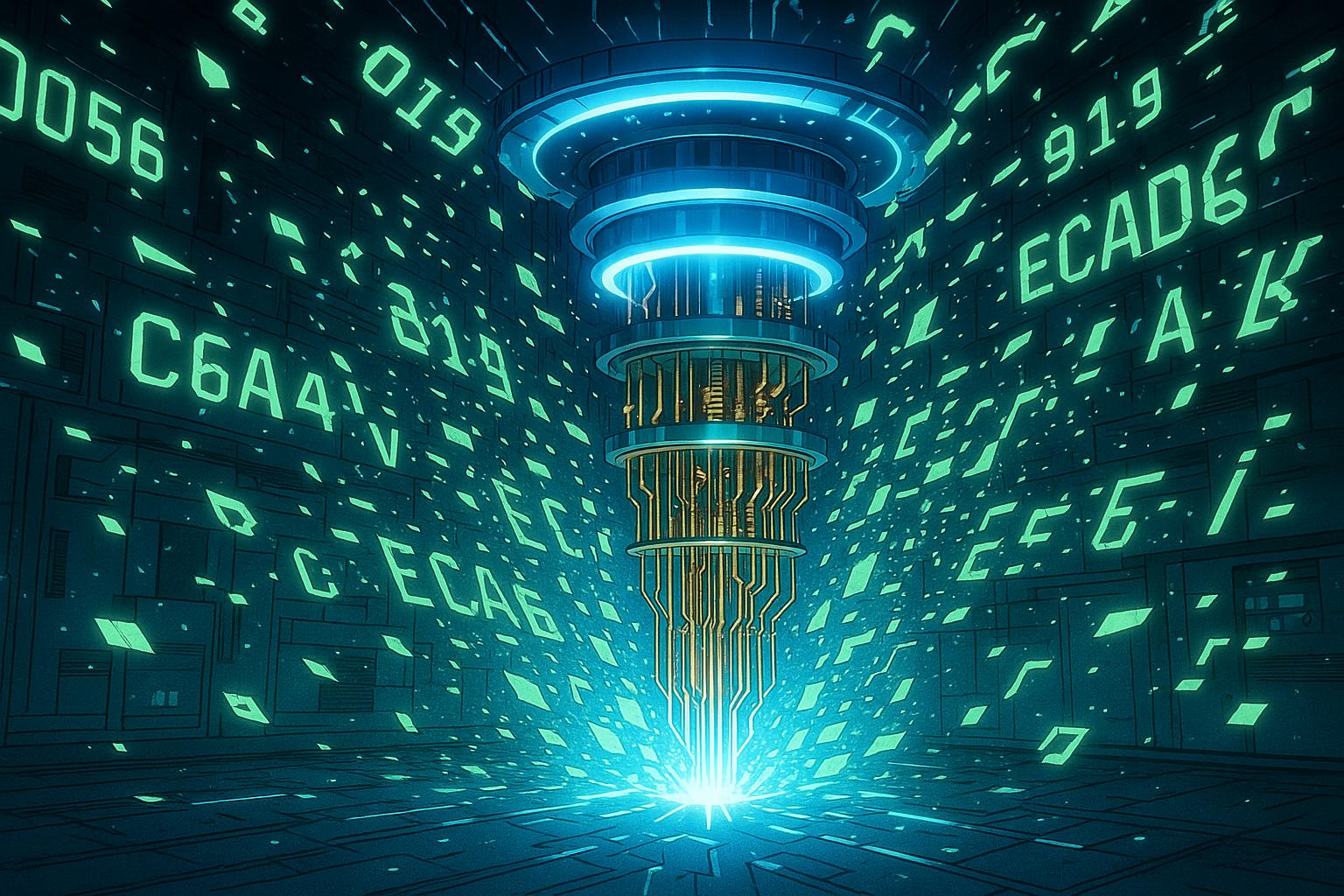
# Quantum breakthrough could crack 2048-bit RSA encryption in just one week



Recent advancements in quantum computing have sparked concern among cybersecurity professionals, particularly with warning signs that a single quantum computer equipped with just one million "noisy" qubits could dismantle the widely used 2048-bit RSA encryption in a mere week. This scenario, once imagined as a distant threat, is now underscored by the rapid evolution of technologies that significantly lower the barriers to executing such attacks.

Historically, the notion of quantum computing as a potential threat to security was tempered by estimates suggesting that 20 million qubits would be necessary to challenge entrenched encryption methods like RSA. However, breakthroughs from Google’s Quantum AI lab, particularly techniques such as yoked surface codes and optimised quantum arithmetic, have radically transformed this landscape. These advancements allow for efficient codebreaking even in the face of operational errors, heralding an age where previously secure digital environments become alarmingly vulnerable.

The implications are staggering. Core institutions rely on RSA encryption to safeguard sensitive online transactions, health records, and classified communications. With the rapid pace of quantum development, the urgency for organisations to transition to quantum-safe encryption is paramount. Experts advise that a concerted shift to post-quantum cryptography must occur within the next five years if we are to mitigate these risks effectively. Already, hackers are engaging in a "harvest now, decrypt later" strategy, archiving data currently protected by encryption, with an expectation that future quantum capabilities will allow them to unlock these treasures.

In response to this looming threat, the National Institute of Standards and Technology (NIST) has been at the forefront of establishing post-quantum cryptography standards. In August 2024, NIST finalised three algorithms designed to withstand potential quantum assaults, recommending that computer system administrators initiate transitions to these robust protocols without delay. These standards are intended to secure a breadth of digital information, from private emails to vital e-commerce transactions and beyond. Their introduction is not merely a precaution; it represents a critical leap towards ensuring that digital security keeps pace with evolving quantum technology.

Despite the considerable strides in quantum-safe methods, the broader implementation across various sectors remains uneven. Financial institutions and telecom companies are among the first to adopt these standards, as they peg their operations on the unyielding protection of sensitive data. In contrast, many other industries lag, creating a patchwork of readiness that leaves vast swathes of data perpetually at risk. The consensus in the field is clear: a coalition approach involving technology companies, academic researchers, and other industries is essential to create comprehensive, trustworthy encryption solutions that stand the test of quantum challenges.

As quantum computers continue to mature, experts predict the arrival of practical quantum machines in the next five to ten years. This timeline prompts an urgent call for organisations to not only reassess their encryption methods but also to embrace a culture of cryptographic agility. This could involve implementing hybrid systems that combine traditional algorithms with new post-quantum methods, ensuring a smoother transition as the landscape evolves. The goal is clear: safeguard digital assets now to avert potential catastrophic breaches in the near future.

Fostering awareness and preparedness regarding quantum threats is vital. Stakeholders must remain vigilant, informed, and proactive by following updates from entities like NIST or Google. By prioritising the implementation of post-quantum algorithms now, organisations can brace themselves against the ever-looming quantum wave, safeguarding the digital future against an impending apocalypse.

## Reference Map:

* Paragraph 1 – [[1]](https://macholevante.com/news-en/182270/the-quantum-leap-that-could-shatter-digital-security-as-we-know-it/), [[7]](https://arxiv.org/abs/2505.15917)
* Paragraph 2 – [[1]](https://macholevante.com/news-en/182270/the-quantum-leap-that-could-shatter-digital-security-as-we-know-it/), [[3]](https://www.ft.com/content/f602b685-8226-42b4-9336-e488c63c37bf), [[5]](https://www.nist.gov/cybersecurity/what-post-quantum-cryptography)
* Paragraph 3 – [[2]](https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards), [[3]](https://www.ft.com/content/f602b685-8226-42b4-9336-e488c63c37bf), [[4]](https://www.ft.com/content/f1d26918-67c5-4b11-b47b-4904606a002f)
* Paragraph 4 – [[2]](https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards), [[5]](https://www.nist.gov/cybersecurity/what-post-quantum-cryptography), [[6]](https://en.wikipedia.org/wiki/NIST_Post-Quantum_Cryptography_Standardization)
* Paragraph 5 – [[1]](https://macholevante.com/news-en/182270/the-quantum-leap-that-could-shatter-digital-security-as-we-know-it/), [[4]](https://www.ft.com/content/f1d26918-67c5-4b11-b47b-4904606a002f), [[6]](https://en.wikipedia.org/wiki/NIST_Post-Quantum_Cryptography_Standardization)
* Paragraph 6 – [[1]](https://macholevante.com/news-en/182270/the-quantum-leap-that-could-shatter-digital-security-as-we-know-it/), [[4]](https://www.ft.com/content/f1d26918-67c5-4b11-b47b-4904606a002f), [[2]](https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards)
* Paragraph 7 – [[1]](https://macholevante.com/news-en/182270/the-quantum-leap-that-could-shatter-digital-security-as-we-know-it/), [[2]](https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards), [[5]](https://www.nist.gov/cybersecurity/what-post-quantum-cryptography)
* Paragraph 8 – [[3]](https://www.ft.com/content/f602b685-8226-42b4-9336-e488c63c37bf), [[1]](https://macholevante.com/news-en/182270/the-quantum-leap-that-could-shatter-digital-security-as-we-know-it/), [[5]](https://www.nist.gov/cybersecurity/what-post-quantum-cryptography)

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://macholevante.com/news-en/182270/the-quantum-leap-that-could-shatter-digital-security-as-we-know-it/> - Please view link - unable to able to access data
2. <https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards> - In August 2024, the National Institute of Standards and Technology (NIST) finalized three encryption standards designed to withstand cyberattacks from quantum computers. These standards aim to secure a wide range of electronic information, from confidential emails to e-commerce transactions. NIST encourages computer system administrators to begin transitioning to these new standards promptly to ensure future-proof cybersecurity.
3. <https://www.ft.com/content/f602b685-8226-42b4-9336-e488c63c37bf> - In August 2024, the National Institute of Standards and Technology (NIST) was on the verge of publishing three new security algorithms aimed at protecting against potential threats from quantum computers. These threats arise because quantum computers, which leverage 'qubits' that can be in multiple states simultaneously, may ultimately crack traditional cryptographic codes. The new algorithms aim to safeguard crucial digital data like financial transactions and medical information from future quantum hacking. While industries such as finance and telecom are preparing for this transition, many other sectors have not yet taken necessary measures. The NIST standards are expected to catalyze broader action and cooperation, involving inputs from tech companies, banks, and researchers globally. Although quantum computers capable of breaking existing cryptographic methods do not yet exist, the risk is significant enough to warrant immediate preparations using techniques like post-quantum cryptography and quantum key distribution. The urgency is underscored by hackers' 'harvest now, decrypt later' strategy, making current data potentially vulnerable when quantum technology advances.
4. <https://www.ft.com/content/f1d26918-67c5-4b11-b47b-4904606a002f> - In December 2024, Google achieved a significant breakthrough in quantum computing by improving error correction techniques, a critical challenge in developing practical quantum computers. This advancement enhances the stability and reduces the error rates of qubits, bringing the realization of scalable quantum systems closer to reality. The findings, published in Nature, indicate that full-scale quantum systems could be achieved by the end of the decade, requiring approximately one million qubits. This progress has profound implications for various fields, including cybersecurity, where quantum computers could potentially break current cryptographic codes.
5. <https://www.nist.gov/cybersecurity/what-post-quantum-cryptography> - The National Institute of Standards and Technology (NIST) is leading a global effort to develop electronic defenses against potential cyberattacks from quantum computers through its Post-Quantum Cryptography (PQC) project. This initiative aims to create encryption methods that can withstand attacks from both conventional and quantum computers, ensuring the security of sensitive electronic information. NIST has already released the first three finalized PQC standards in 2024, marking a significant step toward securing digital assets in the quantum era.
6. <https://en.wikipedia.org/wiki/NIST_Post-Quantum_Cryptography_Standardization> - The NIST Post-Quantum Cryptography Standardization project is an ongoing initiative by the National Institute of Standards and Technology (NIST) to develop cryptographic algorithms resistant to attacks from quantum computers. The project involves multiple rounds of evaluation and standardization, with the third round concluding in 2020. The project aims to ensure that cryptographic systems remain secure in the face of advancing quantum computing technologies.
7. <https://arxiv.org/abs/2505.15917> - A recent study estimates that a quantum computer with less than a million noisy qubits could factor 2048-bit RSA integers in under a week. This significant reduction in required qubits is attributed to advancements in error-correcting algorithms, such as yoked surface codes, and optimized quantum arithmetic. These developments highlight the accelerating threat quantum computers pose to current encryption methods, emphasizing the need for quantum-resistant cryptographic solutions.