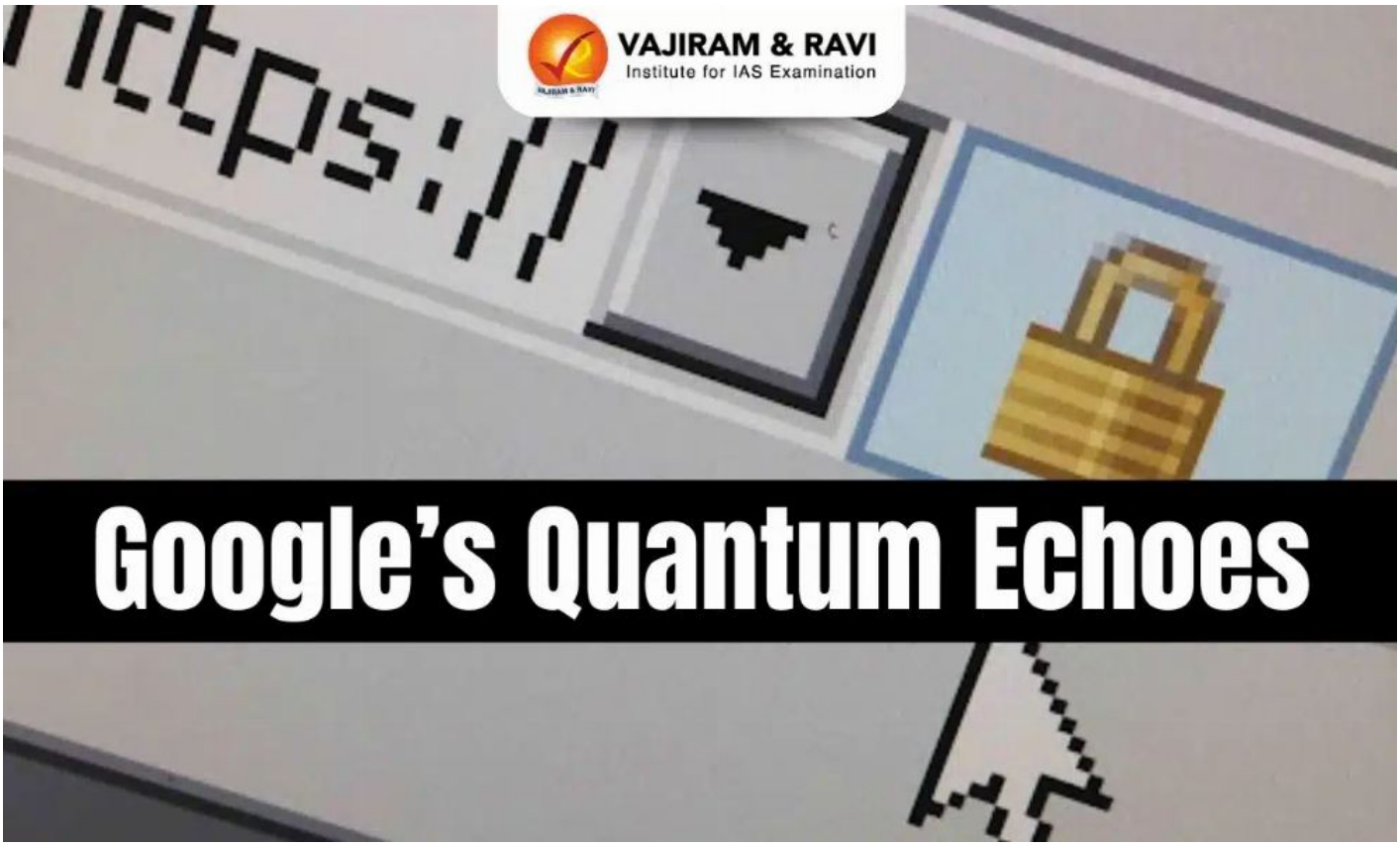
Google’s Quantum Echoes Explained: What It Really Means for Q-Day

December 10, 2025 • vajiramandravi.com



Google’s Quantum Echoes Latest News

- Google’s new **Quantum Echoes** experiment used a 65-qubit quantum processor to study how information moves around inside a quantum system.
- Unlike Google’s 2019 **Sycamore** experiment, which focused on speed, this work was about understanding how quantum bits behave.
- Scientists measured **out-of-time-order correlators (OTOC)** — tiny echoes that reveal how disturbances travel through a network of qubits.
    - Basically, scientists gave the system a tiny “poke,” reversed its evolution, and looked for a small “echo” that came back.
    - This echo helped them see how quickly information spreads or gets scrambled among qubits.
- These insights can help in studying new materials, superconductors, and chemical reactions.
- Even though the research is scientifically important, it does not bring us closer to **Q-day** — the point when quantum computers could break modern encryption. It poses no threat to security systems today.

Q-Day

- Q-day is the future moment when a powerful quantum computer can break today's commonly used encryption systems.
- This doesn't mean data will be exposed instantly — but anything stolen and stored today could be decoded later once such a machine exists.
    - This threat is called "harvest now, decrypt later."

How Are Governments Preparing

- Countries are already working on protections.
- The U.S. National Institute of Standards and Technology (NIST) has approved new post-quantum cryptography (PQC) methods designed to stay secure even against quantum computers:
    - CRYSTALS-Kyber → for encryption
    - Dilithium → for digital signatures
- These rely on tough mathematical problems that quantum computers are not expected to crack.
- Experts believe breaking **RSA-2048** — a widely used encryption standard — will require millions of stable (logical) qubits.
    - RSA encryption works by multiplying two huge prime numbers.
    - Multiplying them is easy. But figuring out the original primes from the final product is extremely hard — so hard that even supercomputers would need billions of years.
- At current progress, this may take 5 to 8 years, so Q-day is still a future risk, not an immediate one.

How Quantum Computers Work

- Quantum computers use special units called qubits. Unlike normal bits (0 or 1), qubits can be 0 and 1 at the same time (superposition).
- They can also be **entangled**, meaning a change in one instantly affects another, even far away.
- Because of this, quantum computers can test many possibilities at once, making them powerful for certain tasks.

Why Quantum Computers Threaten RSA Encryption

- RSA encryption is built on the difficulty of breaking a number into its prime factors — something classical computers take billions of years to do.
- But quantum computers can use **Shor's algorithm**, which turns the factoring challenge into a search for hidden repeating patterns.
- The algorithm uses a special mathematical tool called the **Quantum Fourier Transform** (QFT) to detect these patterns.
- If a quantum computer can run this algorithm on a large scale, it could break RSA encryption exponentially faster than classical computers.

The Problem: Today's Quantum Computers Are Too Small

- Breaking a strong key like RSA-2048 requires enormous quantum machines.
- A 2019 study by Google researchers estimated that breaking RSA-2048 needs:
    - About 20 million physical qubits
    - 8 hours of computation
    - Perfect error correction
- But today's biggest quantum machines (Google's Willow, IBM's Condor) only have a few hundred noisy qubits.

Why We Need Millions of 'Logical Qubits'

- Physical qubits make many errors.
- To perform long, accurate calculations, we need logical qubits — stable units created by combining many physical qubits through error correction.
- A future, powerful quantum computer would need millions of these logical qubits.
- Right now, we aren't even close to that technology.

Shor's Algorithm vs. Quantum Echoes: Why They Are Not the Same

- Shor's algorithm is a **mathematical tool** that could one day break modern encryption by rapidly factoring large numbers — something classical computers struggle to do. Its goal is computational power.
- Quantum Echoes, on the other hand, is a **physics experiment**. It studies how quantum information spreads and comes back like an "echo" inside entangled particles. Its purpose is scientific understanding, not breaking codes.

How Far Are We From Q-Day

- Google's Quantum Echoes experiment does **not** make that day arrive sooner.
- Instead, it marks progress in understanding how quantum systems behave, not in breaking codes.
- The experiment shows that quantum processors are getting better at studying complex interactions inside entangled particles. This is a **scientific milestone**, not a cybersecurity threat.
- While quantum machines are slowly advancing, their biggest potential right now is in understanding nature, chemistry, and materials — not cracking RSA.
- The real challenge is making sure our digital systems become quantum-safe before quantum computers eventually reach that power.
- The technology is evolving, but so must our defences.

Source: TH
