

Quantum-Safe Queensland

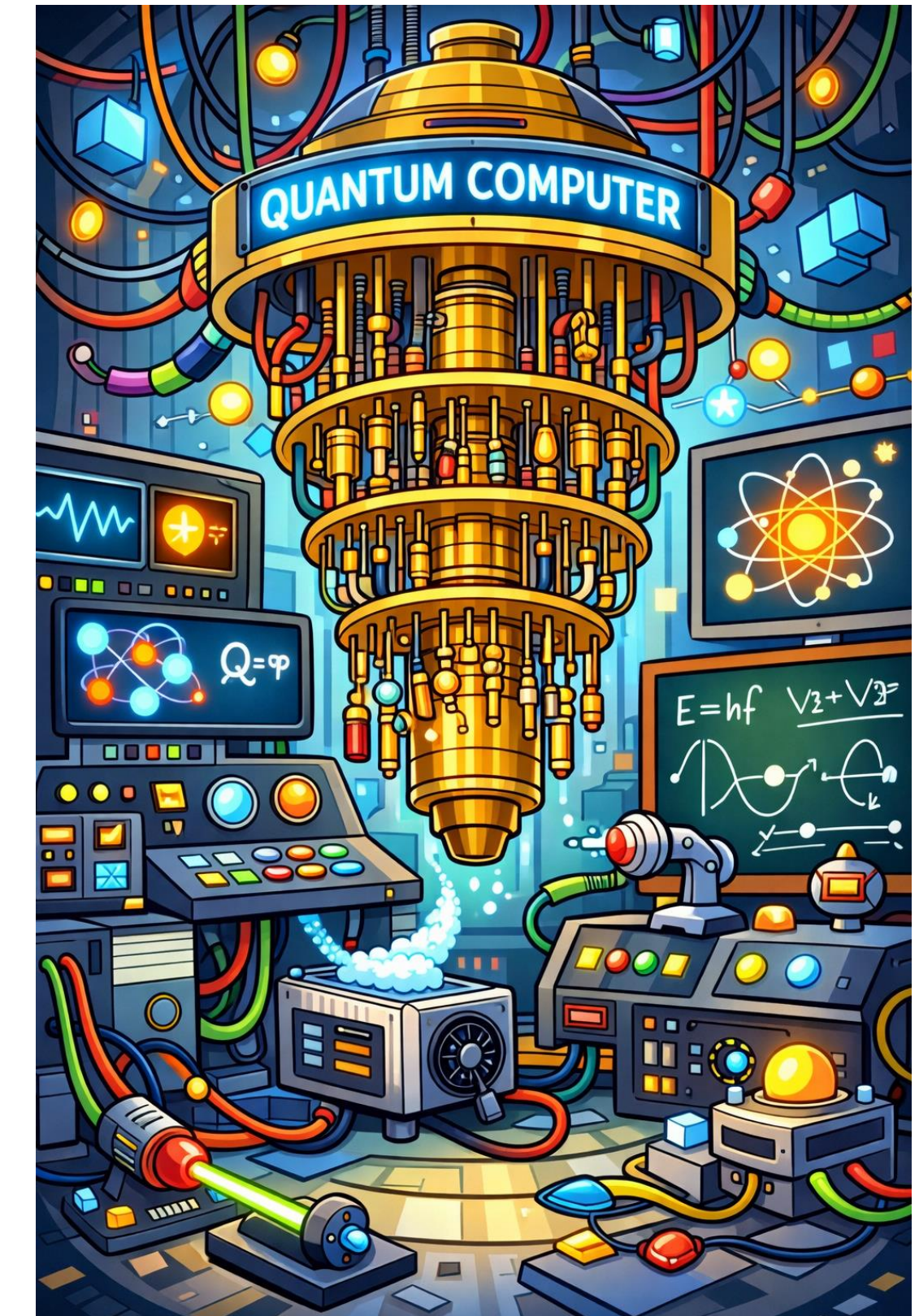


Craig Costello
QUT



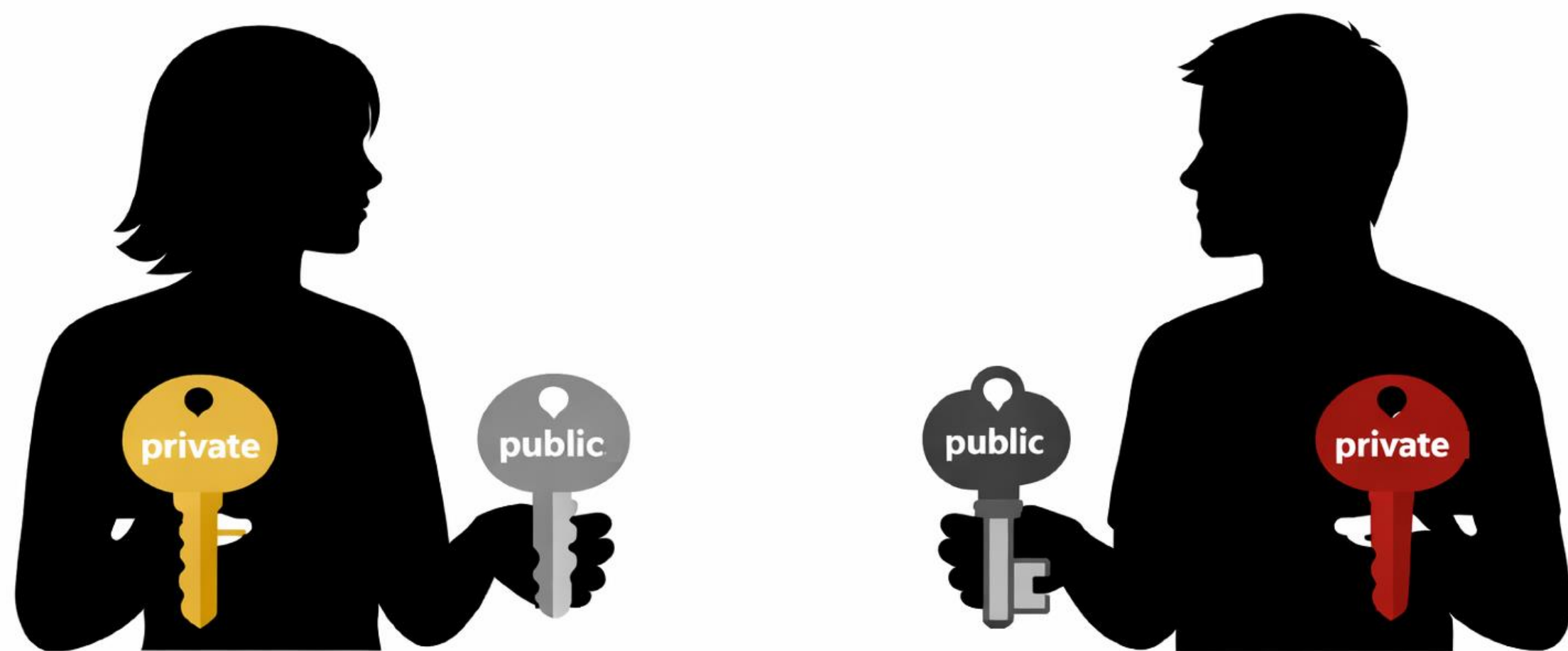
In a nutshell...

1. Public-key cryptography (PKC) underpins trust
2. A large enough quantum computer breaks currently deployed PKC
3. Migration to quantum-safe PKC takes years



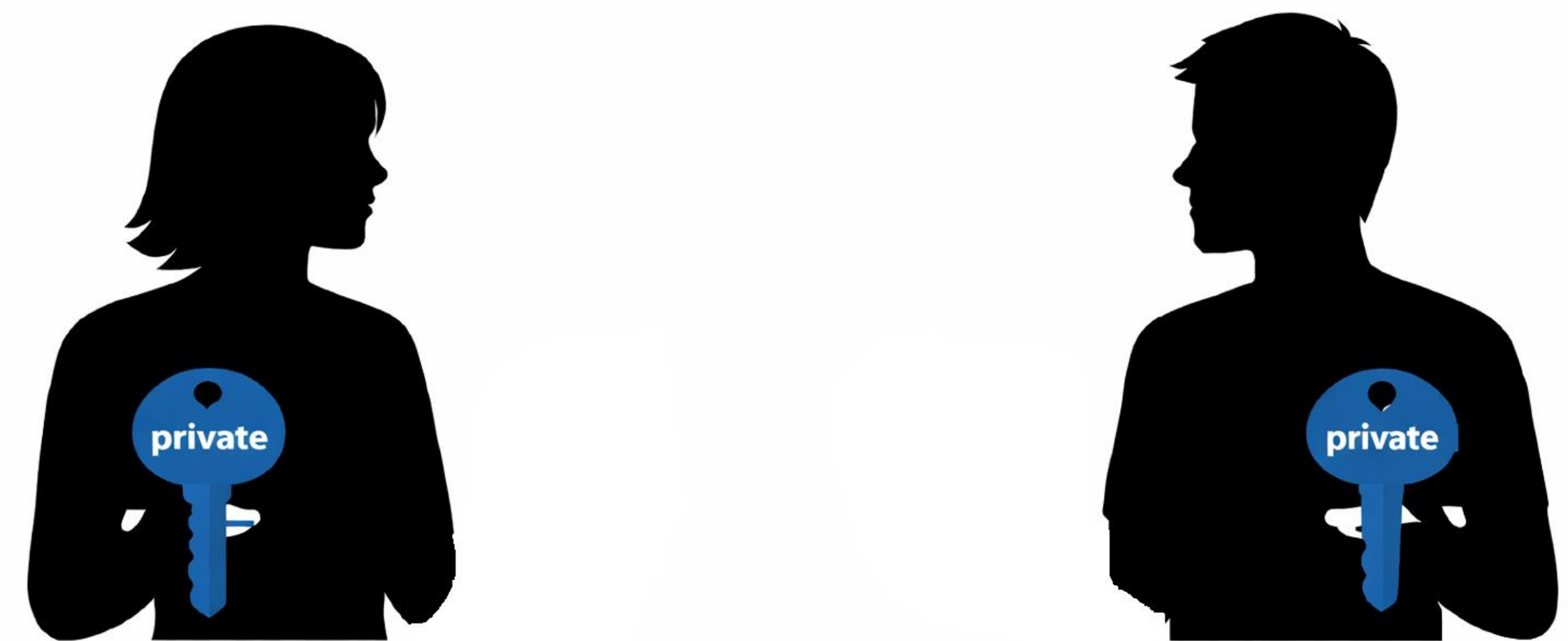
Asymmetric vs. symmetric cryptography

Asymmetric key cryptography



(e.g. DH, ECDH, RSA, ECDSA)

Symmetric key cryptography



(e.g. AES, HMAC)

What breaks

- 1976: Diffie-Hellman (DH) key exchange - assumes discrete logarithm problem (DLP) is hard

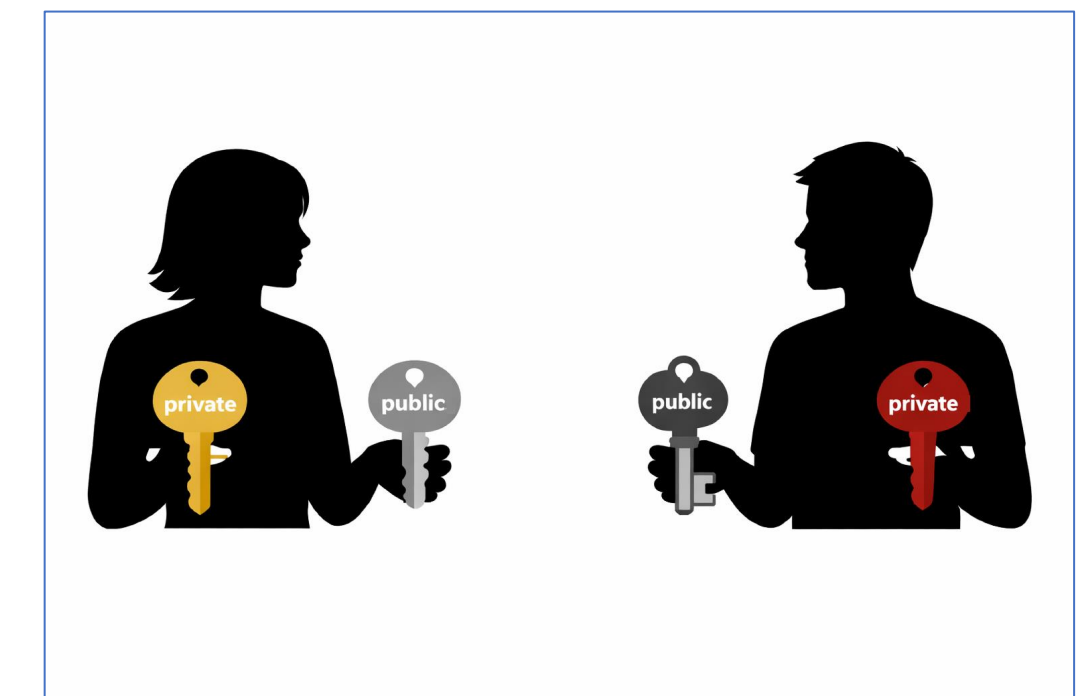
$$3^x \equiv 12 \pmod{17} \quad \dots x = ?$$

- 1978: Rivest-Shamir-Adelman (RSA) signatures - assumes factoring integers is hard

$$247 = p \times q \quad \dots p = ?, q = ?$$

- 1985: Miller-Koblitz introduce elliptic curves to crypto - assumes ECDLP is hard

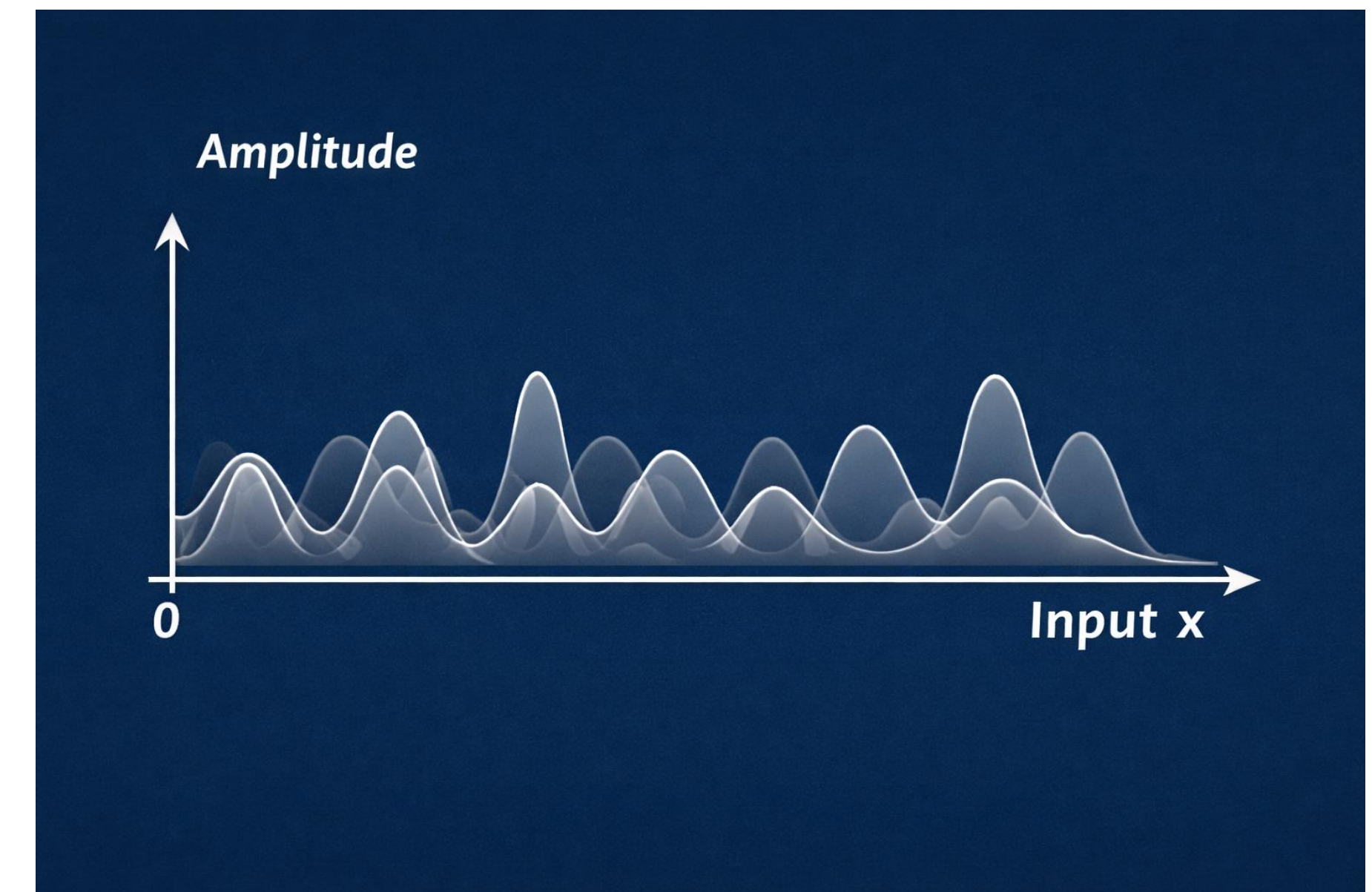
$$Q = [x]P \quad \dots x = ?$$



- 1976 – present day: all standardised/widely used PKC based on (EC)DLP and factoring: DH, ECDH, RSA, ECDSA

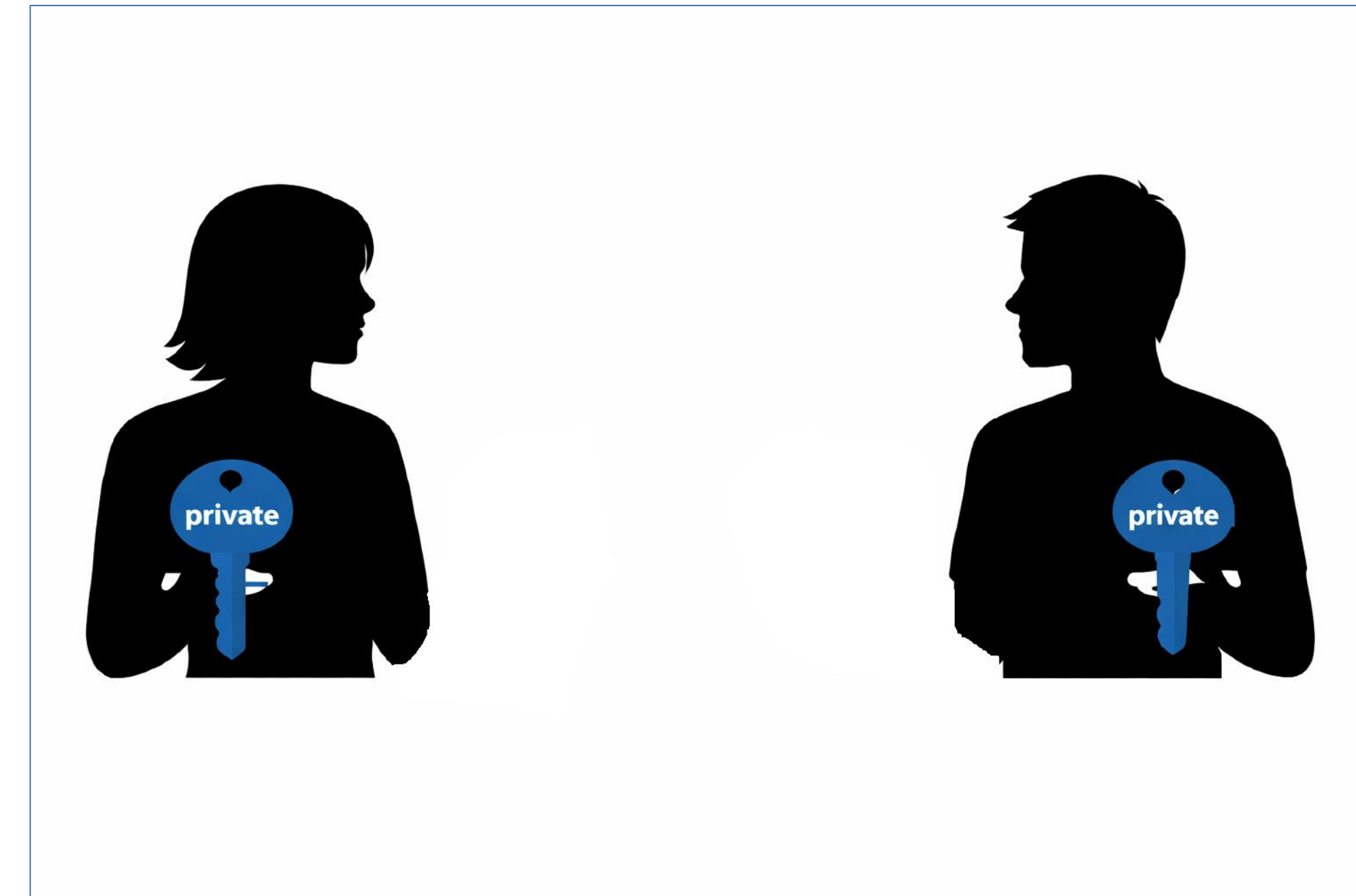
How it breaks

- **1994:** Shor gives polynomial time *quantum* algorithm for factoring and discrete logarithms
- Finding factor of N reduces to finding period of $f(x) = a^x \pmod{N}$
i.e. finding r such that $f(x + r) = f(x)$
- Evaluate $f(x)$ in quantum superposition: $|\psi\rangle = \frac{1}{\sqrt{Q}} \sum_Q |x\rangle |f(x)\rangle$
- QFT detects the interference (i.e. period) $\frac{Q}{r}$ in Fourier domain
- Post-processing reveals r , and $\gcd(a^r \pm 1, N)$ gives non-trivial factor of N



What mostly doesn't break

- **1996:** Grover gives $O(\sqrt{N})$ algorithm for quantum search
- **Symmetric encryption** (e.g. AES)
 - Classical brute force key search: try all 2^k keys
 - Quantum brute force key search: try $\approx 2^{k/2}$ keys
- **Hash functions**
 - Preimage search: 2^k classical vs. $2^{k/2}$ quantum
 - Collisions: $2^{k/2}$ classical vs $2^{k/3}$ quantum
- Upshot: choose stronger parameters (eventually), no urgent action needed
- ASD: “[*impact*] is unlikely to be felt for some time”



Harvest now, decrypt later

- Urgency depends on data shelf life
- Encryption is the priority
- Mosca's theorem:

x : shelf-life

y : migration time

z : time to CRQC / Q-day

if $x + y > z$, then worry...

- Digital signatures have $x = 0$, encryption $x \gg 0$



Q-day reality

- We don't need a date to justify action
- Historically, quantum hardware announcements have been a Q-day yardstick
- Very recent breakthroughs are working from the other direction
 - **June 9, 2025 – Gidney, Google Quant AI, USA**
“How to factor 2048-bit RSA with less than a million noisy qubits”
 - **Feb 12, 2026 – Iceberg Quantum, Sydney**
“Reducing the cost of breaking 2048-bit RSA to 100,000 physical qubits”
 - **Mar 25, 2026 – Google, Inc.**
 - “Quantum frontiers may be closer than they appear”
 - “PQC migration by 2029”

quantum
compute
Shor needs
(*qubits*)

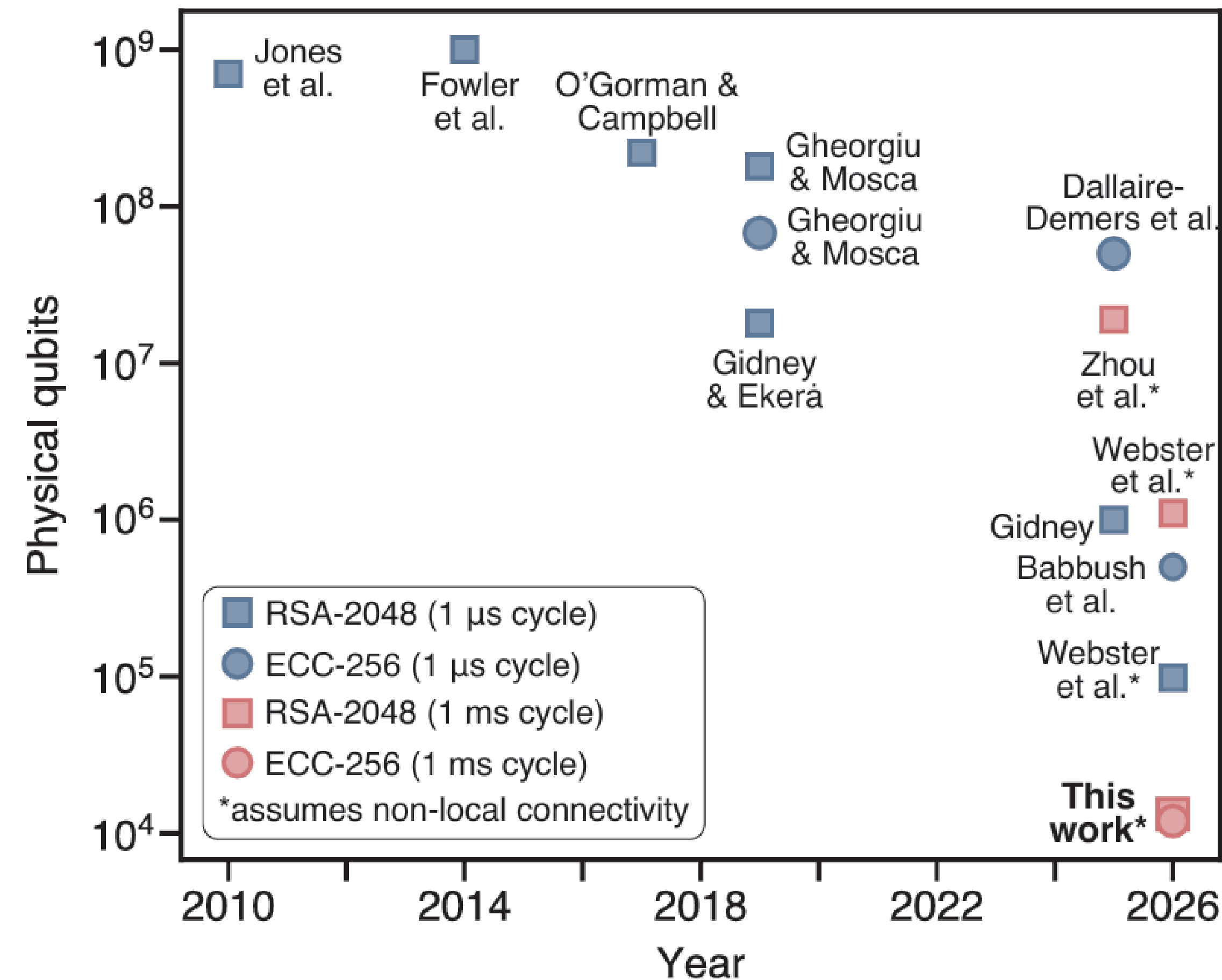


quantum
compute
we have
(*qubits*)



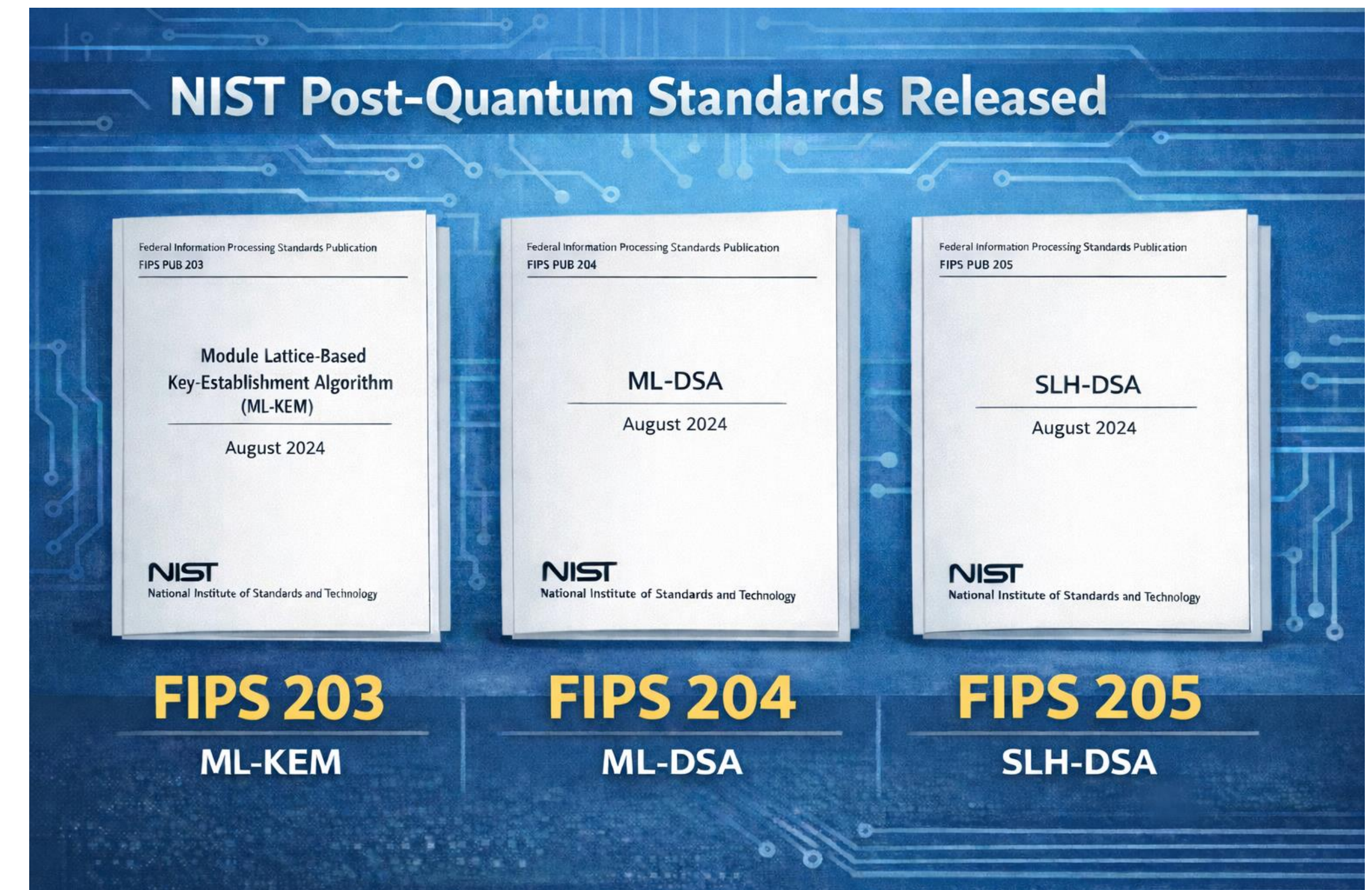
Why some skeptics are changing tone...

- Mar 31, 2026 - Oratomic/Caltech/Berkeley
“Shor’s algorithm is possible with as few as 10,000 reconfigurable atomic qubits”



PQC standards exist now

- FIPS 203 = Lattice-based key encapsulation
FIPS 204 = Lattice-based digital signatures
FIPS 205 = Hash-based digital signatures
- E.g. FIPS 203 (ML-KEM) – three security levels
ML-KEM-512 ($\approx$ AES-128)
ML-KEM-768 ($\approx$ AES-192)
ML-KEM-1024 ($\approx$ AES-256)
- Reminder: quantum computers not required for deployment
- ASD: only ML-KEM-1024, ML-DSA-87 beyond 2030

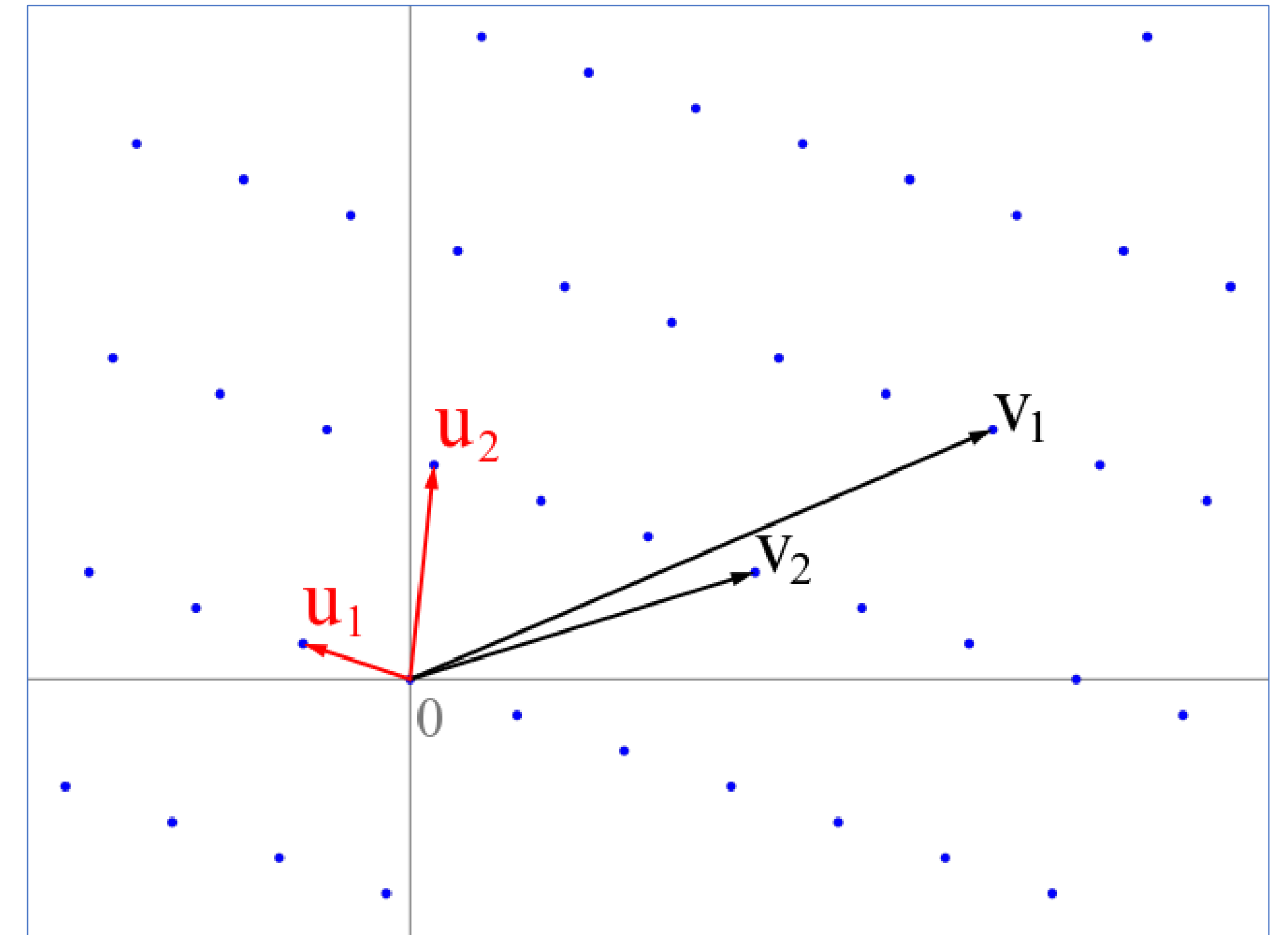


Learning with errors and lattice-based crypto

- 2005 Regev - Learning with errors (LWE) problem

easy	hard
$\begin{cases} 2x + y = 7 \\ 3x + 2y = 12 \\ -x + y = 1 \end{cases}$	$\begin{cases} 2x + y \approx 8 \\ 3x + 2y \approx 12 \\ -x + y \approx 0 \end{cases}$

- Reduction:** if you can solve LWE in average case, you can solve GapSVP (via quantum alg.) in the worst case for all lattices
- ML-KEM-512: think 512 noisy equations mod q , with some structure in the equations...
- ASD: ML-KEM-1024, ML-DSA-87 beyond 2030



Good ($\{u_1, u_2\}$) and bad ($\{v_1, v_2\}$) bases for a 2D lattice

Hybrid is the bridge

- Wise to do classical+PQ hybrids (for a while)
e.g. ECDH+ML-KEM



Australian Government
Australian Signals Directorate

Post-quantum/ traditional hybrid schemes

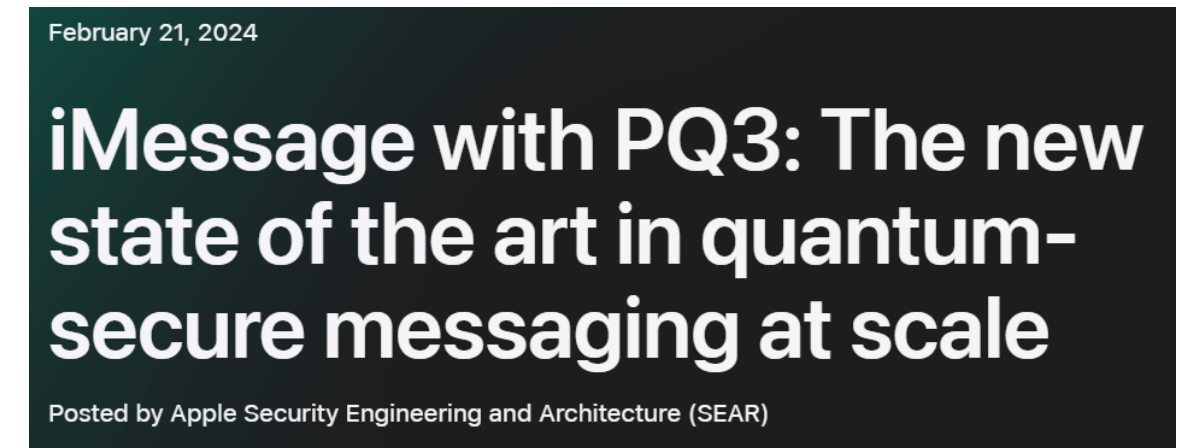
ASD does not recommend, but does not prohibit, the use of post-quantum/ traditional (PQ/T) hybrid schemes. For interoperability and resiliency reasons, organisations may consider a PQ/T hybrid scheme in their PQC transition. However, the presence of a CRQC will render traditional elements of PQ/T hybrid schemes obsolete. This means that all organisations should expect to transition to purely post-quantum cryptographic algorithms in the future.

- Internet (IETF): TLS 1.3 takes X25519MLKEM768 hybrid

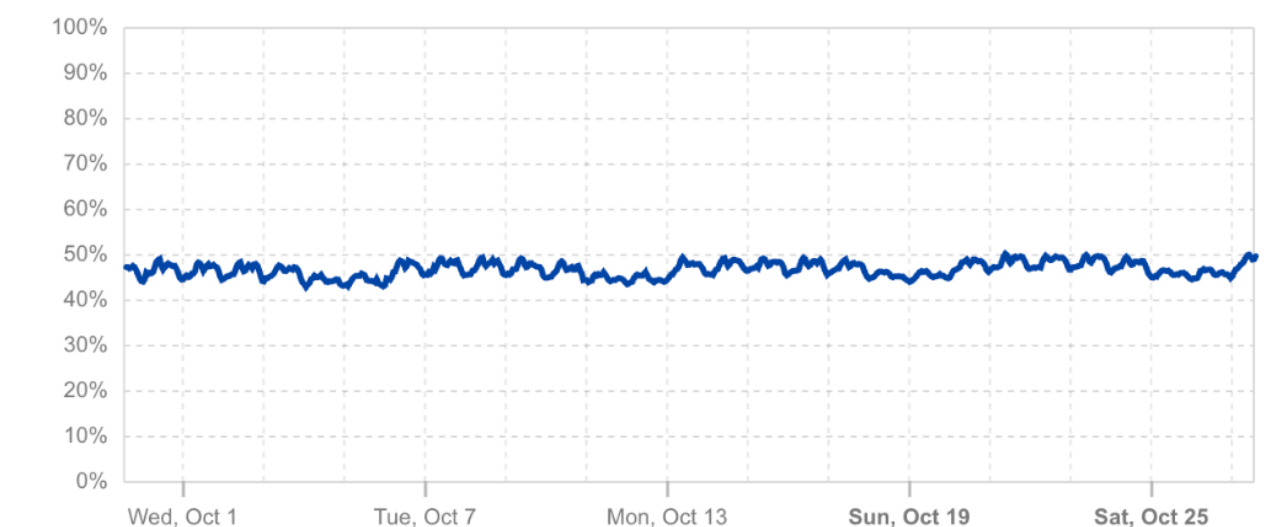


Proof it's real

- Feb 2024: iMessage goes quantum-secure hybrid
“ensuring that PQ3 can can never be less safe than the existing classical protocol”
- May 2024: Chrome (TLS 1.3 and QUIC) defaults to PQC hybrid for key establishment
- October 2025: CloudFlare announces “majority of human-initiated traffic” is protected with PQC (hybrid)



[iMessage with PQ3 - Apple Security Research](#)



[State of the post-quantum Internet in 2025](#)

Authentication is harder

- Two reasons key exchange/encryption comes first
 1. Harvest now, decrypt later
 2. Much easier
- Authentication (i.e. digital signatures) requires we change global certificate ecosystem
- Certificates/CT proofs exchanged in latency-sensitive handshakes (PQC sigs large!), e.g. Google has no immediate plans to add PQC X.509 certs to Chrome Root Store. Instead pursuing Merkle Tree Certificates (MTCs) through IETF
- IETF standardised X.509 identifiers for ML-DSA, foundational building block for cert ecosystem

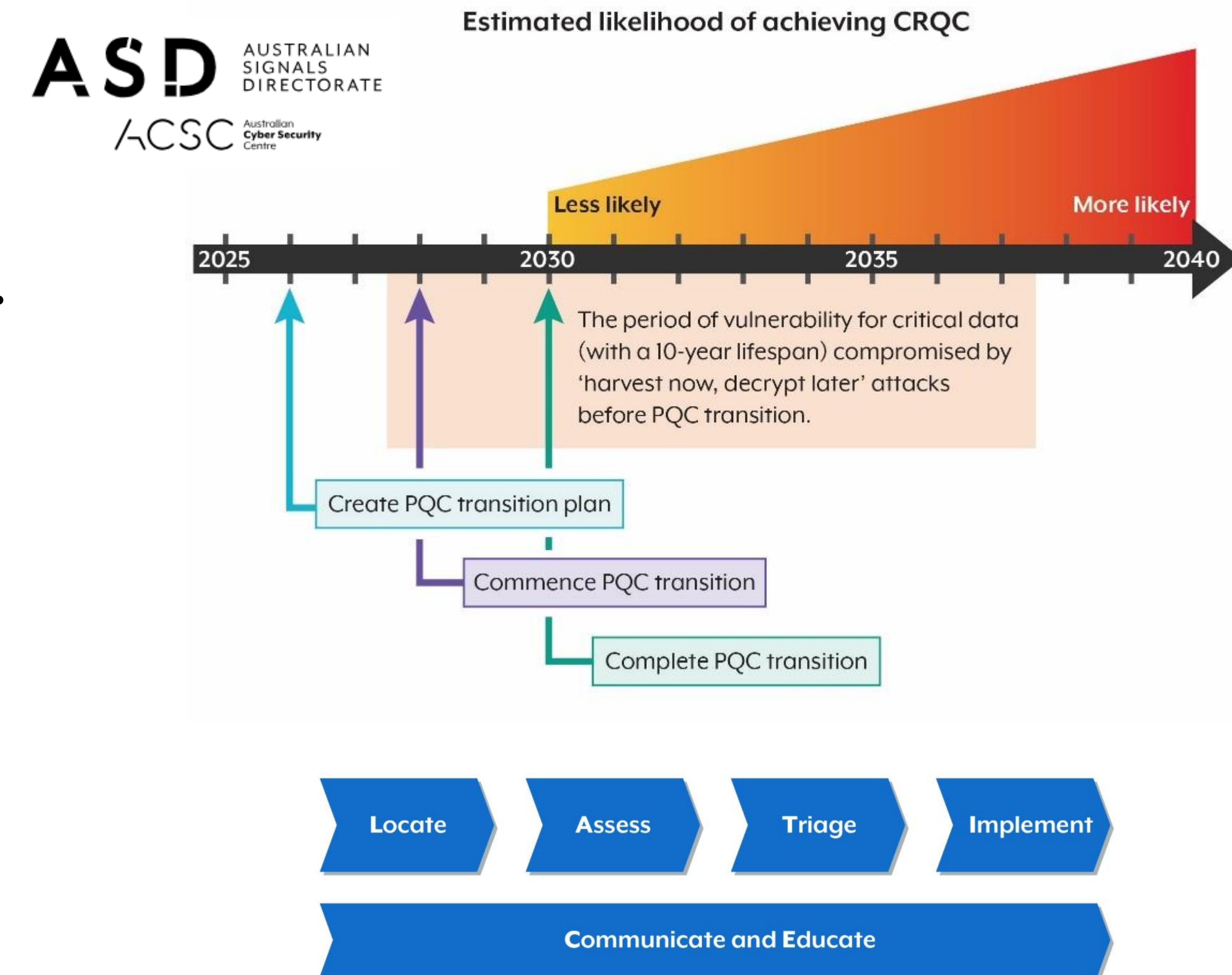
Queensland forcing function

- QLD Gov: - Quantum and Advanced Technologies strategy – “The Quantum State”
 - public claims of being first state to deliver comprehensive quantum strategy
 - Quantum Innovation Queensland supports strategy implementation
 - Commonwealth+QLD gov \$1 B investment to PsiQuantum
- QLD Gov is accelerating local quantum economy
- ASD is accelerating the crypto transition nationally
- Thus, QLD orgs will be asked more & more: “*What’s our quantum-safe plan?*”

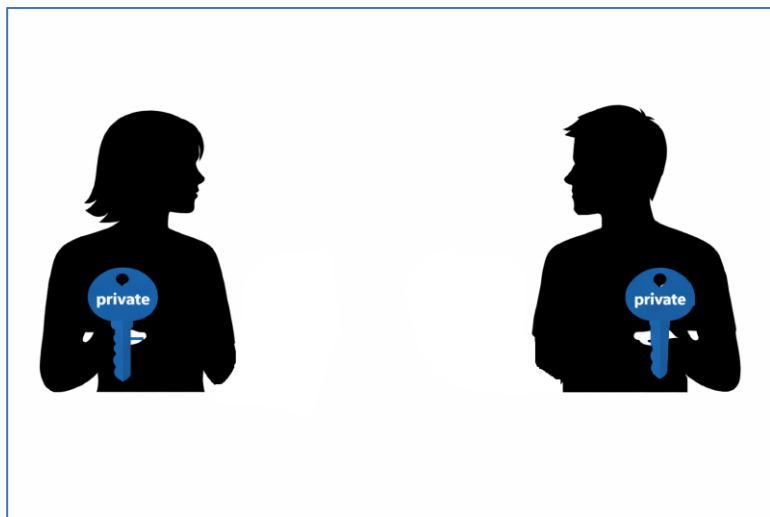
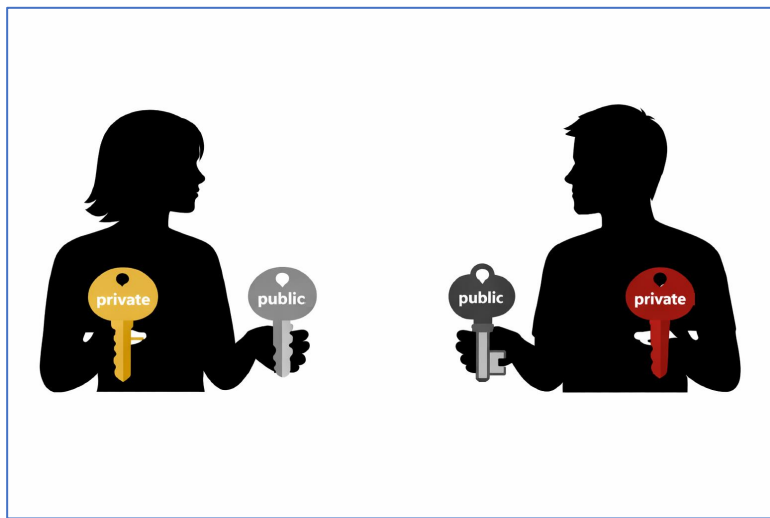


What QLD organisations can do

- **ASD:** 2026 plan / 2028 implement / 2030 complete
- **QLD priority areas:** where HNDDL urgency likely bites...
 - Health and personal data retention
 - Energy, sources, critical infrastructure operational and engineering data
 - Government identity, investigations, legal archives
 - Research IP (value horizon measured in decades)



What breaks, what changes, what to do



Cryptographic job	Common “today” algorithms/systems	Quantum impact	Practical migration consequence
Key exchange / key establishment	RSA key transport; (EC)DH / ECDH in TLS/VPN; SSH key exchange	Broken by Shor on CRQC	Prioritise ML-KEM rollout (often hybrid first) across TLS/VPN/SSH; plan for long tail
Digital signatures / authentication	ECDSA / RSA signatures in PKI, code signing, identity assertions	Broken by Shor on CRQC	Harder/longer: cert formats, HSMs, audits, trust stores, signature sizes
Bulk encryption	AES-GCM, ChaCha20-Poly1305	“Weakened” (speedup) rather than broken outright	Prefer higher security margins (e.g., AES-256) for long-term maintainability
Hashing	SHA-2 / SHA-3 families	“Weakened” (speedup) rather than broken outright	Prefer higher security margins (e.g., SHA-384/512) for long-term maintainability

The work checklist

- **Next week**
 1. Stand up PQC transition owner + steering
 2. Identify where RSA/ECC are used for key exchange, signatures, code signing
.... list top-10 systems by “*confidentiality lifetime × exposure*”
 3. Export certificate inventories: where certs issued, stored, rotated: what’s the failure mode if you had to rotate in 30 days
- **Next month**
 1. Run a crypto discovery scan / CBOM exercise (focus: TLS endpoints, SSH, VPN, identity stack)
 2. Pilot hybrid ML-KEM in one controlled environment (e.g., a non-critical TLS stack) and capture breakages
 3. Update procurement templates with PQC-readiness clauses and vendor evidence requirements
- **Next quarter**
 1. Publish your Phase 1 plan and prioritised backlog aligned to ASD milestones.
 2. Begin engaging managed service providers and SaaS vendors on their PQC timelines and their certificate automation capacity

Window	Deliverable	What “done” looks like
Now → end-2026	Refined PQC transition plan	Crypto inventory baseline; prioritised systems; vendor readiness assessment; program governance
2027 → end-2028	Begin implementation (critical first)	Hybrid ML-KEM in TLS where feasible; pilots for PKI/signatures; rotation playbooks
2029 → end-2030	Scale-out + completion	Deprecation of quantum-vulnerable public-key in supported footprints; operational monitoring



Executive one-page brief

“We’re executing a crypto transition program...”

- **Primary goal:** Maintain confidentiality and trust through a staged transition aligned to ASD milestones plan by end-2026; begin implementing by end-2028; complete by end-2030
- **Next 90 days:**
 1. Complete a crypto inventory (certificates, key exchange, signing, KMS/HSM, libraries) and identify top dependencies
 2. Classify data by confidentiality lifetime and exposure to interception (HNDL triage)
 3. Pilot hybrid ML-KEM in a controlled TLS environment and surface interoperability issues early
 4. Update procurement templates to require PQC readiness and crypto agility beyond 2030
- **Board decisions:**
 1. Approve a 2026-2030 PQC transition program with a named executive sponsor
 2. Approve “crypto agility” as a mandatory procurement requirement for all systems
- **Measuring progress:**

% of critical systems with known crypto dependencies; % of externally exposed TLS endpoints capable of hybrid ML-KEM; certificate rotation time; vendor readiness scorecard coverage

