Google's Founder and Head of the Quantum AI Lab predicts Google will crack RSA and ECC encryption by 2029

A Collection of Peer-Reviewed Studies, Specialist Opinions, and Market Insights

Overview

Dr. Hartmut Neven, the founder and current Head of Google's Quantum Artificial Intelligence Laboratory and Vice President of Engineering, has consistently argued that quantum computers capable of breaking current RSA encryption standards will arrive sooner than conventional wisdom assumes.

His position rests on three mutually reinforcing pillars:

1. **Doubly exponential rate of quantum hardware improvement (Neven's Law**),
   a. So …4, 16, 256, 65,536, 4,294,967,296 - which is 4.3 billion, then it grows to 18,446,744,073,709,551,616, which is 18 quintillion, 446 quadrillion, 740 trillion…). The first part of that number is 18 Quintrillion, which is 18 MILLION **TRILLION** or $2^{\wedge 64}$ (2 to the power of 64), then add 446 quadrillion, which is 446,000 **TRILLION** more, a number so vast it defies human comprehension.
2. **Google's demonstrated breakthroughs in quantum error correction**,
3. **99.9% DECREASE of estimated computational resources needed to factor RSA-2048 and ECC keys. From 1 billion to 1 million qubits (and still dropping).**

   Both RSA and ECC are vulnerable to quantum attacks, but ECC is easier to break with Shor's algorithm because it needs fewer qubits, due to its reliance on the elliptic-curve discrete logarithm problem. Click to confirm that if you can crack RSA, ECC is simpler. Therefore, a quantum computer capable of breaking RSA-2048 can more easily solve the mathematical foundation of ECC. This shared weakness is why the consensus is to replace both RSA-2048 and ECC systems simultaneously with Post-Quantum Cryptography (PQC) standards.

3rd-Party verifiable sources: 18 credible, verifiable sources, and 16 peer-reviewed articles (Nature), Google Quantum AI preprints, Global Risk Institute surveys, and NIST/NSA guidance, appear in this document to support Dr. Hartmut Neven's position. We also created three videos and a technical podcast, which are on the last page of this article (page 9).

An Abundance of Evidence

The convergence of the 5 threads below substantiates the urgency in Dr. Neven's warning that Q-Day—the point at which quantum computers can break current encryption—is closer than the public believes. This concern is further supported by industry roadmaps from major players like Google, IBM, and Quantinuum, all of which anticipate achieving fault-tolerant quantum systems between the late 2020s and early 2030s, aligning perfectly with Neven's timeline.

1. **Hardware is advancing at a doubly exponential rate** (Neven's Law), meaning progress will feel slow until it suddenly isn't.
2. **The fundamental physics barrier of error correction has been cleared** (Willow, Nature 2024), converting the remaining challenge from discovery to engineering.
3. **Algorithmic improvements alone have cut the RSA-2048 attack cost by 95%** in six years (Gidney, 2019 vs. 2025), and there is no reason to assume this optimization has plateaued.
4. **Expert surveys show rising confidence** in an earlier Q-Day, with probabilities increasing year over year (Global Risk Institute, 2024).
5. **U.S. government agencies (NIST, NSA, CISA) are acting with urgency**; they issued post-quantum cryptography standards and accelerated migration timelines.

As Google's own Craig Gidney wrote in his 2025 paper: ***"I prefer security to not be contingent on progress being slow."***

TABLE OF CONTENTS

1. Dr. Neven's Law: Doubly Exponential Growth in Quantum Computing

Neven claims quantum computing power grows at a doubly exponential rate, unlike the single exponential growth of Moore's Law (e.g., 4, 16, 256, 65,536, 4,294,967,296 - which is 4.3 billion, then 18,446,744,073,709,551,616, which is 18 quintillion, 446 quadrillion, 740 trillion…), The first part of that number is 18 Quintrillion which is 18 MILLION **TRILLION** or 2^{64} (2 to the power 64) then add 446 quadrillion which is 446,000 TRILLION more. Truly a number so vast it defies human comprehension.

The extreme acceleration is due to a "doubly exponential" relative growth, which combines:

1. Quantum computers' inherent exponential advantage (n qubits can simultaneously represent 2^n states) with the
2. Exponential improvement in hardware (qubit counts and error rates).

Key Sources

Quanta Magazine / Scientific American (June 2019)

Original reporting on Neven's doubly exponential observation and the underlying two-factor mechanism.

https://www.quantamagazine.org/does-nevens-law-describe-quantum-computings-rise-20190618/

Wikipedia: Quantum Computing Scaling Laws

Contextualizes Neven's Law alongside Rose's Law and Schoelkopf's Law, noting it suggests quantum advantage may emerge much sooner than simpler models predict.

https://en.wikipedia.org/wiki/Rose%27s_law

The Conversation (2019)

Independent academic analysis of Neven's Law, noting that if it holds, it implies today's laptops and smartphones would have been achievable by 1975 under classical doubly exponential growth.

https://theconversation.com/nevens-law-why-it-might-be-too-soon-for-a-moores-law-for-quantum-computers-120706

Notable Endorsement

Scott Aaronson, a leading computer scientist at the University of Texas at Austin, commented on the trend: *"I think the undeniable reality of this progress puts the ball firmly in the court of those who believe scalable quantum computing can't work. They're the ones who need to articulate where and why the progress will stop."*

2. The Error Correction Breakthrough: Google's Willow Chip (2024)

The single most important prerequisite for a useful, large-scale quantum computer is the ability to correct errors faster than they accumulate. For nearly 30 years, since Peter Shor introduced quantum error correction in 1995, no quantum processor has definitively demonstrated "below-threshold" performance—the ability to drive logical error rates down by adding more qubits. In December 2024, Google's Willow chip changed that.

In a paper published in Nature, Google's team showed that as they scaled surface code arrays from 3×3 to 5×5 to 7×7 encoded qubits on their 105-qubit Willow processor, the logical error rate was cut in half with each increase. This exponential suppression of errors as the system grows is the fundamental proof that fault-tolerant quantum computing is achievable at scale.

As Neven stated at the Willow announcement briefing: *"The whole community breathes a sigh of relief because it shows that quantum error correction indeed can work in practice. Now you have the building block in hand, almost ready to scale up to the large machines."*

Key Sources

> **Nature (December 2024) — Peer-Reviewed**
>
> *Google Quantum AI and Collaborators, "Quantum error correction below the surface code threshold." The first demonstration of below-threshold error correction on a superconducting processor.* https://www.nature.com/articles/s41586-024-08449-y

> **American Physical Society — Physics Magazine (December 2024)**
>
> *Expert commentary from Lorenza Viola (Dartmouth) and John Preskill (Caltech) calls it a "notable milestone."* https://physics.aps.org/articles/v17/176

> **Google Research Blog (December 2024)**
>
> *Technical overview by the Google Quantum AI team describing the below-threshold and beyond-breakeven results.* https://research.google/blog/making-quantum-error-correction-work/

> **Nature (February 2023) — Earlier Milestone**
>
> *Google's initial proof that increasing surface code size decreases error rate: "Suppressing quantum errors by scaling a surface code logical qubit."*
> https://research.google/blog/suppressing-quantum-errors-by-scaling-a-surface-code-logical-qubit/

Why This Matters for RSA and ECC

Below-threshold error correction shifts the quantum-versus-RSA/ECC question from "if" to "when." Reliable error suppression during scaling turns building a larger machine into an engineering challenge of modular replication ("copy-paste"), as Neven argues.

3. Collapsing Resource Estimates: From 20 Million to Under 1 Million Qubits

Perhaps the strongest evidence that RSA's demise is approaching faster than expected comes from the dramatic and continuing reduction in the estimated resources needed to execute Shor's algorithm against RSA-2048. In May 2025, Google's own Craig Gidney published a preprint demonstrating a 20-fold reduction in the number of qubits required.

The Trajectory of Resource Estimates

- **2012:** Roughly 1 billion physical qubits estimated to factor RSA-2048.
- **2019 (Gidney & Ekerå):** ~20 million noisy qubits in 8 hours.
- **2025 (Gidney):** Under 1 million noisy qubits in under 1 week—a 95% reduction from the 2019 estimate.

This 99.9% decrease, which is a 1,000-fold reduction in a little over a decade, has been driven not by hardware alone but by algorithmic innovations: approximate residue arithmetic, yoked surface codes for denser qubit storage, and magic state cultivation for more efficient error-correction overhead.

Key Sources

> **arXiv Preprint (May 2025) — Google Quantum AI**
>
> *Gidney, C. "How to factor 2048 bit RSA integers with less than a million noisy qubits." arXiv:2505.15917.*
>
> https://arxiv.org/abs/2505.15917

> **Google Research Publications Page**
>
> *Official Google Quantum AI publication listing and summary of the Gidney 2025 paper.*
>
> https://research.google/pubs/how-to-factor-2048-bit-rsa-integers-with-less-than-a-million-noisy-qubits/

> **Gidney & Ekerå (2021, published in Quantum) — Prior Baseline**
>
> *The 2019/2021 estimate of 20 million noisy qubits and 8 hours—now superseded by the 2025 work.*
>
> https://quantum-journal.org/papers/q-2021-04-15-433/

> **CSO Online (May 2025)**
>
> *Industry analysis: Gartner VP Analyst warned that quantum computing will weaken asymmetric cryptography by 2029. Estimates have plummeted from 1 billion qubits (2012) to 1 million today.*
>
> https://www.csoonline.com/article/3995036/breaking-rsa-encryption-just-got-20x-easier-for-quantum-computers.html

The Implication

As noted by the Post Quantum analysis of Gidney's work: in just six years, a single researcher's own estimate dropped by 20×. Multiple commentators have observed that algorithmic efficiency is a moving target, and that future optimizations or alternative approaches could reduce estimates further in ways that are difficult to predict.

4. Expert Consensus: The Quantum Threat Timeline Is Accelerating

Neven's position is not a lone voice. It aligns with a growing body of expert surveys and government assessments that place the quantum threat to current encryption as more imminent than previously assumed.

Global Risk Institute — Quantum Threat Timeline Report (2024)

The sixth annual report, authored by Dr. Michele Mosca and Dr. Marco Piani, surveyed **32 global quantum experts**. Key findings include:

- **19–34% probability** of a Cryptographically Relevant Quantum Computer (CRQC) emerging within 10 years (up from 17–31% in 2023).
- **5–14% probability** within 5 years (up from 4–11% in 2023).
- Year-over-year, expert confidence in an earlier Q-Day is increasing, not stabilizing.

Global Risk Institute / evolutionQ (December 2024)

Quantum Threat Timeline Report 2024. Annual survey of global quantum computing and cryptography experts. https://globalriskinstitute.org/publication/quantum-threat-timeline/

U.S. Government and Standards Bodies

- **NIST IR 8547 (November 2024):** The National Institute of Standards and Technology recommends deprecating RSA and other vulnerable public-key algorithms after 2030, and disallowing them entirely after 2035.
- **NSA / CISA (August 2023):** A joint advisory from the National Security Agency and CISA recommended that organizations begin preparing for post-quantum cryptography immediately.
- **Biden Executive Order (2024):** Moved the government migration deadline from 2035 to "as soon as practicable."

Industry Analyst Warnings

- **Gartner (2025):** VP Analyst Bart Willemsen warned that quantum computing will weaken asymmetric cryptography by 2029, and urged organizations to begin strategic planning now.
- **Federal Reserve (2025):** FEDS 2025-093 frames the "harvest now, decrypt later" threat as "present, active, and in some circumstances unavoidable."

Resilience / Cybersecurity Analysis (October 2025)

Comprehensive timeline analysis of Q-Day estimates, using NIST, NSA, IBM, & Google roadmaps. https://cyberresilience.com/threatonomics/when-will-quantum-decryption-become-practical/

5. Google's 2029 Roadmap and Neven's "Engineering Scaling" Argument

Google Quantum AI's published roadmap targets six milestones on the path to a large, useful, error-corrected quantum computer. As of late 2024, Google reported that it had completed the first two milestones—quantum supremacy (2019) and scalable error correction (Willow, 2024)—and was on track for the remaining milestones by the end of the decade.

In October 2025, Google demonstrated a further software-track milestone: the Quantum Echoes algorithm running on Willow achieved a 13,000× speedup over the world's fastest supercomputer for a physics simulation, marking Google's first demonstration of quantum advantage for a scientifically meaningful problem.

Neven's central strategic argument is this: once the fundamental physics of fault tolerance has been proven (which Willow accomplished), scaling to the qubit counts required for RSA-2048 and ECC becomes an **engineering problem** of replicating proven modules, not a physics problem requiring new discoveries. At an interview for Google Zeitgeist, Neven stated the team's goal is to build a machine with about a million physical qubits—precisely the threshold Gidney's 2025 paper identifies as sufficient to break RSA-2048 and ECC.

Key Sources

Google Blog — Willow Announcement (December 2024)
Neven's official post describing Willow's milestones and Google's roadmap toward a useful quantum computer by the end of the decade.
https://blog.google/technology/research/google-willow-quantum-chip/

HPCwire — Google Roadmap Briefing (December 2024)
Detailed reporting from Google's media briefing with Neven, Kelly, Newman, and Chou, including roadmap milestones and timeline.
https://www.hpcwire.com/2024/12/09/google-debuts-new-quantum-chip-error-correction-breakthrough-and-roadmap-details/

The Quantum Insider — Google Zeitgeist Interview (November 2022)
Neven discusses the million-qubit goal, encryption implications, and the "end of the decade" timeline in conversation with Google SVP James Manyika.
https://thequantuminsider.com/2022/11/23/james-manyika-senior-vice-president-of-technology-society-at-google-interviews-hartmut-neven-vp-of-engineering-google-quantum-ai-lab/

The Quantum Insider — Quantum Echoes / 13,000× Speedup (October 2025)
Neven's remarks at the press conference on the 2029 real-world applications target and the dual hardware/software roadmap.
https://thequantuminsider.com/2025/10/22/google-quantum-ai-shows-13000x-speedup-over-worlds-fastest-supercomputer-in-physics-simulation/

Appendix: Complete Source List

Peer-Reviewed / Nature Publications

- Google Quantum AI, “Quantum error correction below the surface code threshold,” Nature (December 2024).
- Google Quantum AI, “Suppressing quantum errors by scaling a surface code logical qubit,” Nature (February 2023).

Preprints and Technical Papers

- Gidney, C. “How to factor 2048 bit RSA integers with less than a million noisy qubits.” arXiv:2505.15917 (May 2025).
- Gidney, C. & Ekerå, M. “How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits.” Quantum 5, 433 (2021).

Expert Surveys and Risk Assessments

- Mosca, M. & Piani, M. “Quantum Threat Timeline Report 2024.” Global Risk Institute / evolutionQ (December 2024).
- NIST IR 8547, “Transition to Post-Quantum Cryptography Standards” (Initial Public Draft, November 2024).
- NSA / CISA, “Post-Quantum Cryptography: Recommend How to Prepare Now” (August 2023).
- FEDS 2025-093, Federal Reserve analysis of “Harvest Now, Decrypt Later” risks (2025).

Journalism and Analysis

- Quanta Magazine / Scientific American, “Does Neven’s Law Describe Quantum Computing’s Rise?” (June 2019).
- CSO Online, “Breaking RSA encryption just got 20x easier for quantum computers” (May 2025).
- HPCwire, “Google Debuts New Quantum Chip, Error Correction Breakthrough, and Roadmap Details” (December 2024).
- American Physical Society, “Cracking the Challenge of Quantum Error Correction” (December 2024).

Google Official Sources

- Google Blog, “Meet Willow, our state-of-the-art quantum chip” (December 2024).
- Google Research Blog, “Making quantum error correction work” (December 2024).
- Google Research, Craig Gidney’s publications page.
- Google Research, Hartmut Neven’s profile and publications page.

Additional Resources

19 Min Podcast for CISOs and CTOs.

1. "Q-day," the breaking of current RSA encryption—likely by 2029.
2. Nevin's Law (doubly exponential power growth),
3. Proven error correction (Google's 2020 Willow chip),
4. Algorithmic collapse (Less than 1 million qubits needed to break ECC & RSA 2048)

5 min Video: Why your Security Architecture is Obsolete

1. **Current Flaw:** Existing security fails due to reliance on static, stored encryption keys, creating a critical single point of failure vulnerable to theft.
2. **The Threat:** Adversaries employ a "Harvest Now Decrypt Later" (HNDL) strategy, stockpiling intercepted data for future decryption using AI and quantum computing.
3. **Regulatory Pressure:** A myriad of regulations across 50 states and at the federal level create personal liability for C-suite executives, with criminal penalties and imprisonment.
4. **The Solution:** The necessary paradigm shift is toward self-protecting data in a PQC architecture that eliminates the stored key—the "keyhole"—making data unreadable even if extracted.

5 Min Video. A High-Level Roadmap

- IBM, Google, and SandBox Quantum experts project 2029 as the revised Q-Day, the "Decryption Horizon"—when current asymmetric cryptography fails due to quantum computing.
- The maximum Certificate lifespan for public SSL/TLS certificates is projected to drop sharply to just 47 days by 2029

2 Min video overviews this 9-page Article

- If you want someone to read our 9-page article but believe it's better to start with a 2-minute video summary, here it is.
- This video is also available on the PQC+ page of our website.