

Post-Quantum Cryptography at HPE

Krishna Prasad Shastry, HPE Labs

September 2026

Quantum algorithms exist
which break cryptographic
algorithms on which we
depend for security

The quantum threat to cryptography

BROKEN · Public-key (asymmetric)

- RSA
- DSA
- Elliptic Curve DSA
- Edwards Curve DSA
- Diffie-Hellman
- Elliptic Curve Diffie-Hellman

Shor's Algorithm

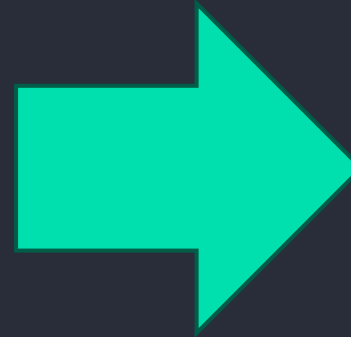
Solves integer factorization and discrete log in polynomial time.

Weakened · Symmetric and hash

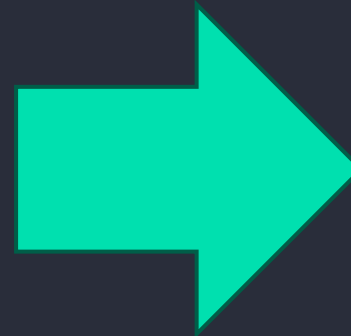
- AES-128 → effective 64-bit security
- AES-256 → effective 128-bit security
- SHA-256 → effective 128-bit security
- SHA-384 → effective 192-bit security

Grover's Algorithm

Halves the effective key length. Mitigated by doubling key size.



New algorithms required



Use stronger versions

What is affected?

A non-exhaustive list

- TLS
- IPsec
- SSH
- Code and firmware signatures
- PKI
- Secure boot
- Data encrypted at rest with AES-128

What are the principal threats?

Due to broken asymmetric cryptography

- Harvest now decrypt later
- Harvest now forge later
- Software and firmware signing
 - Especially keys fused into silicon
- Total failure of authentication
 - Only when a quantum computer exists

What are the new algorithms?

Algorithm	Function	Specification	Comment
ML-KEM	Key establishment	NIST FIPS 203	For general purpose use
ML-DSA	Digital Signature	NIST FIPS 204	For general purpose use
SLH-DSA	Digital Signature for software and firmware signing	NIST FIPS 205	Not suitable for general purpose use. Slow and large signatures.
FN-DSA	Digital Signature	NIST FIPS 206	Not yet finalized, smaller signatures & keys than ML-DSA. More complex implementation.
HQC	Key establishment	TBD	A fallback if ML-KEM proves vulnerable (to be finalized in 2027)
LMS	Digital Signature for software and firmware signing	NIST SP 800-208	One-time keys impose stringent key-management requirements. Slow and large signatures.
XMSS	Digital Signature for software and firmware signing	NIST SP 800-208	One-time keys impose stringent key-management requirements. Slow and large signatures.

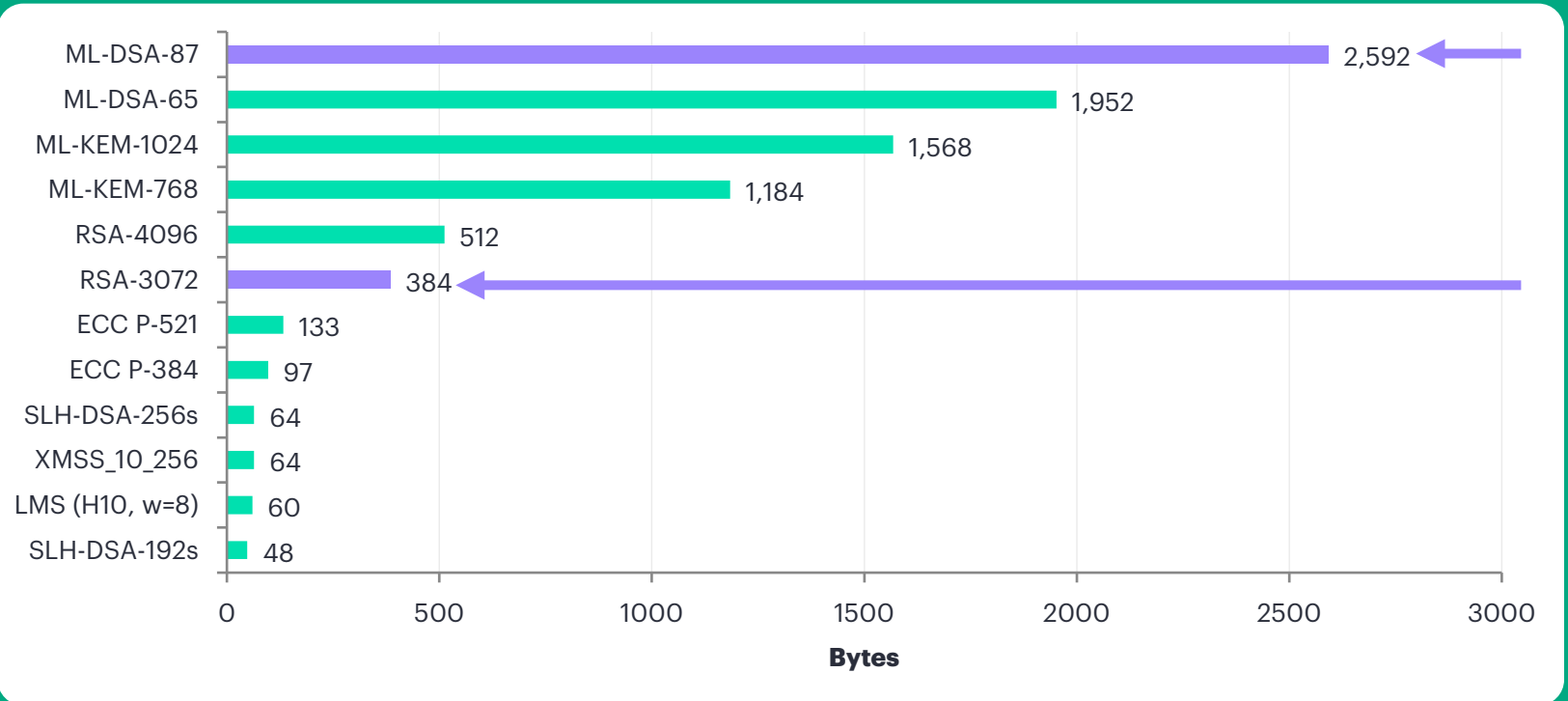
Adapted from: <https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography>

A large teal arrow pointing to the right, positioned behind the text.

Unfortunately, these are not
plug-in replacements for
what we have

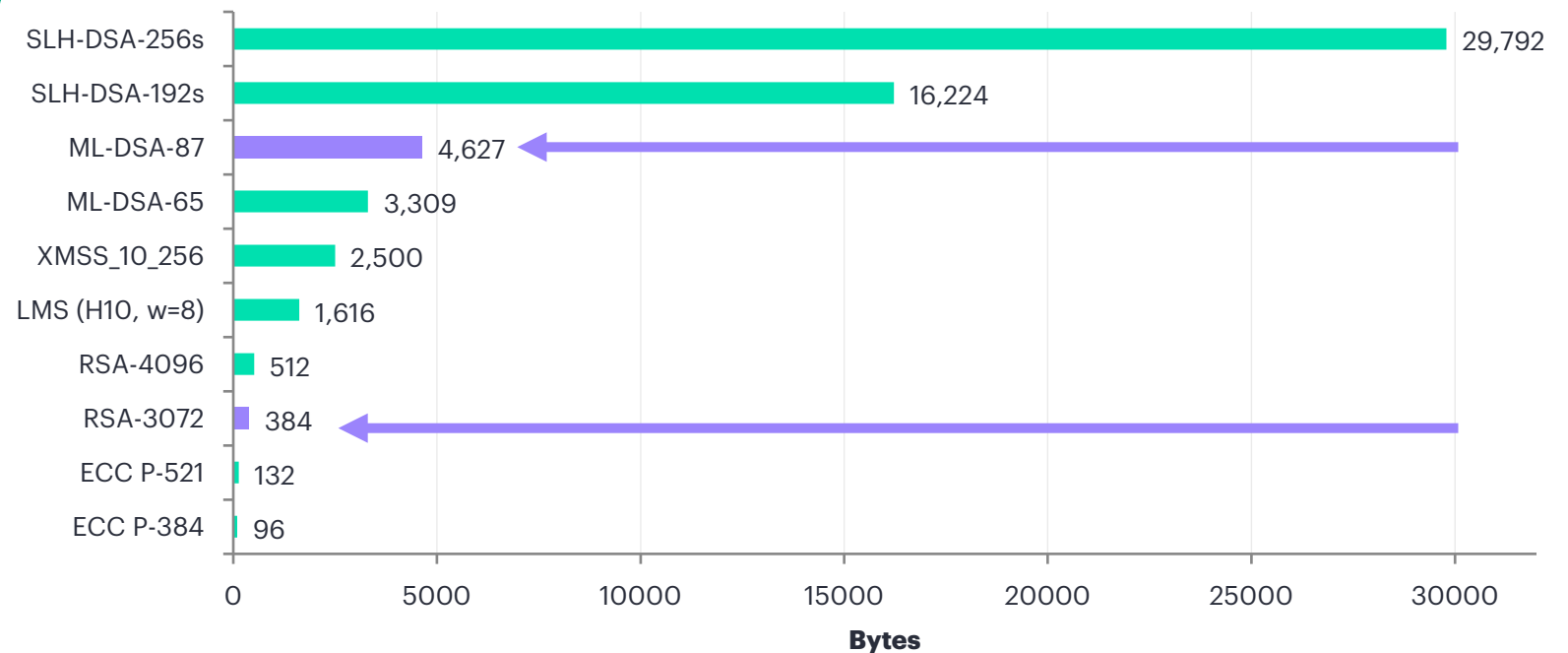
Cryptographic Key Sizes (Public Key)

- ML-DSA and ML-KEM are larger than current public key sizes
- Systems will need to adjust to support larger algorithms
- Devices will need to ensure sufficient storage capacity to handle larger signatures and certificate chains.



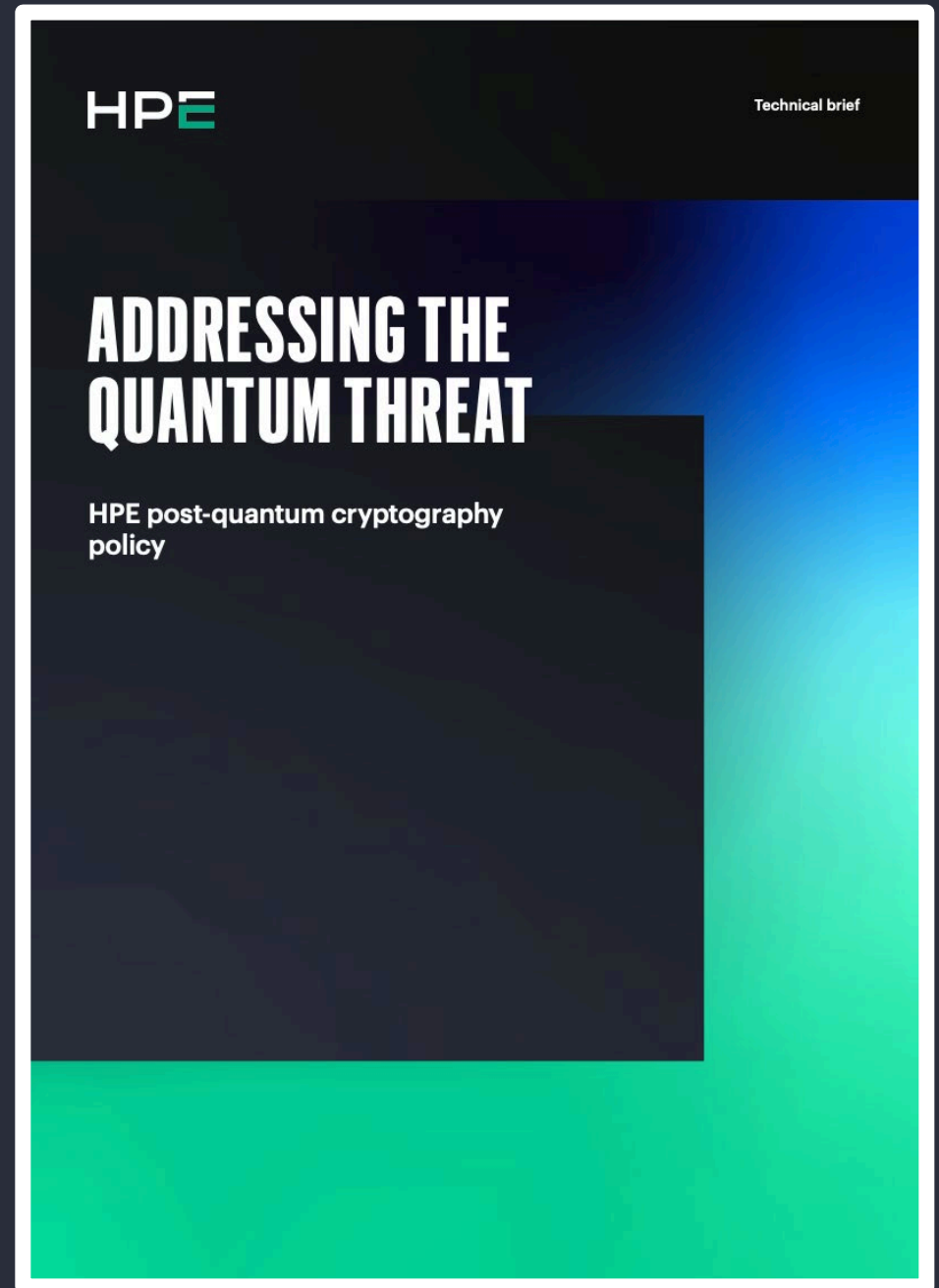
Cryptographic Signature Sizes

- ML-DSA, ML-KEM, XMSS, LMS, and SLH-DSA are larger than RSA and ECC.
- Systems will need to adjust to support larger algorithms
- Devices will need to ensure sufficient storage capacity to handle larger signatures and certificate chains.



HPE's PQC Policy

<https://www.hpe.com/psnow/doc/a50015180enw>



HPE's preferred algorithms – the strongest possible security

From the HPE PQC Policy

Table 1. HPE approved algorithms

Function	Algorithm	NIST specification	Parameters
Digital signatures	Module-Lattice-Based Digital Signature Algorithm (ML-DSA)	FIPS PUB 204	ML-DSA-87
Key establishment	Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)	FIPS PUB 203	ML-KEM-1024
Symmetric encryption	Advanced Encryption Standard (AES)	FIPS PUB 197	AES-256
Digests	Secure Hash Algorithm (SHA)	FIPS PUB 180-4	SHA-384 or SHA-512

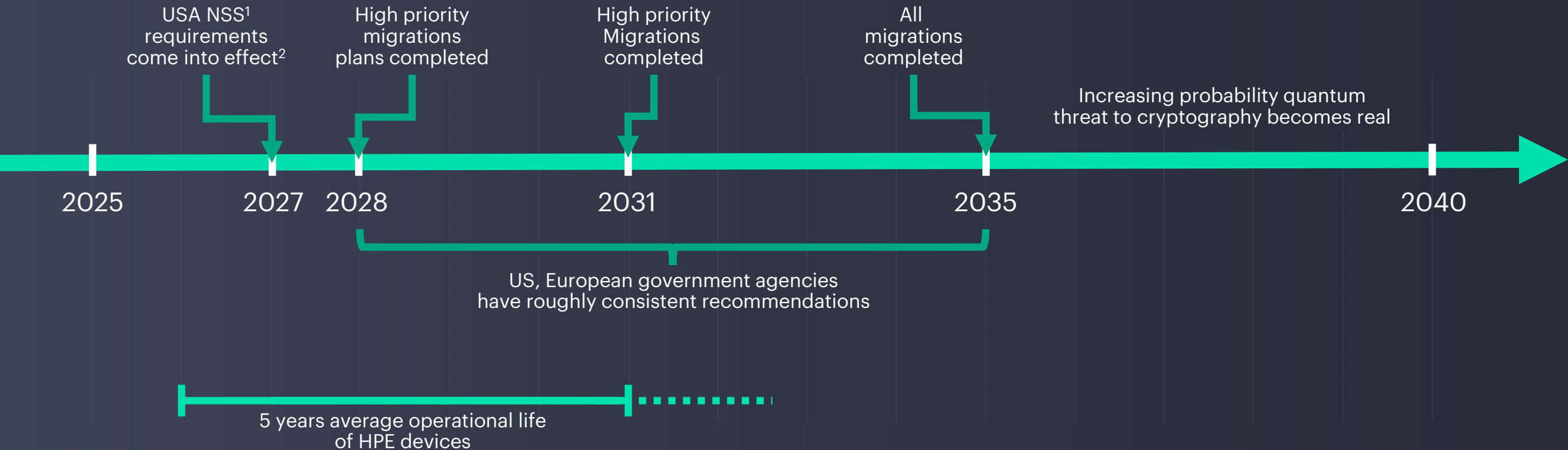
In addition to these general-purpose algorithms, HPE has approved the following algorithms and parameters for specific applications within our products and services:

Table 2. HPE approved algorithms for specific applications

Function	Algorithm	NIST specification	Parameters
Digital signatures	Leighton-Micali Signature (LMS)	NIST SP 800-208	LMS SHA-256/192
Digital signatures	eXtended Merkle Signature Scheme (XMSS)	NIST SP 800-208	All
Digests	Secure Hash Algorithm 3 (SHA3)	FIPS PUB 202	SHA3-384 or SHA3-512 allowed for internal hardware functionality only (e.g., boot-up integrity checks)

For software and firmware
signing HPE is adopting
hybrid

The PQC migration timeline



Note: the above timeline is **still** consistent with government advice

E.G. <https://www.whitehouse.gov/presidential-actions/2026/06/securing-the-nation-against-advanced-cryptographic-attacks/>
<https://www.ncsc.gov.uk/guidance/pqc-migration-timelines>

¹NSS: National Security Systems are information systems used by US security agencies

²The Australian Signals Directorate (ASD) have also specified 1/1/27

HPE actions on PQC

Introduction of PQC-enabled and PQC-capable products to meet recommended timeline

Focus will be new product and major releases
For servers PQC-enabled options will be available

Working with
component
partners suppliers
to develop
roadmaps

Updating protocol
implementations as
standards,
implementations
and RFCs evolve

Updating internal
PKI and code-
signing (dual
signatures)

Updating software
components as
implementations
and community
evolve (e.g. UEFI)

Recommended actions

- Identify high priority systems
- Build a cryptographic inventory
 - Automate with tools
 - Cipher suites offered by protocols?
 - Keys and certificates?
 - Data encryption algorithms?
- Assess availability of PQC software for protocols and other software
 - Standards ratified?
 - Production ready implementations?
- For hardware refresh consider availability of PQC-enabled hardware options

Thank You

Krishnaprasad.shastri@hpe.com

