POST-QUANTUM CRYPTOGRAPHY

The migration ahead



Professor Craig Costello

ISACA Brisbane Conference 2026

QUT

What actually breaks?

Trust.

Connections

Private sessions

Identity

Certificates and signatures

Software

Signed code and updates

All three rely on public-key cryptography.

QUT

Why quantum threatens cryptography

1994

Algorithms for Quantum Computation Discrete Logarithms and Factoring

PETER W. SHOR

A SUFFICIENTLY POWERFUL QUANTUM COMPUTER CAN

Factor large integers

RSA

Compute discrete logarithms

Diffie–Hellman and elliptic curves

Key establishment and signatures are at risk.

Peter W. Shor, FOCS 1994

QUT

AES and modern hashes are fine for now

AES

AES-256 retains a strong security margin.

Hash functions

SHA-384 and SHA-512 retain strong margins.

Quantum speedups reduce margins. Public-key crypto is the priority.

The resource estimates changed in 2026

Modeled attacks on 256-bit elliptic curves

ARCHITECTURE	PHYSICAL QUBITS	ESTIMATED RUN TIME
Superconducting secp256k1	**<500,000**	**Minutes**
Neutral atoms P-256	**≈26,000**	**≈10 days**
Trapped ions secp256k1	**≈20,000**	**≈26 days per attempt**

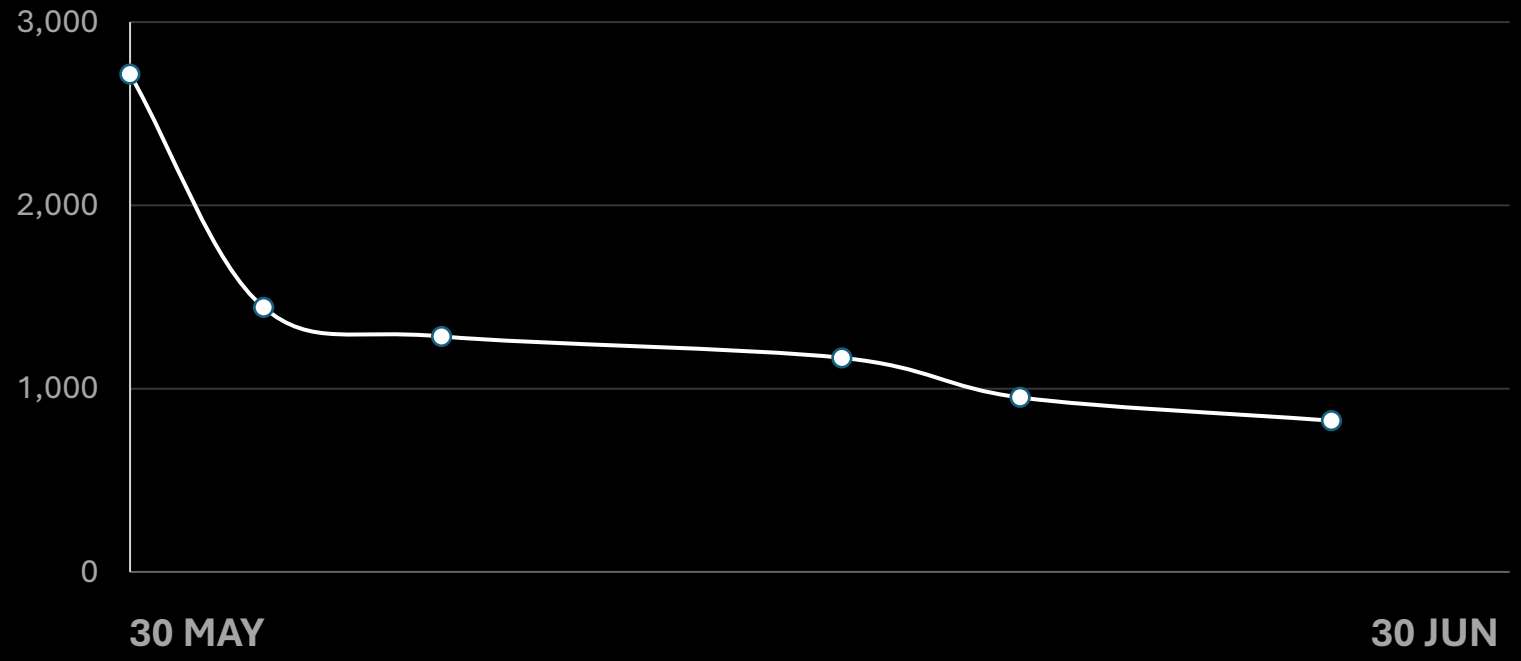
Each estimate assumes a different fault-tolerant machine.

Babbush et al. / Cain et al. / Häner et al. (2026)

QUT

How much smaller can the circuit get?

ECDSA.fail / Peak logical qubits for one secp256k1 point addition



825

logical qubits

489 million Toffolis

per point addition

Selected May–June 2026 results for one component of Shor's algorithm.

ECDSA.fail benchmark / Long et al., arXiv:2609.09582

QUT

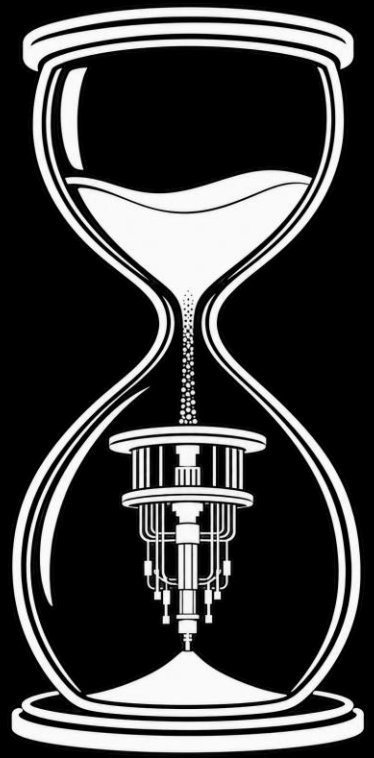
Harvest now, decrypt later

TODAY

Collect encrypted traffic

YEARS LATER

Recover the keys and read it



How long does the data have to stay private?

The migration clock is already running

10 years	+	3 years	=	13 years
DATA CONFIDENTIALITY		TIME TO MIGRATE		PLANNING WINDOW

Example. A session just before migration finishes could stay sensitive for another decade.

Michele Mosca / IEEE Security & Privacy (2018)

QUT

Post-quantum cryptography

New algorithms that run on conventional computers.

KEY ESTABLISHMENT

ML-KEM

Establish a shared secret

DIGITAL SIGNATURES

ML-DSA

SLH-DSA

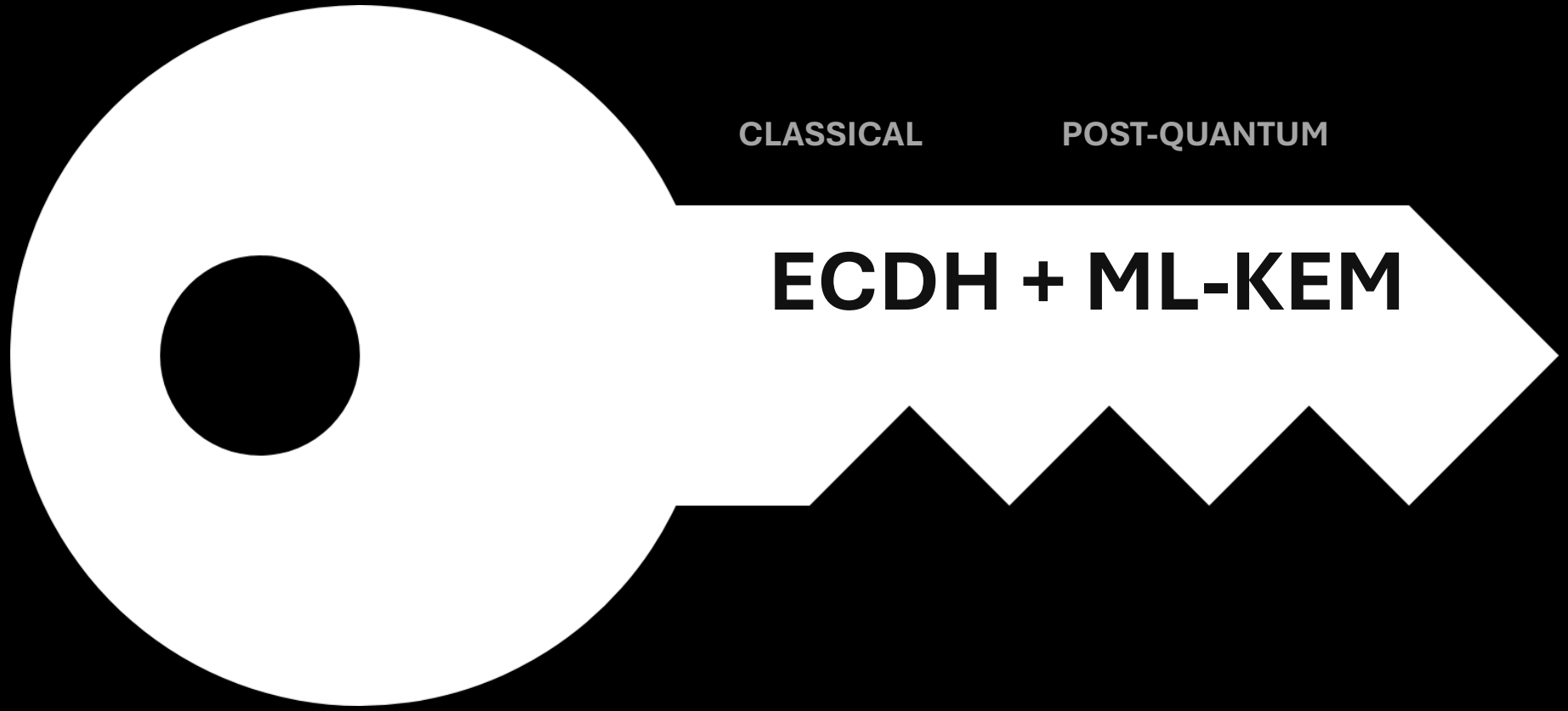
Verify identity or integrity

ASD’s ISM prefers ML-DSA-87. SLH-DSA is outside its approved list.

NIST FIPS 203, 204 and 205 / ASD Information Security Manual

QUT

Hybrid key establishment



ASD discourages hybrids. If you use one, plan an off-ramp to standalone PQC.

IETF RFC 10024 / ASD Information Security Manual / Key artwork from the Queensland briefing

QUT

The transition happens in layers

KEY ESTABLISHMENT

Roll out post-quantum key establishment

SIGNATURES AND PKI

Plan and test now | **Signature and PKI rollout**

Why key exchange first?

Early key exchange upgrades can protect today's traffic from future decryption.

Hybrid TLS can ship while teams work on certificates and trust chains.

IETF RFC 10024 and RFC 9958 / ASD PQC planning guidance

QUT

ASD’s post-quantum timeline

BY END OF

2026

Refined transition

plan

BY END OF

2028

Transition underway

Critical systems first

BY END OF

2030

Transition

complete

ASD’s first milestone is at the end of this year.

What readiness looks like

Exposure	Where does the organisation depend on public-key crypto?
Priorities	Which data stays sensitive? What takes longest to replace?
Transition plan	Who owns the work and what will it take to deliver?

Questions?

