Diffie, Winternitz, and Merkle decades ago. LMS builds on LDWM by adapting ideas published in Leighton and Micali's work from 1995 and introducing certain parameters that offer domain separation. Readers should note that attacker-produced hash collisions are irrelevant for LMS as LMS never hashes a string where the attacker selects the value.

LDWM is already used as a firmware verification algorithm on many Cisco platforms. It also exists in Cisco's Trust Anchor modules implemented using FPGAs in various service provider platforms. The parameters chosen include SHA256 hashes, Winternitz parameter  $W=4$ , and tree height  $H=10$ .

PQ software signing, as designed for certain Cisco FPGAs and hardware when this work started in 2013, leverages LDWM to verify software images or firmware before loading it. New hardware roadmaps will be switching to more PQ image-signing schemes like LMS.

## The path ahead

Ubiquitous PQ Trust Anchors is Cisco's goal, and we plan to continue to introduce quantum-safe algorithms in our Trustworthy Systems technologies. The LDWM and LMS signature schemes will continue to be integrated into more platforms.

We also plan to keep researching PQ cryptography and, along with the industry, introduce it in protocols and use cases to achieve a quantum-safe future where confidential data exchanged online and potentially stored today cannot be decrypted later when viable quantum computing becomes available. More information can be found in the References section at the end of this paper.

# Acknowledgments

Chirag Shroff

[cshroff@cisco.com](mailto:cshroff@cisco.com)

Distinguished Engineer, Security & Trust Organization

Scott Fluhrer

[sfluhrer@cisco.com](mailto:sfluhrer@cisco.com)

Principal Engineer, Security & Trust Organization

Michael Curcio

[micurcio@cisco.com](mailto:micurcio@cisco.com)

Hardware Engineering Technical Leader, Security & Trust Organization

# References

[Module-Lattice-Based Key-Encapsulation Mechanism Standard \(ML-KEM\)](#)

[Module-Lattice-Based Digital Signature Standard \(ML-DSA\)](#)

[Stateless Hash-Based Digital Signature Standard \(SLH-DSA\)](#)

[LMS Hash-Based signatures IETF RFC 8554](#)

[XMSS Hash-Based signatures IETF RFC 8391](#)

[Global Risk Institute 2023 Quantum Threat Timeline Report](#)

[Cisco Post-Quantum Cryptography](#)

[Cisco Trustworthy Solutions](#)