# QUANTUM-SAFE CRYPTOGRAPHY

## Preparing for the Post-Quantum Era

May 2026

# Current State of Quantum Computing Relative to Cryptography

Where hardware, algorithms, standards, and timelines stand today

# Quantum vs Classical Computing

Superposition: both states at once

Entanglement: Measure one, know the other

# Quantum vs Classical Computing

Why Shor's and Grover's Algorithms Matter

## Shor's Algorithm

- Factors large integers and solves discrete logarithms in polynomial time
- Breaks RSA, ECC, and Diffie-Hellman — the foundation of public-key cryptography
- Exponential speedup over classical: turns millennia into hours
- Requires a fault-tolerant quantum computer with enough logical qubits

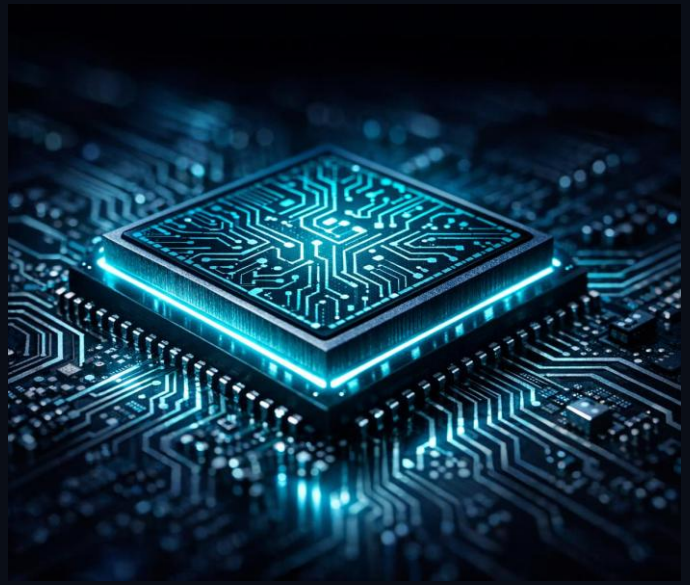
## Grover's Algorithm

- Searches unsorted databases in $\sqrt{N}$ time — quadratic speedup
- Halves the effective security of symmetric keys: AES-256 → 128-bit equivalent
- Impact is manageable: double key sizes (AES-128 → AES-256) to compensate
- Hash functions similarly weakened but SHA-384+ remains adequate

# Where Hardware Stands Today

Resource estimates are falling faster than hardware is scaling — and that's the problem

| | | |
|---|---|---|
| 2019 | **20M qubits** | Gidney original RSA-2048 estimate |
| May 2025 | **<1M qubits** | Gidney revised — 20× reduction via algorithmic improvements alone |
| Feb 2026 | **~100K qubits** | Iceberg Quantum Pinnacle architecture using QLDPC codes |
| Mar 2026 | **~10K qubits** | Oratomic/Caltech — reconfigurable neutral atoms (ECC-256) |



*Hardware milestones: Google Willow (105 qubits, Dec 2024) • Microsoft Majorana topological qubits (2025) • QuEra 96 logical qubits (Jan 2026)*

# Standards and Policy Landscape

| Standard | Algorithm | Type | Replaces | Status |
|---|---|---|---|---|
| **FIPS 203** | ML-KEM | Key Encapsulation | RSA, ECDH, DH | Final (Aug 2024) |
| **FIPS 204** | ML-DSA | Digital Signature | RSA-PSS, ECDSA | Final (Aug 2024) |
| **FIPS 205** | SLH-DSA | Digital Signature | RSA, ECDSA | Final (Aug 2024) |
| **FIPS 206** | FN-DSA | Digital Signature | RSA, ECDSA | Draft (exp. 2026) |
| **TBD** | HQC | Backup KEM | Code-based alt. | Selected Mar 2025 |

## Key Policy Mandates

- NSM-10 (May 2022): Federal migration target by 2035; annual crypto inventories required under M-23-02
- CNSA 2.0 (Sep 2022): NSS must adopt PQC; new acquisitions compliant by Jan 2027; full compliance by 2031-2033
- NIST CSWP 39 (Dec 2025): Crypto agility elevated from buzzword to design imperative
- BSI (Germany): PQC migration deadline 2030 for critical infrastructure

# What Is a "Cryptographically Relevant Quantum Computer"?

**28–49%**

probability of a CRQC within 10 years

**51–70%**

probability within 15 years

## Enterprise Framing

- A CRQC can execute Shor's algorithm at scales that break RSA-2048 and ECC-256 in operational time
- Threshold is not a single number — it depends on architecture, error correction, and runtime tolerance
- Migration timelines (3-7 years) mean the decision window is now, not when a CRQC arrives
- GRI 2025 survey: experts say timeline has accelerated from prior reports

*Source: Global Risk Institute Quantum Threat Timeline Report 2025 (26 expert survey)*

*The question is not whether quantum computers will break today's encryption — it's whether your migration will finish before they do.*

II

# Current Risks Posed by Quantum Computers on Cryptography

What's vulnerable, what's exposed, and how attacks unfold

# Algorithms at Risk

| Algorithm | Type | Quantum Attack | Impact | PQC Replacement |
|---|---|---|---|---|
| **RSA** | Public Key / Sig | Shor's | Completely broken | ML-KEM / ML-DSA |
| **ECC / ECDSA** | Key Exchange / Sig | Shor's | Completely broken | ML-KEM / ML-DSA |
| **Diffie-Hellman** | Key Exchange | Shor's | Completely broken | ML-KEM |
| **AES-128** | Symmetric | Grover's | Halved to 64-bit | AES-256 |
| **AES-256** | Symmetric | Grover's | Reduced to 128-bit | Remains adequate |
| **SHA-256** | Hash | Grover's | Weakened, usable | SHA-384+ |

Public-key cryptography is existentially threatened. Symmetric and hash algorithms need parameter upgrades, not replacement.

# Use-Case Mapping: What's Exposed

## TLS / HTTPS

Every web connection uses RSA/ECC key exchange. Hybrid ML-KEM already shipping in Chrome, Edge and Firefox.

## Code Signing

Software updates, firmware, and packages rely on RSA/ECDSA signatures.

Compromised signing = supply chain attacks.

Digital Media and Software License Keys.

## VPN / Ipsec / WPA

IKEv2 key exchange uses DH/ECDH. Hybrid PQC via RFC 9370 available but adoption is early.
Wi-Fi uses TLS with RSA/ECDSA certificates or PAKE over finite fields/ECC for key exchange.
BGPSEC and DNSSEC.

## PKI / Certificates

X.509 certificate chains use RSA/ECDSA. Larger PQC signatures impact handshake performance.

Oauth, SAML, WebAuthn, Fido2, EMV, RFID.

## Archived Backups

Encrypted data stored today with RSA/AES key wrapping is vulnerable to future decryption.

## Blockchain / DeFi

ECC underpins all major cryptocurrencies. Google's March 2026 paper specifically targets ECC-256. Also, legacy banking SWIFT MT Messages.

# Attack Scenarios and Timelines

## Harvest Now, Decrypt Later Is Already Happening

### 1 HARVEST

Adversaries intercept encrypted traffic today — VPN sessions, TLS connections, archived data. Storage is cheap (<$20K/PB). Nation-states operate dedicated data centers.

### 2 STORE

Data sits in storage for years. Nothing active happens. Detection is nearly impossible. Intelligence agencies in multiple countries are actively warning this is underway.

### 3 DECRYPT

When a CRQC is operational, stored data is decrypted. Information that was secure when transmitted becomes readable. The damage is irreversible.

Vulnerability condition: Ld > Ha — if data confidentiality lifetime exceeds the attacker's decryption horizon, that data is compromised

# Attack Scenarios and Timelines

**Harvest Now, Decrypt Later Is Already Happening**

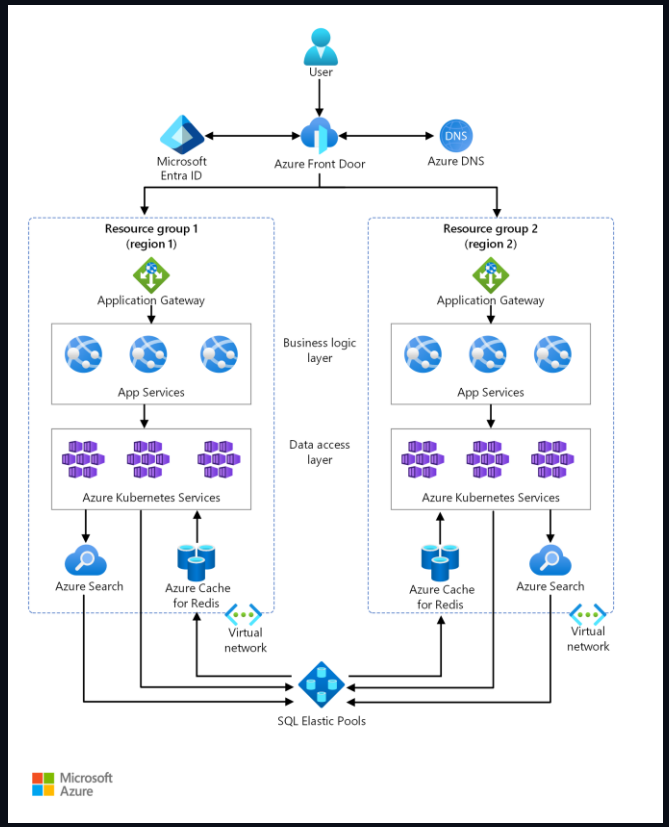
## 1 HARVEST

How many places is TLS used?

How many RSA/ECC/DH keys are used?

How many network segments are involved in transmission of the data?

Who operates the networks who transmit the data?



# Risk Assessments Companies Should Perform

Inventory, classify, model, and prioritize before you migrate

# Inventory and Data Lifetime Analysis

## Cryptographic Asset Inventory

- Map all cryptographic algorithms in use across the enterprise
- Catalog keys, certificates, and their expiration/rotation schedules
- Identify cryptographic libraries and their versions (OpenSSL, BoringSSL, etc.)
- Document where each algorithm is deployed: TLS endpoints, databases, APIs, backups
- Build a Cryptographic Bill of Materials (CBOM) per NIST CSWP 39 guidance
- M-23-02 requires annual inventory submissions — use this as your template

ACTION ITEM

## Data Lifetime Analysis

- Classify data by required confidentiality duration (1yr, 5yr, 10yr, 25yr+)
- Identify regulatory/legal retention requirements (HIPAA, GDPR, SOX)
- Map data categories to HNDL risk levels:
  - Healthcare records: lifetime confidentiality → critical risk
  - Government classified: 25yr+ → critical risk
  - Financial data: 7-10yr → high risk
  - Marketing data: 1-2yr → low risk
- Apply vulnerability condition: Ld > Ha = compromised

ACTION ITEM

# Threat Modeling and Prioritization

## HNDL Channel Identification

- Map all channels where adversaries can intercept encrypted data in transit
- Internet-facing TLS/VPN endpoints are highest priority
- Internal network segments with sensitive data flows
- Cloud provider interconnects and API traffic
- Backup replication channels and archival transfers

## Prioritization Matrix

ACTION ITEM

| Factor | Weight | Inputs |
|---|---|---|
| Data Value | High | Revenue impact, regulatory penalties |
| Confidentiality Lifetime | High | Years data must stay secret |
| Exploitability | Med | Internet-facing vs. air-gapped |
| Remediation Cost | Med | Rewrite vs. config change |
| Vendor Dependency | Low | PQC readiness of supply chain |

## Framework Alignment

- ISACA Risk IT Framework provides a structured approach: Governance → Risk Evaluation → Risk Response
- NIST SP 800-37 (RMF) integrates quantum risk into existing assessment cycles
- Combine data value × lifetime × exploitability × remediation cost to produce a ranked work queue

# IV What Can Be Done Now to Prepare

Crypto agility, PQC pilots, key management, and governance

# Crypto Agility and PQC Migration Pilots

## Adopt Crypto Agility

- Design systems for algorithm swap without major rewrites — modularity, abstraction, policy-driven control
- Use hybrid constructions (classical + PQC) during transition — already in Chrome/Edge/Firefox TLS 1.3
- PQC Ninja | Browsertest
- Implement centralized cryptographic configuration — no hardcoded algorithm choices
- NIST CSWP 39 provides the blueprint: maturity model from ad-hoc to adaptive

## Start PQC Migration Pilots

- Test NIST-selected algorithms in non-critical paths first — internal APIs, dev environments
- Measure performance impact: ML-DSA-65 signatures are ~50× larger than ECDSA
- Server implementations show <5% latency overhead; IoT devices up to 12× variance
- Reference deployments: Apple iMessage PQ3, Cloudflare, Google Chrome hybrid TLS
- QCready - Evaluate your TLS Quantum readiness
- PQC Lab | Keyfactor

## Key Management

ACTION ITEM

Shorten key lifetimes, centralize inventory, automate rotation

## Governance & Procurement

ACTION ITEM

Require PQC readiness in vendor SLAs and procurement templates

# Risks, Tradeoffs, and the Path Forward

## Migration Costs

Enterprise PQC migration is multi-year and resource-intensive. Crypto is embedded everywhere — every TLS endpoint, certificate, API, and library needs assessment and potential replacement.

## Performance Impacts

ML-DSA-65 signatures are ~50× larger than ECDSA. TLS handshakes slow with larger certificate chains. IoT and constrained devices face up to 12× computational variance between PQC algorithms.

## HNDL Privacy Gap

Already-harvested data cannot be retroactively protected. The privacy gap for data encrypted with RSA/ECC before migration is permanent. This is the residual risk that cannot be mitigated.

## The Window Is Now

Standards are finalized. Compliance deadlines are live. Resource estimates are falling faster than hardware is scaling.

The cost of starting now is measured in budget and engineering effort.

**The cost of waiting is measured in data that can never be re-protected.**

# References

## Articles Referenced in this Presentation


Q-Day Just Got Closer: Three Papers in Three Months Are Rewriting the Quantum Threat Timeline

Encryption timelines shorten as two groups cut qubit requirements for Shor's algorithm

10,000 Qubits to Run Shor's Algorithm

Shor, QLDPC Codes, and the Compression of RSA-2048 Resource Estimates (Part I) - Quantum Computing Report

Post-Quantum Cryptography (PQC) Standardization - 2025 Update

NIST Post-Quantum Cryptography Standards: The Enterprise Summary | Quantum Security Defence

NIST Post-Quantum Cryptography Standards in 2026: Where We Stand | Q by Wentzel

Quantum Threat Timeline Report 2025 - Global Risk Institute

CNSA 2.0 Explained: PQC Requirements and Timelines

Post-Quantum Cryptography for Government and Defense – QNSQY

CSA_CNSA_2.0_ALGORITHMS.PDF

Crypto Agility Goes from Buzzword to Blueprint - NIST Releases "Considerations for Achieving Crypto Agility"

(PDF) Harvest Now, Decrypt Later: A Time-Dependent Threat Model and Migration Framework for Post-Quantum Cryptography

Post-Quantum Cryptography Authentication Migration Guide 2026: NIST Standards and Enterprise Roadmap

Post-Quantum Cryptography: Why Enterprises Must Transition Their Encryption Now

They're Recording Everything You Send. Quantum Computers Will Read It Later. - State of Surveillance

What Is "Harvest Now, Decrypt Later" and Why Should You Care?

Crypto Agility | CSRC

A Practical Performance Benchmark of Post-Quantum Cryptography Across Heterogeneous Computing Environments

2025 Volume 10 How to Conduct a Quantum Risk Assessment Using ISACAs Risk IT Framework

QUBIP - CRQC, a 2025 perspective

(8) 2025 Was an Inflection Year for Q-Day — and China + AI Made It Sharper | LinkedIn

[2603.28627] Shor's algorithm is possible with as few as 10,000 reconfigurable atomic qubits

NIST Post-Quantum Cryptography Standards FIPS 203 204 205 Guide

Post-Quantum Cryptography for Developers: NIST's Final Standards and How to Migrate Before It's Urgent | Abhishek Gautam

Decoding NIST PQC Standards: What They Are, What's Final, and What's Next | Encryption Consulting

Quantum risk is no longer tomorrow's problem: Why U.S. organizations must act now

M-23-02

Crypto-agility and quantum-safe readiness | IBM Quantum Computing Blog

Operationalizing cryptography agility for PQC readiness | HCLTech

Quantum Computing Milestones 2025-2026: IBM, Google, IonQ, Quantinuum — Technerdo | Technerdo

Quantum 2026 — IBM Technology Atlas

IBM Unveils "Nighthawk" and "Loon" Quantum Chips: Milestones Toward Quantum Advantage and Fault Tolerance

Quantum Computing: IBM Shares New Chip, New Timeline To Quantum Advantage

Quantum Computing Progress in 2026: IBM, Google, and What Developers Should Watch | iBuidl.org

Crypto Agility Is the New Foundation for PQC Migration

Crypto Agility & Post-Quantum Cryptography (PQC) Migration Framework - Crypto Agility Made Easy

Post-Quantum Cryptography: Creating Truly Secure Communications

Shor's Algorithm: Why Quantum Computers Threaten | H33 Blog

Post-quantum readiness and cryptographic transition planning for enterprise cloud | Cybersecurity | Springer Nature Link