

What quantum computing means for the **encryption** behind your AI

No quantum computer can break RSA today. The size of the machine needed keeps shrinking, and your AI stack rests on the algorithms it would break.

Six things this deck covers

- 01 Which encryption a quantum computer breaks
 - 02 How fast the estimates have fallen
 - 03 What experts expect in the next ten years
 - 04 Where AI systems depend on public-key cryptography
 - 05 The standards and the regulators' dates
 - 06 Six steps to take this year
-

Which algorithms quantum computers break

Algorithm	Large quantum computer
RSA	Broken
Elliptic-curve (ECDH, ECDSA)	Broken
Diffie-Hellman	Broken
AES-128	Weakened; move to AES-256
AES-256, SHA-256	Remain secure

Shor's algorithm breaks key exchange and signatures. Grover's algorithm only halves symmetric key strength. Sources: NIST IR 8547 draft; UK NCSC.

<1 million

noisy qubits to factor RSA-2048 in under a week

The 2019 estimate was 20 million qubits. Gidney, Google Quantum AI, 2025. In March 2026 Google cut the estimate for 256-bit elliptic curves by about twentyfold, to under 500,000 physical qubits.

28–49%

**chance of a cryptographically
relevant quantum computer within
ten years**

Averaged estimate from 26 experts, the highest ten-year figure in the survey's seven-year history. Global Risk Institute, Quantum Threat Timeline Report 2025.

Where AI rests on public-key cryptography

Training data and prompts cross networks on elliptic-curve key exchange

Model weights are encrypted with AES, but their keys are wrapped and shared with RSA or elliptic curves

Model files are vouched for by digital signatures

AI agents prove who they are with signed tokens and certificates

Generated media carries signed provenance

The two risks arrive at different times

Harvest now, decrypt later

WHAT FAILS

Confidentiality

WHEN

Exposure has already started

FIX

Hybrid ML-KEM key exchange now

Forged signatures

WHAT FAILS

Authenticity

WHEN

From the day a large quantum computer exists

FIX

Plan the ML-DSA migration

The standards and the deadlines

Body	Date
NIST	FIPS 203, 204, 205 published August 2024
Google	Own migration complete by 2029
NIST IR 8547 draft	RSA-2048 and P-256 deprecated after 2030
EU roadmap	High-risk systems migrated by end 2030
UK NCSC	Discovery 2028, priority 2031, full 2035
MAS	Crypto inventory and strategy, advisory 2024

Six steps to take this year

- 01 Inventory cryptography across the AI stack
 - 02 Rank data by how long it must stay secret
 - 03 Turn on hybrid ML-KEM key exchange
 - 04 Plan ML-DSA for model signing and agent credentials
 - 05 Make algorithms configuration, so they can be swapped
 - 06 Write post-quantum dates into AI vendor contracts
-

Start the migration in the AI stack this year

Data taken today can be read later. The inventory is the first step, and most organisations have not mapped their AI platforms yet.



Terence Kok · AI & Innovation Strategist

[SAVE](#) · [COMMENT](#) · [FOLLOW](#)