Quantum security

QKD, PQC and what they change in network platforms

Abhishek Mande
Principal Architect, APJC

October 2026

Agenda

01 Quantum-era encryption

02 Why it is needed

03 QKD and PQC

04 Design considerations

05 Current adoption

06 Impact on CPU, NPU and DPU

07 Standardization

08 Qubits and quantum networks

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Three meanings of “quantum” in security

The threat

Quantum computing

A large, error-corrected quantum computer running Shor's algorithm breaks RSA, Diffie-Hellman and elliptic-curve cryptography.

No such machine exists yet. Estimates of what it takes keep falling.

Response 1 · PQC

Post-quantum cryptography

New public-key algorithms that resist quantum attack and run on today's processors. A software and firmware change.

ML-KEM · ML-DSA · SLH-DSA

Response 2 · QKD

Quantum key distribution

Symmetric keys generated from quantum states of light over an optical link. Dedicated hardware at both ends.

BB84 · E91 · CV-QKD

“Quantum-safe” and “quantum-resistant” name the goal, not a technology. Every national roadmap makes PQC the baseline; QKD is an optional extra layer.

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

What a quantum computer breaks

Algorithm today	Used for	Quantum attack	Outcome
RSA	Key exchange, signatures, certificates	Shor (1994)	**BROKEN**
Diffie-Hellman	Key exchange in IKE, TLS and SSH	Shor	**BROKEN**
Elliptic curves: ECDH, ECDSA, Ed25519	Key exchange and signatures	Shor	**BROKEN** with fewer qubits than RSA
AES	Bulk encryption in IPsec, MACsec, TLS	Grover (1996)	**HOLDS** with 256-bit keys
SHA-2, SHA-3, HMAC	Hashing, integrity, key derivation	Grover, BHT	**HOLDS** at 384 bits or longer

The exposure is in public-key cryptography: key establishment and signatures. Bulk encryption and hashing carry over once keys and digests are long enough.

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Migration deadlines by jurisdiction

Jurisdiction	Start	Critical systems	Complete
United States · federal	2026: agency leads and inventory	2030 key exchange, 2031 signatures	2035: RSA and ECC disallowed
United States · national security	Jan 2027: new buys compliant	2030: network equipment	2031 to 2033
European Union	End 2026: national roadmaps	End 2030: high-risk use cases	End 2035, as far as feasible
United Kingdom	2028: discovery and plan	2031: priority migrations	2035
Australia	End 2026: refined plan	End 2028: critical systems started	End 2030: no classical public-key
Singapore · CII owners	Mar 2027: plan filed with CSA	Jan 2028: new systems PQ-ready	End 2031
India · task-force roadmap	2027: critical-sector foundations	2029: critical sectors on PQC	2033: enterprises
Japan · South Korea	National strategies under way	Not yet dated	2035 targets

First deadlines fall between 2026 and 2028. Equipment bought now will still be in service when the 2030 dates arrive.

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

The algorithms at a glance

ATTACKS on a quantum computer	**Shor** 1994. Factoring and discrete logs: breaks RSA, DH and ECC		**Grover** 1996. Search: halves the strength of symmetric keys		**BHT** 1997. Hash collisions: a modest speed-up	
POST-QUANTUM on classical processors	**ML-KEM** Key exchange (Kyber)	**ML-DSA** Signatures (Dilithium)	**SLH-DSA** Hash signatures (SPHINCS+)	**FN-DSA** Small signatures (Falcon)	**HQC** Backup key exchange	**LMS · XMSS** Firmware signing
QKD PROTOCOLS on photonic hardware	**BB84** Prepare and measure	**E91 · BBM92** Entangled photon pairs	**COW · DPS** Coherent pulse trains	**CV-QKD** Continuous variable	**MDI-QKD** Untrusted relay node	**TF-QKD** Twin-field, long reach
UNCHANGED symmetric cryptography	**AES-256** Bulk encryption in IPsec, MACsec and TLS		**SHA-384 · SHA-512 · SHA-3** Hashing and integrity		**HMAC · HKDF** Message authentication and key derivation	

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Which algorithm to use when

Key exchange

ML-KEM-768 hybrid

With X25519 or P-256, for TLS 1.3, IKEv2, SSH and QUIC. Fast, standardized, already the browser default.

Authentication

ML-DSA-65

For certificates and for IKEv2 and TLS signatures. ML-DSA-44 where every byte counts.

Firmware, secure boot

LMS or XMSS

Fast to verify and approved since 2020. Signing state must live in an HSM; ML-DSA avoids that.

Long-lived roots

SLH-DSA

Rests on hash functions alone. Accept 8 kB signatures and slow signing for a key that lasts 20 years.

US national security

ML-KEM-1024, ML-DSA-87

CNSA 2.0 parameter sets, with AES-256 and SHA-384 or SHA-512. LMS or XMSS for firmware.

Tight size budgets

FN-DSA, once final

666-byte signatures for DNSSEC, IoT and long certificate chains. Sign offline, verify anywhere.

Hedge on lattices

HQC, when standardized

Code-based backup key exchange. Classic McEliece or FrodoKEM where a regulator asks for them.

High-value links

QKD on top of PQC

Decoy-state BB84 on dedicated fiber adds a physics-based key source. PQC still authenticates.

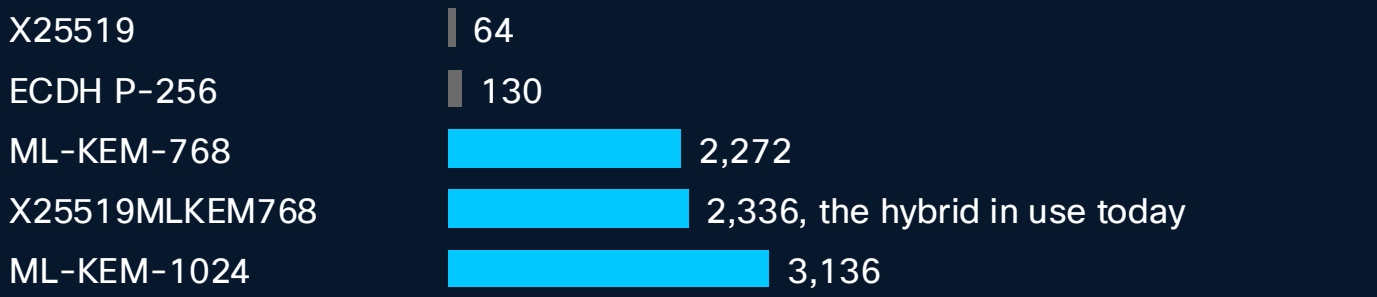
For most networks: hybrid ML-KEM-768 for key exchange now, ML-DSA-65 for authentication as PKI and platforms allow.

© 2025 Cisco and/or its affiliates. All rights reserved.

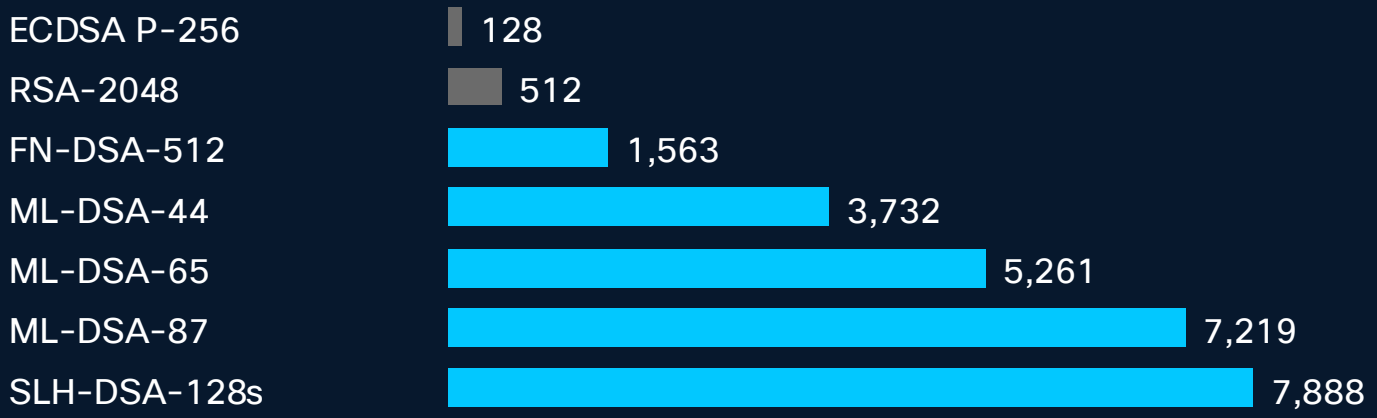
Cisco Confidential

Key and signature sizes

Key exchange · bytes on the wire, both directions



Authentication · public key plus one signature



IKEv2

An ML-KEM-768 share no longer fits IKE_SA_INIT inside a 1,500-byte MTU. It moves to IKE_INTERMEDIATE (RFC 9370), where fragmentation applies.

TLS 1.3

The ClientHello grows by about 1.2 kB and can span two packets, which some middleboxes mishandle. A full ML-DSA certificate chain adds about 15 kB.

What it means

Key exchange grows by kilobytes and is manageable. Signatures and certificates are the hard part.

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Design principles for migration

01

Hybrid first

Pair ML-KEM with X25519 or P-256 so a flaw in one does not expose the session. Germany and France expect hybrids; US national-security and Australian guidance prefer pure PQC.

02

Key exchange now, signatures next

Key exchange is exposed to harvesting today and is a software change. Certificates, PKI and code signing take longer and must be finished before a capable machine exists.

03

Crypto-agility

Negotiate algorithms; never hard-code them. Keep an inventory of where cryptography lives, and leave room for HQC, FN-DSA and new parameter sets.

04

Symmetric at 256 bits

AES-256-GCM and SHA-384 or better across IPsec, MACsec and TLS. Retire hardware paths that only support 128-bit keys.

05

Mind the MTU

Larger handshakes mean IKE fragmentation, split ClientHellos and an extra round trip. Test firewalls, load balancers and control-plane policers.

06

Anchor trust in hardware

Secure boot, firmware signing and device identity need a post-quantum root in anything bought now and still in service after 2030.

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Adoption in numbers

Key exchange

2/3

of human-generated TLS traffic to Cloudflare uses hybrid ML-KEM (April 2026)

Key exchange

44%

of the top 1 million websites negotiate X25519MLKEM768, now the most common group (June 2026)

Certificates

0%

of 32,011 surveyed domains present a post-quantum certificate (June 2026)

Enterprises

7%

of organizations run quantum-safe or hybrid cryptography across most of their certificates (May 2026 survey)

Key exchange moved because browsers and CDNs changed their defaults. Authentication, private networks and enterprise estates have barely started.

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Most widely deployed algorithms

#	Algorithm	Where it runs	Evidence
1	**X25519MLKEM768**	TLS 1.3: ML-KEM-768 with X25519 in browsers, OpenSSL 3.5 and Go	Two-thirds of Cloudflare's human traffic; 44% of the top 1 million sites
2	**mlkem768x25519**	SSH key exchange in OpenSSH	The OpenSSH default since version 10 (2025)
3	**ML-KEM-1024 (Kyber)**	Signal (PQXDH) and Apple iMessage (PQ3)	Consumer messaging since 2023 and 2024
4	**LMS, XMSS**	Firmware and secure-boot signing	The first CNSA 2.0 deadline: software and firmware signing
5	**ML-DSA**	Private PKI, IKEv2 authentication, TPM 2.0	Early: no public web certificates yet
6	**SLH-DSA, FN-DSA, HQC**	Niche uses, or the standard is not final	Minimal
QKD	**BB84 + decoy states**	China's backbone and most commercial fiber links	Dominant among QKD protocols; a small footprint next to PQC

One key-exchange algorithm, ML-KEM-768 in a hybrid, accounts for nearly all post-quantum cryptography in use.

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

What is shipping today

Area	What ships	Since
Browsers	Chrome, Edge, Firefox and Safari negotiate hybrid ML-KEM by default	2024 to 2025
Libraries and languages	OpenSSL 3.5 and Go enable hybrid ML-KEM by default	2024 to 2025
Operating systems	Apple iOS, iPadOS and macOS 26	Oct 2025
Cloud and CDN	Cloudflare by default; Google front ends; AWS KMS, ACM and Secrets Manager	2022 to 2025
Messaging and SSH	Signal PQXDH, Apple iMessage PQ3, OpenSSH 10	2023 to 2025
Network platforms	ML-KEM for IKEv2 in Cisco IOS XE 26.1, Fortinet FortiOS 7.6 and Palo Alto PAN-OS 11.2	2024 to 2026
Managed network services	Cloudflare IPsec with hybrid ML-KEM, interoperating with Cisco and Fortinet	Apr 2026
Hardware trust	TPM 2.0 library specification 1.85 adds ML-KEM and ML-DSA	Mar 2026

Clients and large platforms moved by default. Origin servers, private PKI and network devices are where the remaining work sits.

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

The handshake changes. The packet path does not.

Key exchange and signatures run once per session on the control-plane CPU. AES-256-GCM still encrypts every packet in the NPU, ASIC or DPU.

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Control plane and data plane

CONTROL PLANE
CPU
once per session

Key exchange
ECDH + ML-KEM

→

Authentication
RSA or ECDSA, then ML-DSA

→

Key derivation
symmetric session keys

CHANGES
About 1.5 kB and 0.1 ms more per key exchange; one more IKE round trip; larger certificates once ML-DSA arrives.

↓ Session keys are installed in the data path

DATA PLANE
NPU · ASIC · DPU
on every packet

AES-256-GCM bulk encryption
IPsec ESP · MACsec · TLS records

UNCHANGED
Same throughput, latency and packet size, provided AES-256 is already in use.

QKD keys or pre-shared keys, where used, feed the key derivation step (RFC 8784). They do not touch the packet path either.

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

CPU cost of post-quantum key exchange

~0.1 ms

more CPU per TLS handshake for hybrid X25519MLKEM768: 0.04 to 0.07 ms per side on OpenSSL 3.5; AWS reports 0.08 to 0.15 ms

Red Sift 2026 · AWS 2025

−2.3%

AWS KMS requests per second when every request opens a new TLS connection; 0.05% lower with connection reuse

AWS 2025

<5 ms

added to IKEv2 tunnel set-up by ML-KEM in a strongSwan testbed: 2.7 to 4.7 ms measured

Perera et al. 2026

ML-KEM itself is faster than the X25519 it is paired with. The cost of a hybrid is doing both, plus about 1.5 kB on the wire.

For scale: choosing an RSA-2048 server certificate over ECDSA P-256 costs the server about 0.5 ms per handshake in the same test, several times the post-quantum increment.

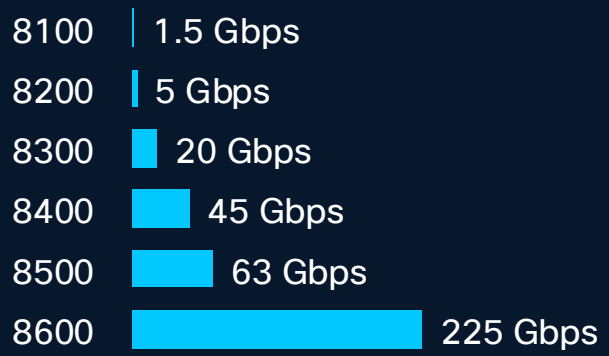
© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Cisco: published performance numbers

Data plane

IPsec throughput at 512-byte packets



Data-sheet maximums for each secure-router series. The packet path still runs AES, so a post-quantum key exchange does not change them.

Handshake

Whole IKEv2 exchange with ML-KEM-768

Signature	Frames	Bytes
RSA-2048	7	7,111
ML-DSA-44	16	19,033
ML-DSA-65	20	24,401
ML-DSA-87	24	31,497

Measured on C8235-G2 routers, IOS XE 26.2. The key exchange accounts for 2 frames and 2,548 bytes of each.

Time in a strongSwan lab: about 21 ms hybrid against 20 ms classical.

Quantum networking

Research prototypes and trials

Entanglement chip · 2025

Up to **200 million** entangled photon pairs per second, 1 million per output channel; under 1 mW at room temperature

Universal quantum switch · Apr 2026

At most **4%** average loss of fidelity in polarization tests; switches in as little as **1 ns**; under 1 W

Metro trial with Qunnect · Feb 2026

Entanglement swapping over 17.6 km of New York fiber: **5,400** pairs per hour, over 99% fidelity

Sources: Cisco data sheets and FAQ (2025–2026); Cisco Blogs (Jul, Sep 2026); Cisco Newsroom (2025, Apr 2026); Qunnect (Feb 2026)

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

NIST: algorithm standards

Document	Covers	Status
FIPS 203, 204, 205	ML-KEM, ML-DSA and SLH-DSA	Final since August 2024
FIPS 206	FN-DSA: compact lattice signatures	Not yet final; expected late 2026 or 2027
HQC standard	Backup key establishment from a different maths family	Selected March 2025; final expected about 2027
Additional signatures	Nine candidates: FAEST, HAWK, MAYO, MQOM, QR-UOV, SDitH, SNOVA, SQIsign, UOV	Round 3 opened May 2026; about two years
SP 800-208	LMS and XMSS stateful hash-based signatures	Final since 2020
IR 8547	Transition timeline: RSA and ECC deprecated from 2030, disallowed from 2035	Draft since November 2024
FIPS 140-3 validation	Certified cryptographic modules that include the new algorithms	FIPS 140-2 certificates became historical in September 2026

The core set is final. Still moving are the alternates: FN-DSA, HQC and a second generation of signatures.

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

IETF: protocol standards

Document	Covers	Status
RFC 10024, RFC 9954	Hybrid ML-KEM key exchange for TLS 1.3, and its general design	Published July and August 2026
RFC 9370, RFC 9242	Multiple key exchanges and the intermediate exchange in IKEv2	Published 2022 and 2023
RFC 8784	Pre-shared keys mixed into IKEv2 for quantum resistance	Published 2020
RFC 9881, RFC 9935	ML-DSA and ML-KEM in X.509 certificates	Published
ML-KEM for IKEv2	Code points for ML-KEM-512, -768 and -1024	Approved; in the RFC Editor queue
ML-DSA in TLS 1.3 and IKEv2	Post-quantum signature authentication for both protocols	Approved; in the RFC Editor queue
Composite signatures	Certificates carrying a classical and a post-quantum signature	Approved; in the RFC Editor queue
Merkle Tree Certificates	Smaller post-quantum certificate chains for the web	In development

Key exchange is standardized for TLS and nearly so for IKEv2. The authentication documents are approved and waiting for RFC numbers.

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

QKD and platform standards

Body	Work	Status
ETSI	GS QKD 014 key-delivery API; GS QKD 016 Common Criteria protection profile	Published
ITU-T	Y.3800 series on QKD networks; X.1710 security framework	Published
ISO/IEC	23837 security requirements and tests for QKD modules; 18033-2 adds Classic McEliece	Published
3GPP	Release 20 study on moving 5G procedures to PQC (TR 33.703)	Study in progress
Trusted Computing Group	TPM 2.0 library specification 1.85 with ML-KEM and ML-DSA	Published March 2026
CA/Browser Forum	Rules for post-quantum certificates in the public web PKI	Not yet in place
National programs	South Korea's KpqC algorithms; China's own algorithm program; BSI and ANSSI profiles	Diverging in places

Still open: post-quantum certificates for the public web, 3GPP procedures, and certification of QKD products.

Sources: ETSI; ITU-T; ISO; 3GPP TR 33.703 drafts (2026); Trusted Computing Group (Mar 2026); Cloudflare (2025)

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Interconnecting quantum computers

Centimeters

Inside one machine

Chips or ion traps are joined by couplers, or ions are shuttled between zones, inside one cryostat or vacuum chamber.

IBM plans to entangle two modules in 2027 on the way to its 2029 machine.

Meters

Between machines in a room

Photons carry entanglement over fiber, and gates are teleported between modules. Superconducting qubits first need a microwave-to-optical transducer.

Oxford linked two ion-trap modules and ran Grover's algorithm across them (Nature, 2025).

Kilometers

Between sites

Entanglement is distributed over metro or long-haul fiber, or by satellite. Loss cannot be amplified away, so long routes need quantum repeaters and memories.

IBM and Cisco aim to show a network of fault-tolerant machines by the end of 2030.

How it works	No qubit travels. A photonic link creates an entangled pair shared by two machines, and the pair is used up to teleport a state or a gate. The rate and quality of those pairs set the speed of the whole system.

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Standards for quantum computing and networking

Area	What exists	Status
Vocabulary	ISO/IEC 4879 quantum computing vocabulary; IEEE P7130 definitions	ISO/IEC published in 2024
Programming interfaces	OpenQASM 3 and QIR, the Quantum Intermediate Representation	De facto, industry-led
Benchmarking	Quantum volume, CLOPS, algorithmic qubits; IEEE P7131; DARPA QBI	No agreed standard yet
Quantum network architecture	IRTF QIRG: RFC 9340 principles, RFC 9583 application scenarios	Informational RFCs, 2023–2024
QKD networks	ITU-T Y.3800 series; ETSI GS QKD series; ISO/IEC 23837	Published; certification maturing
Links between quantum computers	Vendor and laboratory protocols only	No formal standard
Committees at work	ISO/IEC JTC 3, CEN-CENELEC JTC 22, ETSI, ITU-T, IEEE	JTC 3 formed in 2024

Security standards are well ahead of computing standards. FIPS 203 can be deployed today; there is no standard way yet to link two quantum computers.

Sources: ISO; IETF datatracker (RFC 9340, RFC 9583); ITU-T; ETSI; IEEE Standards Association

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Next steps

The next twelve months

01	**Inventory**	Find where RSA, DH and ECC live: protocols, certificates, firmware, suppliers
02	**Turn on hybrid key exchange**	TLS 1.3 and IKEv2 first, on the paths that carry long-lived data
03	**Buy for 2030**	ML-KEM, ML-DSA, AES-256 and a post-quantum root of trust in every RFP
04	**Test at scale**	Handshake rate, MTU and fragmentation, policers, rekey behavior
05	**Plan authentication**	PKI, certificates and code signing, ahead of the 2029 to 2031 deadlines
06	**Place QKD deliberately**	Where a point-to-point optical link and a policy case both exist

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Thank You

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential