Crypto News

Compiled by Dhananjoy Dey, Indian Institute of Information Technology, Lucknow, U. P. - 226 002, India, ddey@iiitl.ac.in

September 01, 2025

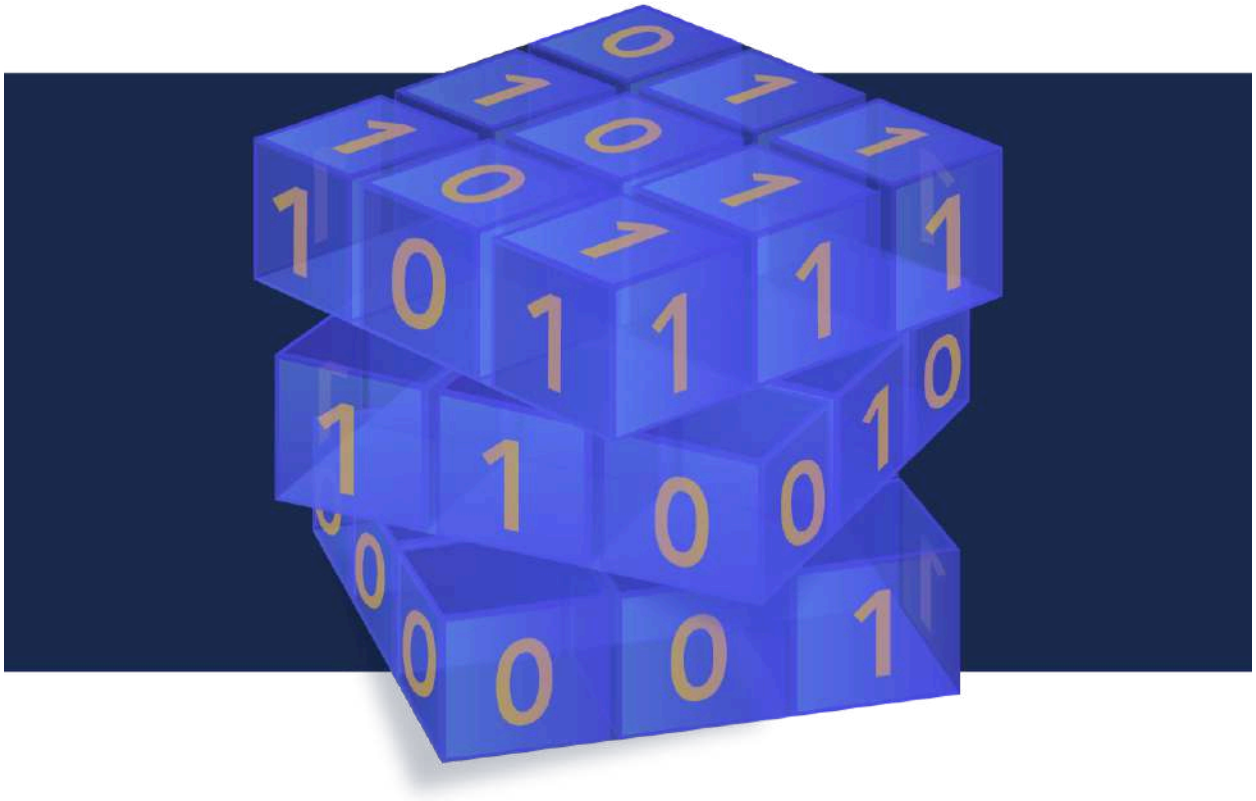


Table of Contents

Editorial

Dear Quantum-Safe enthousiasts,

I hope that you had a great summer. We thought that quantum might slow down a bit during this time, but as you can see from the number of articles over these two months (53 of them!), we were wrong.

So, what can we make of this selection?

First, let's start with some good news: as described in 51, China has not really broken RSA (yet!). As often, there was more hype than substance. However, due to progress in quantum computing , complacency is totally forbidden. 11 is again a bit too much hype, but progress is there as presented in 17 and 22 and some interesting discussion on the quantum advantage in 9 and 34.

Fortunately, it seems that people are starting to understand that there is a need for beginning the quantum-safe journey. Many articles discuss the need for post-quantum cryptography (PQC), both in the standard IT world and for IoT devices. I counted about twenty articles mentioning PQC: you have a large choice to select from. With a focus on variety, I would recommend: 8, which describes the view of Microsoft; 13, from NIST on IoT; 27 for its description of crypto-agility, 44 for the explanation of cryptographic inventory; and, of course, something on the role of the Cloud in 49.

Note that there is also a contrariant view from Prof Gutmann in 36, who believes that the quantum computer will present no threat for many years to come and that PQC is a distraction. Personally, I think that this article underestimates the scale of the threat. Even if there is no certainty that the QC will break RSA soon, the risk associated with this threat (total breakdown of our cybersecurity infrastructure) is so large, that the move to quantum-safe solutions is a must today.

I wish you all an easy return to work (assuming you could take some time off...).

Have a good read!

Bruno

The Crypto News editorial is authored by the Chair of the Quantum-Safe Security Working Group (QSS WG) of the Cloud Security Alliance (CSA), Bruno Huttner, Director of Strategic Quantum Initiatives at ID Quantique SA and it is compiled by Dhananjoy Dey.

Disclaimer. The QSS WG does not express an opinion on the validity of the ideas and the claims presented in the articles in this newsletter.

1. Scientists Crack a 40-Year Puzzle in Unbreakable Encryption

by The Hebrew University Of Jerusalem
https://scitechdaily.com/scientists-crack-a-40-year-puzzle-in-unbreakable-encryption/

For decades, scientists thought unbreakable quantum encryption required flawless light sources, a nearly impossible feat. But a team has flipped the script using tiny engineered "quantum dots" and clever new protocols.

By making imperfect light behave more securely, they proved that encrypted messages can travel farther and more safely than ever before. Real-world tests have shown that their method outperforms even the best current systems, bringing practical, affordable quantum-safe communication a significant step closer.

Breakthrough in Quantum Encryption

A team of physicists has made a breakthrough that could bring secure quantum communication closer to everyday use – without needing flawless hardware.

The research, led by PhD students Yuval Bloom and Yoad Ordan, under the guidance of Professor Ronen Rapaport from the Racah Institute of Physics at Hebrew University in collaboration with researchers from Los-Alamos National Labs, and published in *PRX Quantum*, introduces a new practical approach that significantly improves how we send quantum encrypted information using light particles – even when using imperfect equipment.

Cracking a 40-Year-Old Challenge

For four decades, the holy grail of quantum key distribution (QKD) – the science of creating unbreakable encryption using quantum mechanics – has hinged on one elusive requirement: perfectly engineered single-photon sources. These are tiny light sources that can emit one particle of light (photon) at a time. But in practice, building such devices with absolute precision has proven extremely difficult and expensive.

To work around that, the field has relied heavily on lasers, which are easier to produce but not ideal. These lasers send faint pulses of light that contain a small, but unpredictable, number of photons – a compromise that limits both security and the distance over which data can be safely transmitted, as a smart eavesdropper can "steal" the information bits that are encoded simultaneously on more than one photon.

A Better Way with Imperfect Tools

Bloom, Ordan, and their team flipped the script. Instead of waiting for perfect photon sources, they developed two new protocols that *work with what we have now* – sub-Poissonian photon sources based on quantum dots, which are tiny semiconductor particles that behave like artificial atoms.

By dynamically engineering the optical behavior of these quantum dots and pairing them with nanoantennas, the team was able to tweak how the photons are emitted. This fine-tuning allowed them to suggest and demonstrate two advanced encryption strategies:

- **A truncated decoy state protocol:** A new version of a widely used quantum encryption approach, tailored for imperfect single photon sources, that weeds out potential hacking attempts due to multi-photon events.
- **A heralded purification protocol:** A new method that dramatically improves signal security by "filtering" the excess photons in real time, ensuring that only true single photon bits are recorded.

In simulations and lab experiments, these techniques outperformed even the best versions of traditional laser-based QKD methods — extending the distance over which a secure key can be exchanged by more than 3 decibels, a substantial leap in the field.

Real-World Test of Quantum Networks

To prove it wasn't just theory, the team built a real-world quantum communication setup using a room-temperature quantum dot source. They ran their new reinforced version of the well-known BB84 encryption protocol — the backbone of many quantum key distribution systems — and showed that their approach was not only feasible but superior to existing technologies.

What's more, their approach is compatible with a wide range of quantum light sources, potentially lowering the cost and technical barriers to deploying quantum-secure communication on a large scale.

Toward Affordable Quantum-Secure Communication

"This is a significant step toward practical, accessible quantum encryption," said Professor Rapaport. "It shows that we don't need perfect hardware to get exceptional performance — we just need to be smarter about how we use what we have."

Co-Lead author Yuval Bloom added, "We hope this work helps open the door to real-world quantum networks that are both secure and affordable. The cool thing is that we don't have to wait; it can be implemented with what we already have in many labs worldwide."

2. Post-quantum cryptography (PQC) knocks on MCU doors

by Majeed Ahmad
https://www.edn.com/post-quantum-cryptography-pqc-knocks-on-mcu-doors/

An MCU facilitating real-time control in motor control and power conversion applications incorporates post-quantum cryptography (PQC) requirements for firmware protection outlined in the Commercial National Security Algorithm (CNSA) Suite 2.0. These MCUs also support Platform Security Architecture (PSA) Level 3 compliance.

PSA Certified Level 3 is an Internet of Things (IoT) security standard that focuses on robust protection against software and hardware attacks on a chip's root of trust. It provides an independently evaluated and validated environment that can securely house and execute the PQC algorithms.

"By adopting both PSA Certified Level 3 and PQC compliance with other regulations, companies can proactively address current and future cyber threats," said Erik Wood, senior director of cryptography and product security at Infineon Technologies. He is responsible for defining the security requirements of Infineon MCUs.

Quantum computers, exponentially faster than classical computers, are still under development. However, cybercriminals can collect encrypted data now and decrypt it later using quantum computers. That calls for future-proofing of current systems to ensure that companies remain secure as quantum computing technologies advance.

Enter PQC, a collection of cryptographic algorithms designed to be secure against attacks from powerful quantum computers. In MCUs, which mainly use cryptography during boot-time and run-time operations, it commands significant changes in security architecture amid evolving regulations.

For instance, MCU's memory size is a key design consideration. "More memory size is required because encryption keys are longer," Wood said. "The certificate size is different because the signatures of these certificates are much bigger."

Next comes the throughput shortfall. "While certificates are currently transferred through an I2C bus, the throughput falls short with QPC use," he added. "Now you need to have three I3C buses." Wood said that the industry is even procrastinating about whether every MCU will have a USB port in four years.

In other words, integrating QPC into MCUs will entail a primary upgrade of cryptographic algorithms. Next come memory upgrades, and finally, interface upgrades will follow.

Wood claimed that Infineon is the first MCU supplier to have integrated and ported PQC algorithms. "We offer an integrated library already hooked up to the accelerators for peak optimization and performance in a PSA-3 level device."

3. How AI malware works and how to defend against it

by Matthew Smith
https://www.techtarget.com/searchsecurity/tip/How-AI-malware-works-and-how-to-defend-against-it

Malicious actors continuously tweak their tools, techniques and tactics to bypass cyberdefenses and perform successful cyberattacks. Today, the focus is on AI, with threat actors finding ways to integrate this powerful technology into their toolkits.

AI malware is quickly changing the game for attackers. Let's examine the current state of AI malware, some real-world examples and how organizations can defend against it.

What is AI malware?

AI malware is malicious software that has been enhanced with AI and machine learning capabilities to improve its effectiveness and evasiveness.

Unlike traditional malware, AI malware can autonomously adapt, learn and modify its techniques. Namely, AI enables malware to do the following:

- Adapt to avoid detection by security tools.
- Automate operations, speeding the process for attackers.
- Personalize attacks against target victims, as in phishing attacks.
- Identify vulnerabilities to exploit.
- Mimic real people or legitimate software, as in deepfake attacks.

Using AI malware against a victim is a type of AI-powered attack, also known as an AI-enabled attack.

Types and examples of AI malware

The main types of AI malware include polymorphic malware, AI-generated malware, AI worms, AI-enabled social engineering and deepfakes.

Polymorphic malware

Polymorphic malware is software that continuously alters its structure to avoid signature-based detection systems. Polymorphic AI malware uses generative AI to create, modify and obfuscate its code and, thus, evade detection.

BlackMamba, for example, is a proof-of-concept malware that changes its code to bypass detection technology, such as endpoint detection and response. Researchers at HYAS Labs demonstrated how BlackMamba connected to OpenAI's API to create a polymorphic keylogger that collects usernames, passwords and other sensitive information.

AI-generated malware

Many malicious actors use AI components in their attacks. In September 2024, HP identified an email campaign in which a standard malware payload was delivered using an AI-generated dropper. This marked a significant step toward the deployment of AI-generated malware in real-world attacks and reflects how evasive and innovative AI-generated attacks have become.

In another example, researchers at security vendor Tenable demonstrated how the open source AI model DeepSeek R1 could generate rudimentary malware, such as keyloggers and ransomware. Although the AI-generated code required manual debugging, it underscores how bad actors can use AI to fuel malware development.

Similarly, a researcher from Cato Networks bypassed ChatGPT's security measures by engaging it in a role-playing scenario and leading it to generate malware capable of breaching Google Chrome's Password Manager. This prompt engineering attack showcases how attackers prompt AI into writing malware.

AI worms

AI worms are computer worms that use AI to exploit large language models (LLMs) to propagate and spread the worm to other systems.

Researchers demonstrated a proof-of-concept AI worm dubbed Morris II, referencing the first computer worm that infected about 10% of internet-connected devices in the U.S. in 1988. Morris II exploits retrieval-augmented generation (RAG), a technique that enhances LLM outputs by retrieving external data to improve responses, to propagate autonomously to other systems.

AI-enabled social engineering

Attackers are using AI to improve the effectiveness and success of their social engineering and phishing campaigns. For example, AI can help attackers do the following:

- Create more effective and professional email phishing scams with fewer grammatical errors.
- Gather information from websites to make campaigns more timely.
- Conduct spear phishing, whaling and business email compromise attacks more quickly than human operators.
- Impersonate voices to create vishing scams.

Deepfakes

Attackers use deepfake technology -- AI-generated videos, photos and audio recordings -- for fraud, misinformation, and social engineering and phishing attacks.

In a high-profile example, the British engineering group Arup was scammed out of $25 million in February 2025 after attackers used deepfake voices and images to impersonate the company's CFO and dupe an employee into transferring money to the attackers' bank accounts.

How to defend against AI malware

Given the ease with which AI malware adapts to evade defenses, signature-based detection methods are less effective against it. Consider the following defenses:

- **Behavioral analytics.** Deploy behavioral analytics software that monitors and flags unusual activity and patterns in code execution and network traffic. Integrate more in-depth analysis techniques as AI malware evolves.
- **Use AI against AI.** Adopt AI-enhanced cybersecurity tools capable of real-time threat detection and response. These systems adapt to shifting attack vectors more efficiently than traditional methods, effectively fighting fire with fire.
- **Learn how to spot a deepfake.** Know common characteristics of deepfakes. For example, facial and body movement, lip-sync detection, inconsistent eye blinking, irregular reflections or shadowing, pupil dilation and artificial audio noise.
- **Use deepfake detection technology.** The following technologies can help detect deepfakes:

- Spectral artifact analysis detects suspicious artifacts and patterns, such as unnatural gestures and sounds.
- Liveness detection algorithms base authenticity on a subject's movements and background.
- Behavioral analysis detects inconsistencies in user behavior, such as how a subject moves a mouse, types or navigates applications.
- Behavioral analysis ensures the video or audio shows normal user behavior.
- Path protection detects when camera or microphone device drivers change, potentially indicating deepfake injection.

- **Adhere to cybersecurity hygiene best practices.** For example, require MFA, use the zero-trust security model and hold regular security awareness training.
- **Follow phishing prevention best practices.** Get back to basics and teach employees how to spot and respond to phishing scams, AI-enabled or otherwise.
- **Use the NIST CSF and AI RMF.** Combining recommendations in the NIST Cybersecurity Framework and NIST AI Risk Management Framework can help organizations identify, assess and manage AI-related risks.
- **Stay informed.** Keep up to date with how attackers use AI in malware and how to defend against the newest AI-enabled attacks.

4. Researchers assess Post-Quantum Cryptography support in nine libraries by early 2025

by Quantum News
https://quantumzeitgeist.com/researchers-assess-post-quantum-cryptography-support-in-nine-libraries-by-early-2025/#google_vignette

The looming threat of quantum computers necessitates a shift towards new cryptographic methods, and a recent study assesses how well existing software tools are prepared for this change. Nadeem Ahmed, Lei Zhang, and Aryya Gangopadhyay, all from the University of Maryland Baltimore County, investigated the support for post-quantum cryptography (PQC) within nine popular open-source cryptographic libraries, including OpenSSL and Bouncy Castle. Their analysis reveals a mixed landscape of preparedness, with some libraries actively integrating PQC algorithms like CRYSTALS-Kyber and CRYSTALS-Dilithium, while others still lack substantial support. This research is significant because it identifies critical gaps in current cryptographic infrastructure, highlighting the urgent need for coordinated efforts to ensure a secure transition to a quantum-resistant future and mitigate potential security risks as quantum computing technology advances.

The study details key findings and takeaways regarding the preparedness of these libraries for a post-quantum future. The paper emphasizes the urgent need to transition to PQC due to the potential of quantum computers to compromise widely used public-key cryptosystems. Governments and major technology companies are actively preparing for this transition, while standards bodies like NIST are finalizing PQC algorithms.

The research assesses PQC support in several key libraries, revealing a varied landscape of progress. wolfSSL/wolfCrypt emerges as a leading library with strong and early PQC support, including implementations of NIST-selected algorithms such as Kyber, Dilithium, Falcon, and SPHINCS+. OpenSSL,

historically slower to adopt PQC, is now incorporating these algorithms, though integration remains ongoing. Bouncy Castle offers PQC implementations, particularly for Java and C#, and is actively updating to support the latest standards. Botan provides PQC support and is a versatile library used in various applications.

LibreSSL and mbed TLS also demonstrate increasing PQC support, though at a slower pace compared to wolfSSL. Integrating PQC algorithms into existing libraries presents challenges related to performance, code size, and compatibility with existing protocols. PQC algorithms generally exhibit different performance characteristics than classical algorithms, often requiring larger key sizes and more computational resources. NIST's standardization process is crucial, and the selected algorithms, Kyber, Dilithium, Falcon, and SPHINCS+, are central to the transition. Combining classical and PQC algorithms in hybrid approaches is a common strategy to provide both security and compatibility during this period, particularly within the widely used TLS protocol.

PQC is particularly important for securing Internet of Things (IoT) devices, which often have limited resources and long lifecycles. Protecting critical infrastructure from quantum attacks is a high priority, and data requiring long-term confidentiality is vulnerable to future quantum attacks and requires PQC protection. Future work should focus on optimizing PQC algorithms, finalizing and widely adopting standards, leveraging hardware acceleration, and deploying PQC in real-world applications. This paper provides a valuable snapshot of the current state of PQC implementation, highlighting progress, challenges, and the importance of preparing for the quantum era.

NIST PQC Standards		
Structured Lattices	KEM	ML-KEM (CRYSTALS-Kyber) NIST FIPS 203
	DSA	ML-DSA (CRYSTALS-Dilithium) NIST FIPS 204
Stateless Hash Based	DSA	SLH-DSA (SPHINCS+) NIST FIPS 205
		FN-DSA (FALCON) NIST FIPS 206 (Draft)
Stateful Hash Based	DSA	LMS (Leighton-Micali Signature) NIST SP 800-208
		XMSS (eXtended Merkle Signature Scheme) NIST SP 800-208

Post-Quantum Crypto Library Implementation Survey

Researchers undertook a comprehensive survey of nine widely used open-source cryptographic libraries to assess their preparedness for post-quantum cryptography (PQC). The study focused specifically on implementation support for the algorithms selected by the National Institute of Standards and Technology (NIST) following its multi-year standardization process, initiated to address vulnerabilities posed by advancing quantum computing. The core of the research involved identifying the extent to which each library supported the four NIST-selected PQC algorithms: CRYSTALS-Kyber, a key encapsulation mechanism; CRYSTALS-Dilithium, a lattice-based digital signature scheme; FALCON, another lattice-based signature algorithm optimized for smaller signature sizes; and SPHINCS+, a stateless hash-based signature scheme offering a different security foundation. Researchers also noted support for

older stateful hash-based signatures like Leighton-Micali and XMSS, to provide a broader picture of PQC implementation.

This detailed examination allowed scientists to map the current landscape of PQC support within these critical cryptographic tools. To ensure a rigorous and comparable assessment, the team established clear criteria for defining a "supported" algorithm, focusing on practical implementation within the libraries rather than theoretical compatibility. By maintaining a high-level conceptual focus, the team aimed to provide actionable insights for decision-makers and developers navigating the evolving cryptographic landscape. The research methodology mirrored the rigor of the NIST standardization process itself, acknowledging the importance of both security and performance. Scientists considered factors such as key and ciphertext sizes, computational efficiency on diverse platforms, and potential patent implications when evaluating each library's implementation. This holistic approach allowed for a nuanced understanding of the trade-offs involved in adopting PQC algorithms and informed a comprehensive assessment of the current state of PQC readiness within the open-source cryptographic community.

Post-Quantum Crypto Support in Open-Source Libraries

This research comprehensively evaluates the support for post-quantum cryptographic (PQC) algorithms within nine widely used open-source cryptographic libraries. The analysis reveals a varied landscape of preparedness, with some libraries actively integrating PQC algorithms and others lagging behind, despite the growing threat to current cryptographic systems posed by advances in computing. Researchers examined support for CRYSTALS-Kyber, a key encapsulation mechanism, and three digital signature schemes, recognizing the importance of both encryption and authentication in a post-quantum world. The study also considered support for older, stateful hash-based signature schemes like the Leighton-Micali Signature and the eXtended Merkle Signature Scheme, acknowledging their role as potential interim solutions. By surveying these widely adopted libraries, the research provides a clear picture of the current state of PQC implementation and highlights the challenges and opportunities for ensuring a secure transition to quantum-resistant cryptography. The findings underscore the urgent need for continued research, standardization efforts, and coordinated adoption strategies to protect sensitive data in the face of evolving quantum threats.

5. Protecting mission data in the AI era

by Kelvin Quezada
https://breakingdefense.com/2025/08/protecting-mission-data-in-the-ai-era/

Federal agencies and defense programs are rapidly embracing artificial intelligence (AI) to accelerate decision-making, enhance situational awareness, and improve operational efficiency. As AI workloads become more embedded in devices deployed to the tactical edge, whether on unmanned vehicles, mobile command systems, or field-deployed laptops, the data residing on these devices is becoming both increasingly valuable and vulnerable.

This shift to edge computing is driven in large part by security concerns. Sending sensitive mission data back to centralized cloud systems or data centers can introduce unacceptable risks. Instead, agencies are pushing computing closer to the mission, where data processing can occur locally, without risking exposure

through network transmissions. While this approach mitigates one set of threats, it introduces another: securing mission-critical data at rest, wherever it resides.

AI at the Edge: New Capabilities, New Risks

AI-driven capabilities at the edge have revolutionized operations. Real-time analytics, automated decision making, and enhanced sensor processing have significantly increased mission effectiveness. However, these same advancements have heightened the risk associated with losing physical control of devices, unauthorized access, or insider threats. Attackers, aided by AI tools themselves, are becoming more adept at quickly exploiting vulnerabilities and compromising sensitive data.

Moreover, these threats are not limited to traditional edge scenarios. Even devices within secure facilities, including laptops, servers, and workstations, remain vulnerable. A misplaced device, compromised insider, or targeted intrusion can expose sensitive information, underscoring that comprehensive Data at Rest (DAR) protection is critical for all endpoints, not just those deployed remotely.

Data at Rest Security: NSA's CSfC Mandate

Recognizing these challenges, the National Security Agency (NSA) has established the Commercial Solutions for Classified (CSfC) program. This program defines standards and guidelines for securing classified data through commercial, off-the-shelf solutions. Specifically, CSfC for DAR requires agencies to implement two independent, certified encryption layers to secure sensitive information stored on devices that are powered down or in an unauthenticated state.

The dual-layer model typically includes an outer encryption layer provided by hardware-based encryption solutions combined with Pre-Boot Authentication (PBA), alongside an inner layer consisting of approved Software Full Drive Encryption (SW FDE) protected by authentication. This layered approach significantly reduces the likelihood of compromise, even if one layer is breached.

Why Traditional Encryption Isn't Enough

Standard operating system (OS) encryption or standalone software encryption solutions often fall short against sophisticated adversaries. Attackers increasingly leverage advanced techniques such as brute force attacks, firmware manipulation, hardware-level exploits, and side-channel attacks to bypass conventional protections. Many of these techniques specifically target the weakest link, often credentials or encryption keys stored within the operating system environment itself.

Implementing Pre-Boot Authentication (PBA) alongside a Self-Encrypting Drive (SED) provides critical protection by securing devices before the operating system even loads. Because PBA operates independently of the OS, it cannot be bypassed by software vulnerabilities, zero-day exploits, or operating-system-level CVEs. While PBA solutions offer a critical layer of defense, it's essential to recognize that not all PBAs provide equal protection. Only those rigorously tested and validated by independent Common Criteria Testing Laboratories (CCTLs) against NIAP-defined security standards can truly assure agencies that encryption methods and key management practices meet the stringent demands of federal cybersecurity.

Additionally, deploying Software Full Drive Encryption (SWFDE) as a separate inner encryption layer interrupts the OS boot process, requiring independent authentication. Together, these two independent layers significantly reduce the available attack surface compared to traditional OS-level encryption alone.

For sensitive government operations, relying solely on OS-level encryption approaches is insufficient. Federal programs must adopt robust, comprehensive solutions that offer multiple, independent layers of security and built-in defenses against advanced threats.

Cigent's Mission-Ready Data Protection

Cigent offers federal agencies a full-stack, CSfC-aligned data protection solution that ensures sensitive mission data remains secure throughout its lifecycle. Rather than relying on OS-based encryption alone, Cigent's approach leverages hardware-embedded security measures and dedicated software solutions that provide superior resilience against advanced threats. Cigent's hardware and software solutions are NIAP-listed, NSA-approved, or currently undergoing rigorous validation in accredited testing labs.

Key Capabilities of Cigent Secure Storage:

- **Hardware Full Drive Encryption (Outer Layer):** Provides robust AES-256 encryption, securely managed independently of the operating system.
- **Pre-Boot Authentication (Outer Layer):** Ensures that encrypted drives remain inaccessible until valid credentials are provided, preventing unauthorized access from compromised OS environments.
- **Software Full Drive Encryption (Inner Layer)**: Delivers a secondary encryption layer requiring separate authentication, significantly increasing protection even if the hardware layer is compromised.
- **Enterprise Administration**: Supports efficient deployment, configuration, and management across fleets of devices through existing federal enterprise management tools.
- **Tamper-Resistant Security Controls:** Protects data from cloning, unauthorized extraction, and wiping attempts, even if adversaries have physical access.
- **Verified Sanitization:** Ensures that data can be securely wiped, complying with end-of-life or emergency destruction requirements.

Trusted Across Federal Agencies

Cigent's security solutions are widely deployed and trusted across numerous federal and defense programs, including within the Department of Defense (DoD), intelligence community (IC), and federal civilian agencies. Built for real-world operations, Cigent technology ensures that federal programs can maintain compliance and protect sensitive data, no matter where the mission takes them.

Mission-Ready: Today and Tomorrow

The continued growth of AI-driven operational capabilities and the inherent sensitivity of mission data demand a new standard for DAR protection. Federal agencies must adopt integrated solutions capable of delivering security, compliance, and operational flexibility at scale. With Cigent, agencies gain the assurance that mission data is protected at every stage, on every device, and in every environment.

6. Encryption, Backdoors, and the Economics of Weakness

by Nic Adams
https://ceoworld.biz/2025/08/21/encryption-backdoors-and-the-economics-of-weakness-by-nic-adams-co-founder-ceo-0rcus/

The UK's retreat from mandating an encryption backdoor in Apple's cloud data exemplifies a monumental policy reversal. This decision demonstrates an intricate interplay between national security, economic stability, and technological integrity. Governments, investors, and adversaries worldwide were all watching, understanding that had London proceeded, such an action would have set a dangerous precedent. Once established, the principle of forced compromise would have spread across borders, legal jurisdictions, and markets, fundamentally weakening digital trust. Policymakers worldwide must understand that the mathematics of cryptographic integrity cannot be circumvented by political will. This policy debate exemplifies a new, high-stakes competition among nations to position themselves as trustworthy digital havens.

The Financialization of Cryptographic Risk

In the contemporary financial environment, digital trust is a hard asset class, priced and valued by sophisticated markets. An attempt to compel a systemic weakness would have introduced a persistent, unhedgeable risk factor into an economy. Institutional investors, accustomed to quantifying political and regulatory risks, would have viewed this as a deliberate, self-inflicted wound. Any mandated backdoor would be a permanent liability on the national balance sheet, a recurring deduction against every enterprise valuation and a negative externality that would penalize businesses far beyond the tech sector. This is not a direct economic reality. Companies with greater cybersecurity exposure consistently underperform their peers in the stock market. The UK's reversal is a tacit acknowledgment of this market dynamic, demonstrating that a nation's appeal as a destination for capital and innovation is directly proportional to the strength of its data protection laws. Had the UK proceeded, the nation would have effectively de-rated its entire digital economy, triggering a predictable flight of capital to more secure jurisdictions. The pricing of this cryptographic risk would have been reflected in higher capital costs, reduced foreign direct investment, and a compression of valuation multiples for all tech-enabled enterprises operating under its jurisdiction.

The Nature of Encryption

Encryption is the foundational infrastructure of the digital age. Without this technology, the systems that underpin global commerce, from payment rails and supply chains to healthcare records and defense platforms would fail entirely. The notion of a "backdoor" is a dangerous misnomer; a controlled, law enforcement-only access point is not a reality. Instead, this would be a permanent and attractive attack surface for state-sponsored adversaries, cybercriminals, and corporate espionage units. The paradox is acute since any tool framed as a national security measure instantly becomes a new vector for attack, exposing citizens and fundamental systems to a higher degree of risk. Such a policy stands as the equivalent of a nation deliberately introducing default risk into its own financial system. This conscious decision embraces systemic fragility. The 2008 financial crisis provides a historical analogue; just as subprime

mortgages were a latent flaw capable of triggering a market-wide collapse, a compromised cryptographic system is a digital counterpart, a single point of failure with the potential to detonate trust across the entire ecosystem. The technical reality of a backdoor is that it cannot be limited to a specific user or context.

Asymmetry of Offense and Defense

The geometric asymmetry between digital offense and defense makes the concept of a "contained" backdoor a mathematical impossibility. Attackers need to succeed via exploitable vulnerabilities, while defenders must succeed reactively, by default, protecting systems. This economic and strategic imbalance means that every legislated weakness becomes a liability that grows over time. The UK's retreat is a recognition of this unsustainable asymmetry. Policymakers who attempt to legislate vulnerability are not creating a shortcut for law enforcement. But rather, guaranteeing exploitation by malicious actors. The debate is far from over, however the leaders who implement uncompromised encryption will secure a market premium by demonstrating how their trust layer is durable, geopolitical exposure is reduced, and their economies are resilient. These nations will attract capital and intellectual property, whereas those which concede will see their trust premiums disappear plus enterprise value decline. Ultimately, a cryptographic weakness isn't merely local. This vulnerability scales globally, instantly, and irreversibly. The relentless evolution of cyber threats means a backdoor's exposure only compounds over time, making its long-term maintenance an economically ruinous and strategically untenable proposition.

A New Chapter in Digital Geopolitics

Ultimately, the UK's decision marks a new chapter in the geopolitics of technology. The role of the United States in this matter, with U.S. Director of National Intelligence Tulsi Gabbard explicitly confirming the UK's reversal, underscores the transnational nature of this issue. American officials were not merely advocating for corporate interests but protecting the data and civil liberties of their own citizens, who would have been exposed by a UK mandate. This inter-governmental pressure highlights the emergence of a new form of digital diplomacy, where policy decisions in one country can directly impact the national security and economic interests of another. The UK's legal framework, specifically the Investigatory Powers Act of 2016, still contains the power to compel companies to provide access to encrypted data. The current reversal is a temporary reprieve. Furthermore, this fact alone indicates the need for a fundamental re-evaluation of legal frameworks to align them with the realities of modern cryptography. The continued legislative pursuit of decryption powers by intelligence agencies, despite the evident economic costs, reflects a deep-seated tension between traditional security paradigms and the new realities of digital commerce. This conflict will continue to dictate international relations.

7. Are We Witnessing the Death of the Browser, Websites, and Email?

by Roger Grimes
https://www.linkedin.com/pulse/we-witnessing-death-browser-websites-email-roger-grimes-rdvle/?trackingId=PURuuuKYTSOj5Utbu8SiXQ%3D%3D

It's 2 AM and I can't sleep.

There has been this growing narrative, based on facts, that AI is killing the website and the browser. I think there is a decent chance that email isn't far behind.

How will that change what you and I do on a daily basis? How will that change what companies offer? How will that change the company you work for?

I've been increasingly listening to podcasts and reading newsletters and posts by very smart people that say...again...based on facts...that AI is killing websites and the browser.

Here's an example. Just read the first section of this newsletter from Steve Gibson, one of the smartest guys on the Internet, especially on all things web.

It notes that AI and, in particular, LLMs, are significantly decreasing the amount of traffic that websites are getting. Which is existentially ironic because LLMs basically consume and train on website data, and I'm not sure what that means for LLMs if there are far fewer things to consume. How does the LLM model progress and change?

The facts are this: Since the release of ChatGPT by OpenAI in October 2022, more and more people are bypassing using browsers to look for things that then take them to websites. Today, in a growing trend, users either just use their favorite AI to learn something or use an Internet search engine that uses an AI to search for and return information. The process stops there.

It is less and less likely that anyone goes to a search engine to search for something, gets a bunch of links returned, and clicks on those links, which then take them to websites where they learn more. It's clear that the method of surfing the Internet is dying.

I certainly don't think today's young kids will be doing that when they are adults. It might happen sooner.

AI alone didn't kill the traditional web search experience. Instant messaging, TikTok, social media, and streaming certainly helped bury the bodies. Today's kids consume most of their news and experience through instant messaging, TikTok, and social media. Streaming is killing traditional television and cable programs.

Then you throw AI LLMs into the mix.

On a related note, just yesterday (in a single day) three of my closest friends told me they ditched their favorite browser for Perplexity, the hot new service that is basically an AI add-on that takes what your favorite AI LLM returns and juices it up. I spent a part of a morning this week watching Alan Ross Sorkin of CNBC (who I love) tell me he was loving using Perplexity, and CNBC is never on the cutting edge of technology trends. They are followers of emerging trends. If they are talking about something technology-wise, the smart money is already on it. Perplexity is a private company, but I wish I could invest in it.

Today's whole Internet is built on the idea that we get lots of free things...websites, services, etc., based on our visitation of their sites and services. They've got to earn money somehow to pay the bills. So far, this has meant selling ads and/or collecting data about us as we use their website and service. "If the site or service

is free, you are the product." Only a very small percentage of sites and services are able to charge for what they provide.

AI LLMs and AI-enabled search engine results are killing that revenue stream. Less visits mean less money.

I've heard from friends who work on browser development from within one of the big players that...excuse the related pun...the vibe has changed. Browsers manufacturers are not going to be developing significant new features. They are more in status maintain mode right now. If there is a new feature being added, it's something to bring more AI to the browser user and not more browsing to the browser user. Coders who want to be doing the best work are not going to browser development teams. It would like working on Archie and FTP servers of yesteryear.

That Internet economic model as we know it is soon over. What will replace it? I don't know.

The future vision of our online world is one where we have one or more personal AI agents that do everything we want for us. We don't go to a travel site to book travel; our personal AI agent does it for us. We don't go to an online store to buy something; our personal AI agent does it for us. We don't use an Internet search engine to look for something; our personal AI agent does it. We won't ask an AI to make up code for a website that we will review, modify, and then post. We will just ask our personal AI agent to make a website for us and it does the rest. We won't go to Amazon or Craigslist to buy or sell something; our personal AI agent will do it for us. You get the picture.

The idea that we go to this centralized search thing, type in something, look at the results that it brings back, and then spend time following links is just not something the world will be doing a few years from now. It's always been an inefficient time sink. By every metric we have, death of that traditional Internet experience is already happening.

I've long thought that it is very inefficient when I see something on TV that I want and then have to go to my browser, hopefully type in the right search string, which brings up the right sites that have what I want, is very inefficient. Why can't I just interact with the thing I'm seeing on TV and buy it?

I literally unsuccessfully tried for years to get patents on this technology when I was at Microsoft ten years ago. I never could get Microsoft to bite. But it's now clear that our future Internet experience will involve less Internet browser searches.

Google and Bing are likely to be the Digital Research, Alta Vista, and Blackberry of this generation.

Note: Phone calls have been dying for years as well. Who calls you? Do your kids want you to call them about anything?

And if you think about what the new model looks like, led by AI, TikTok, and instant messaging, it looks like a decent chance that email is also going away.

Lately, I've had friends, co-workers, and new bosses tell me that their preferred method of communication is instant messaging. Not email.

And I gotta tell you, this one hits just as hard. I love email. My email inbox is my workday and life. I love that I can look back at an email to refresh myself on a particular task or hold myself or someone else accountable for what they said they would do. I hate that I have to go browse through an instant messaging thread to hopefully find what they or I said or committed to.

Is email dying?

Websites, email, video downloads (including porn) were the killer apps that made the Internet the Internet. Without them, we don't have the Internet revolution.

Over 350B emails a day are sent worldwide.

I'd love to have some email metrics from the big boys (e.g., Gmail, Outlook.com, and Microsoft Office 365, etc.). Are we sending fewer emails per person over time, or is it like passwords, where we constantly say passwords are going away soon, even as we have more passwords than ever? Breakdown the metrics between personal email use and business use. Personal email use will likely decline faster than business email use.

Or maybe the better metric to ask for is the number of useful and wanted emails per person over time. I still get a lot of emails, but most are unwanted (e.g., ads, spam, phishing, etc.). It's like postal mail. I get a lot of paper mail, but almost none of it is wanted. The postal service could not survive if not for sending people a lot of junk they throw away immediately.

But if I think about it, a lot of my emails today are basically links to online social media posts where the real news is located. I get a lot of emails from people who post stories on LinkedIn telling me to visit LinkedIn to read the whole post. The rest is ads.

I get instant messages from my friends telling me to watch a particular video on TikTok. When I send an email to a bunch of friends about something funny or a post on social media, I literally feel like the dinosaur in the group. They aren't sending me emails. My kids certainly aren't sending me emails. My grandkids have never sent me an email and likely never will.

The new people I meet in my life are telling me to send them instant messages: Slack, SMS, or WhatsApp. We send over 24B SMS/MMS messages a day and over 84T a year. We send over 150M WhatsApp messages a day. Right now, there are more email messages sent than instant messaging messages, but the trend is clear. Instant messaging platforms are gaining users. Email platforms are being used less by young people. Their experience is not my experience.

My own anecdotal experience is telling me that email is dying.

I am a dinosaur.

So, imagine that Internet search engines, websites, and email are soon gone. It's replaced by personalized AI agents.

What does that online life look like?

As a 38-year computer security practitioner, what does computer security look like? Nearly my entire career has been spent fighting email and browser attacks.

Well, it looks like a world where the war trenches are agentic AI-focused, stopping and fighting attacks that come through us in our personalized AI agent(s). Everything we do online will be through our personalized AI agents. It will be doing everything for us. Our communication history will be there. Our news will be there. What we are working on will be there. The ads that we will see will be there. The reachout from others will be there.

The threats will be there.

It blows me away to think that my browser, Internet search, and email are soon likely to be gone. But you can't look at the data or interface to young kids and see any different outcome. They are not spending their time online like their parents and grandparents did.

I would love to be wrong. I don't think I am.

8. Quantum-safe security: Progress towards next-generation cryptography

by Mark Russinovich and Michal Braverman-Blumenstyk
https://www.microsoft.com/en-us/security/blog/2025/08/20/quantum-safe-security-progress-towards-next-generation-cryptography/

Quantum computing promises transformative advancements, yet it also poses a very real risk to today's cryptographic security. In the future scalable quantum computing could break public-key cryptography methods currently in use and undermine digital signatures, resulting in compromised authentication systems and identity verification.

While scalable quantum computing is not available today, the time to prepare is now. Microsoft is preparing to be quantum-safe and partnering with regulatory and technical bodies like the NIST, IETF, IISO, Distributed Management Task Force (DMTF), Open Compute Project (OCP), and ETSI to align on quantum-safe encryption standards and support worldwide interoperability.

The opportunity and challenge ahead

Migration to post quantum cryptography (PQC) is not a flip-the-switch moment, it's a multiyear transformation that requires immediate planning and coordinated execution to avoid a last-minute scramble.

It is also an opportunity for every organization to address legacy technology and practices and implement improved cryptographic standards. By acting now, organizations can upgrade to modern cryptographical architectures that are inherently quantum safe, upgrade existing systems with the latest standards in cryptography, and embrace crypto-agility (the ability to easily change algorithms) to modernize their cryptographic standards and practices and prepare for scalable quantum computing.

The investment in a quantum future

At Microsoft, we have been investing in this shift by developing both the advances in quantum computing, such as the Majorana 1 quantum processor and 4D geometric error correction codes, and the requirements for PQC.

Our PQC effort began in 2014 when we published research on post-quantum algorithms and later quantum cryptanalysis to more rigorously determine when contemporary algorithms will be broken. To contribute to PQC algorithm development we participated in four submissions to the original 2017 NIST PQC call and one submission to the current call. Since 2018 we have been experimenting with verified versions of PQC algorithms and in 2019 Microsoft Research completed testing of an experimental PQC-protected VPN tunnel between Redmond, Washington, and Scotland using the Project Natick underwater datacenter.

To support standards development and foster the integration of post-quantum cryptographic algorithms into internet protocols, Microsoft joined as a founding member of the Open Quantum Safe project. Additionally, we led the integration workstream of the NIST NCCoE Post-Quantum project. Microsoft Research was contributing to updating the ISO cryptography standard to include PQC, with our FrodoKEM cryptosystem, developed in collaboration with academic and industry partners, poised to become an ISO standard algorithm.

In 2024, we announced and contributed Adams Bridge Accelerator, an open-source quantum resilient cryptographic hardware accelerator and integrated into Caliptra 2.0, part of Open Compute Project (OCP).

Finally, to help customers and partners begin exploration and integration of quantum-safe algorithms into their environments we previewed PQC capabilities for Windows Insiders and Linux and updated SymCrypt to support verified PQC algorithms. This will help them proactively prepare their software and services for PQC support.

Creating a Quantum Safe Program

In 2023, Charlie Bell, Executive Vice President for Microsoft Security, outlined Microsoft's vision to build a quantum-safe future, which led to the creation of the Microsoft Quantum Safe Program (QSP). This program unifies and accelerates Microsoft's efforts to protect our infrastructure, as well as that of our customers, partners, and ecosystems, from the evolving risk of quantum computing.

The following timelines shows a consolidated view of where we are today, and what to expect in the near future as we progress this important program as an industry.

The Microsoft QSP is aligned with United States government requirements and timelines for quantum safety, including the US Office of Management and Budget (OMB), the Cybersecurity and Infrastructure Security Agency (CISA), NIST, and the National Security Agency's guidance for organizations to start preparing and transitioning for PQC enablement. We also closely monitor quantum-safe initiatives from international governments, including the European Union, Japan, Canada, Australia, and the United Kingdom, to align with their efforts.

You can learn more about our collaboration with standards bodies and recommendations for effective government policies to accelerate the quantum-safe transition in the Microsoft On the Issues blog by Amy Hogan Burney, Vice President, Customer Security and Trust.

The Microsoft QSP strategy

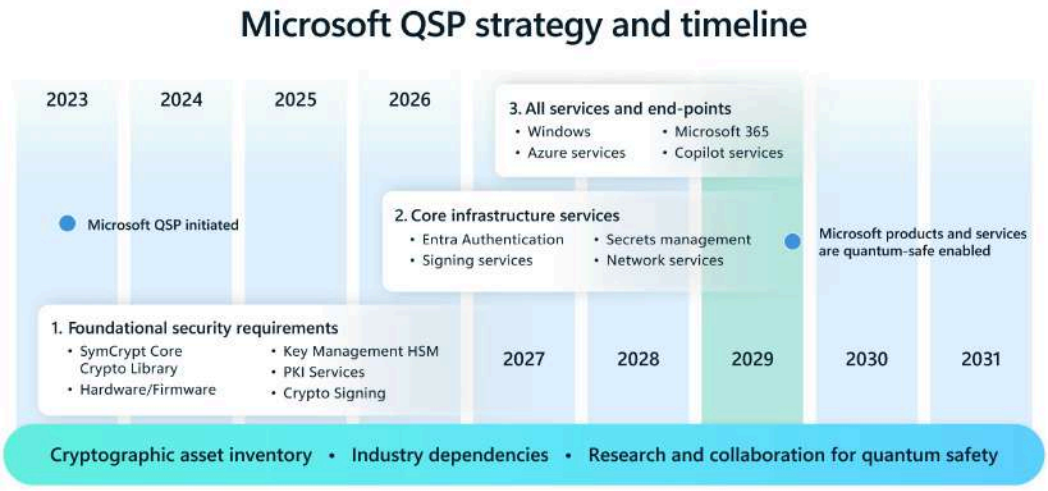
Our QSP is a comprehensive and company-wide effort to enable Microsoft, our customers, and partners, to transition smoothly and securely into the quantum era. The program is governed by the QSP leadership team with representatives across all major business groups, research and engineering divisions, and functions.

The QSP strategy is guided by three priorities:

1. Make Microsoft quantum safe by updating Microsoft first- and third-party services, supply chain, and ecosystem to become quantum safe and crypto-agile.
2. Support customers, partners, and ecosystems to become quantum safe with appropriate tools and guidance.
3. Promote global research, standards, and solutions for quantum-safe technologies and crypto-agility.

Our quantum-safe journey began with an enterprise-wide inventory to assess and prioritize cryptographic asset risks. From there, we partnered with industry leaders to address critical dependencies, investing in quantum safe research and collaborating on hardware and firmware innovation. We accelerated the adoption of quantum-resilient algorithms across core infrastructure, supported by Microsoft's open-source silicon initiatives.

As a result of this foundational work, we are aligned with global government timelines, striving to meet even the most forward-leaning CNSA 2.0 deadlines outlined in CNSSP-15. Combining the different regulations' aspects and timelines worldwide, Microsoft's roadmap aims to complete transition of its services and products by 2033—two years before the 2035 deadline set by most governments—aiming to enable early adoption of quantum-safe capabilities by 2029, gradually making them default in subsequent years, or sooner where possible.



To maintain the resilience of Microsoft's services and systems against quantum computers powerful enough to break modern cryptographic algorithms, we've developed a phased transition strategy built on a modular framework. This approach considers each service unique requirements, performance constraints, and risk profile, resulting in either a direct shift to full PQC or a hybrid approach combining classical and quantum-resistant algorithms as an interim step. Therefore, as early adoption will begin by 2029, core services will reach maturity a few years before then.

Here are the three key phases for this strategy:

1. **Foundational security components**

   Microsoft has integrated PQC algorithms into foundational components like SymCrypt, the primary cryptographic library that provides consistent cryptographic security across Windows, Microsoft Azure, Microsoft 365 and other platforms. SymCrypt supports both symmetric (for example, AES [Advanced Encryption Standard]) and asymmetric algorithms (for example, RSA [Rivest–Shamir–Adleman], ECDSA [Elliptic Curve Digital Signature Algorithm]), providing essential cryptographic operations such as encryption, decryption, signing, verification, hashing, and key exchange. Most recently we've made ML-KEM (Module-Lattice Key Encapsulation Mechanism) and ML-DSA (Module-Lattice Digital Signature Algorithm) available through Cryptography API: Next Generation (CNG) and Certificate and Cryptographic messaging functions. These capabilities are available to Windows Insiders and Linux customers now, with additional foundational capabilities coming through the next five years, always aligning and timebound to evolving industry standards and advancements.

   As quantum computing advances, the threat of Harvest Now, Decrypt Later (HNDL) cyberattacks become increasingly pressing—where threat actors record and store encrypted data today with the intention of decrypting it once quantum capabilities mature. To counter this risk, security protocol standards are prioritizing quantum-safe key exchange mechanisms. For instance, TLS 1.3 is being enhanced to support both hybrid and pure post-quantum key exchange methods, making it a robust adaptable foundation for integrating PQC algorithms. With version 1.9.0 of SymCrypt-OpenSSL, we've enabled TLS hybrid key exchange as per the latest IETF internet draft, providing an early opportunity to help prepare for HNDL threats. This capability will be coming to Windows TLS stack soon.

2. **Core infrastructure services**

   Updating foundational components in products and services, considered core infrastructure service, to provide quantum safety for Microsoft and our customers from future quantum risks. Examples include Microsoft Entra authentication, key and secret management, and signing services. By prioritizing these services, Microsoft will protect the most sensitive and essential components first, providing a strong foundation for the broader transition.

3. **All services and endpoints**

   Integrating PQC into Windows, Azure services, Microsoft 365, data platforms, AI services, and networking enables the broader ecosystem of Microsoft services to be quantum safe, providing comprehensive protection across all platforms and applications.

9. "Quantum Advantage" Means Different Things to Quantum Scientists and End Users

by *Doug Finke*
https://quantumcomputingreport.com/quantum-advantage-means-different-things-to-quantum-scientists-and-end-users/

The term "Quantum Advantage" is getting a lot of play these days, and it is indicative of the fact that quantum computers are providing ever increasing performance almost on a daily basis creating expectations on when they will surpass the capabilities of classical machines. But have you stopped to consider how one would define "Quantum Advantage" or the fact that different people might look at it differently.

A quantum scientist would define "Quantum Advantage" as when a quantum computer can solve a useful, real-world problem more effectively than any classical computer. "More effectively" can mean that it solves the problem faster, with greater accuracy, at a lower cost, or with less energy consumption. But there is a possible catch here. The quantum scientist would compare the quantum solution against the latest state-of-the-art classical computing algorithm running on a large classical computing HPC system developed by their most capable programmer or brilliant PhD student who might need a long period of time to develop the right approach.

End users are more pragmatic. End users generally don't care if they obtain the solution on a classical or a quantum computer. Also, a CIO in a commercial organization may not have access to the most brilliant PhD student, the latest hardware, or the latest software packages containing state-of-the-art algorithms. They also may not have a large amount of time. They just want something that works as quickly as possible as easily as possible.

In addition, different end users may have different requirements that are much better than classical solutions. A quantum solution needs to be in order to use it? I recently talked with a developer working at a large industrial company working on optimization software for one of their manufacturing plants. He had developed a quantum-based solution for scheduling production and created a solution that could provide a

10% efficiency advantage than the classical one his company was currently using. When I asked him when they were planning on putting this into production, he replied that a 10% improvement was not quite good enough for his management to approve changing the operation to install new software and train the employees on how to use it. His next step is to improve his solution to provide an even better performance advantage to make the transition worthwhile.

On the other hand, a quantum advantage of 10% in a financial application, could likely incentivize a financial company to make the switch to quantum, because small improvements could still be very significant when you are dealing with a large amount of money.

A final factor that could influence an end user's choice between a quantum solution and a classical solution is the ease of use. In some cases, a quantum solution that is easier to use might win over a classical based solution that is harder to use, even if there isn't much of a performance advantage.

The bottom line for quantum providers is to provide a strategic quantum advantage that provides value to the end users who use their services. And that is not quite the same as providing just a pure technical advantage. So, for a quantum provider, a focus on applications, customer support, and getting their users into production is what will bring in the revenue and help make the quantum provider more successful.

10. US says UK has agreed to drop encryption 'back door' demands against Apple

by Bill Goodwin
https://www.computerweekly.com/news/366629434/US-says-UK-has-agreed-to-drop-encryption-back-door-demands-against-Apple

The US director of national intelligence has said that the UK has agreed to drop demands for Apple to create a "back door" that would have enabled the UK to gain access to the data of US citizens.

Tulsi Gabbard said the announcement followed discussions over the past few months with the UK, US president Donald Trump and vice-president JD Vance over the UK's decision to issue an order against Apple requiring back-door access to encrypted data stored on Apple's iCloud that could affect US citizens.

The announcement brings an end to a simmering political row between the US and the UK, following home secretary Yvette Cooper's decision to issue a secret order under the Investigatory Powers Act 2016 against Apple in January.

The decision led Apple to withdraw its Advanced Data Protection (ADP) service, which offers encrypted cloud storage services, from UK customers, stating: "We have never built a back door or master key to any of our products or services and we never will."

The Home Office has not stated whether it would continue to require Apple to provide access to encrypted data stored by UK users if Apple were to reinstate its ADP Service to Apple customers in the UK.

The Home Office said in a statement that it had longstanding arrangements with the US to tackle threats such as terrorism and child abuse, which included safeguards for privacy and state sovereignty.

Risk to US civil liberties

Gabbard wrote in a statement on X: "Over the past few months, I've been working closely with our partners in the UK, alongside @POTUS and @VP to ensure Americans' private data remains private and our Constitutional rights and civil liberties are protected.

"As a result, the UK has agreed to drop its mandate for Apple to provide a 'back door' that would have enabled access to the protected encrypted data of American citizens and encroached on our civil liberties," she said.

According to a report by the *Financial Times*, Vance – who has previously attacked Europe and the UK for limiting free speech – intervened to ensure the UK government withdrew "the current back-door order" to Apple.

Gabbard publicly raised concerns in a letter to US lawmakers that the UK's order against Apple could "undermine Americans' privacy and civil liberties". President Trump has also criticised the order as something that would be expected in China.

Apple has made a formal complaint to the Investigatory Powers Tribunal over the UK order, known as a Technical Capability Notice, which is due to be heard in early 2026.

The Investigatory Powers Act 2016, also known as the "Snoopers' Charter", allows the UK to impose orders on companies requiring them to make technical changes to their systems and allow access to data by UK law enforcement and intelligence services, and applies both in the UK and extraterritorially.

UK users may still face encryption ban

Commenting on the US announcement, Jim Killock, Executive Director of Open Rights Group, a campaign organisation, said that although the UK may have dropped its demands for Apple to backdoor all of its users across the globe, UK users may still be banned from using Apple's ADP encryption service.

"If Apple does restore ADP to UK users, there will be serious questions of trust," he added. "The UK's powers to attack encryption are still on the law books, and pose a serious risk to user security and protection against criminal abuse of our data."

Christopher Weatherhead, technology lead at civil society group, Privacy International has filed a legal challenge against the Home Office with Liberty at the Investigatory Powers Tribunal, said there fundamental issues with Technical Capability Notices.

"While Tulsi Gabbard's statement appears to be a positive step for American citizens, it neither changes the secret regime that exists with Technical Capability Notices, nor stops the UK Government from issuing other such notices in the future," he added.

Call to amend US Cloud Act

In the US , Greg Nojeim, of the non-profit Centre for Democracy and Technology, said the organisation cautiously welcomed the UK's apparent decision to drop its demand for a back door, adding that back doors "put the privacy and security of consumers, businesses and nationals at risk."

"The Administration should be more transparent about any deal it cut with the UK, and Congress should amend the CLOUD Act to prevent other countries from issuing similar orders to U.S. service providers. No foreign government should be able to force providers to disable end-to-end encryption, and threaten the privacy and security of Americans and users around the world," he said.

Critical safeguards

The Home Office said its joint security and intelligence arrangements with the US to tackle the most serious threats, such as terrorism and child sexual abuse, "have long contained safeguards to protect privacy and sovereignty".

The Home Office pointed to the US-UK Data Access Agreement, which allows UK and US law enforcement to request data from telecommunications companies when investigating serious crimes, and "includes critical safeguards to prevent the UK and US from targeting the data of each other's citizens".

"We will continue to build on those arrangements and we will also continue to maintain a strong security framework to ensure that we can continue to pursue terrorists and serious criminals operating in the UK," a spokesman said. "We will always take all actions necessary at the domestic level to keep UK citizens safe."

The Home Office said that it did not comment on operational matters including confirming or denying the existence of orders made under the Investigatory Powers Act.

11. "Terrifying Quantum Shock": China's Processor Leaps 1 Quadrillion Beyond Limits and Throws Google's Willow Into Global Crisis

by Noah Bennett
https://www.rudebaguette.com/en/2025/08/terrifying-quantum-shock-chinas-processor-leaps-1-quadrillion-beyond-limits-and-throws-googles-willow-into-global-crisis/#google_vignette

Quantum computing has crossed a new frontier with the unveiling of the Zuchongzhi 3.0 processor by the University of Science and Technology of China (USTC). This processor reportedly operates at speeds a quadrillion times faster than the most advanced supercomputers available today. Such a groundbreaking development marks a significant milestone in the field of quantum technology, setting a new benchmark for computational speed and efficiency. While the implications of this technological leap are vast, it primarily positions China as a formidable player in the ongoing race for quantum supremacy.

The Mechanics of Superconducting Qubits

The Zuchongzhi 3.0 quantum processor is a marvel of engineering, utilizing 105 transmon qubits strategically arranged in a 15-by-7 lattice. These qubits are crafted from superconducting materials like tantalum and niobium, which enhance the processor's resilience to noise—a critical factor in quantum computing. The transition to 105 qubits from its predecessor's 66 signifies a tremendous leap forward.

Superconducting qubits are pivotal in achieving the much-desired goal of quantum supremacy, where quantum computers can outperform classical supercomputers in specific tasks. The coherence time of these qubits, or the duration they can maintain their quantum state, is essential for performing complex calculations. Zuchongzhi 3.0 showcases advanced coherence and gate fidelity, with single-qubit gate fidelity reaching 99.90% and two-qubit gate fidelity at 99.62%. These metrics are on par with leading technologies like Google's Willow chip, indicating a significant stride towards reliable quantum computations.

Evaluating Quantum Supremacy Through Benchmarks

To validate its performance, the Zuchongzhi 3.0 processor was subjected to the random circuit sampling (RCS) benchmark, a standard test in quantum computing. It completed the task in mere seconds, a feat that the previous Sycamore chip from Google required substantially more time to achieve. This demonstration underscores the advancements made by the USTC team in propelling quantum computing capabilities forward.

While the results are impressive, it's crucial to acknowledge that RCS benchmarks are tailored to leverage quantum advantages. As classical computing algorithms evolve, they may close the performance gap with quantum methods. Nevertheless, Zuchongzhi 3.0's achievements illuminate the potential of quantum processors to address complex real-world issues, marking the dawn of a new computing era.

Innovations in Engineering and Design

The remarkable performance of Zuchongzhi 3.0 is attributed to a series of engineering innovations. The design enhancements include improved fabrication techniques that optimize qubit structures. These structures are created using tantalum and aluminum, bonded through a sophisticated indium bump flip-chip process, which enhances precision and minimizes contamination.

Such engineering advancements are crucial in overcoming challenges related to quantum error correction and gate fidelity. By achieving higher fidelity in qubit operations, the processor minimizes errors, boosting computational accuracy. These improvements are vital as they bring the prospect of practical quantum computing applications closer to reality.

Quantum Computing's Path Forward

The development of the Zuchongzhi 3.0 processor is a pivotal milestone in the pursuit of quantum computing supremacy. As quantum processors evolve, they promise transformative impacts across various fields, including cryptography, pharmaceuticals, and complex optimization problems. However, the path forward is fraught with challenges such as enhancing scalability, improving coherence times, and integrating these processors with existing technologies.

The relentless push to expand the horizons of quantum computing begs the question: *How will these technological breakthroughs redefine the landscape of technology and society in the years to come?* The journey to fully harness quantum computing's potential is only beginning, and its implications are set to be both profound and far-reaching.

12. What is lattice-based cryptography, and why does it matter in the post-quantum era?

by Akash Deep
https://www.expressvpn.com/blog/lattice-based-cryptography/

It's easy to forget how much our lives depend on encryption. Every time you log into your bank account, send a message, or save a password, there's some heavy-duty math working quietly in the background to keep your data safe.

The problem? Most of the encryption we use today (things like RSA and elliptic-curve cryptography) was designed long before anyone worried about quantum computers. And quantum machines, once powerful enough, could break those systems in ways that regular computers can't.

We're not at that point yet, but it's not science fiction anymore, either. Experts agree it's only a matter of time, and that's why cryptographers are already working on "quantum-resistant" solutions.

One of the strongest contenders? Lattice-based cryptography. It's not a brand-new concept, but it's getting a lot more attention these days, and for good reason. In this article, we'll break down what lattice-based cryptography is, how secure it can be, and the challenges it faces before becoming mainstream.

Introduction to lattice-based cryptography

Lattice-based cryptography is a type of encryption and digital signature system built on the math of lattices: multi-dimensional grids made up of repeating points. These structures give rise to some incredibly challenging mathematical problems, the kind that even quantum computers don't have known shortcuts for.

That's exactly why lattices are so appealing for cryptography. Their complexity makes them an excellent foundation for building secure systems designed to withstand future quantum threats.

What is a lattice in cryptography?

Imagine looking at a sheet of graph paper with its neat 2D grid pattern. Every intersection follows a set of mathematical rules based on how its lines (vectors) combine.

Lattices extend this concept into hundreds or even thousands of dimensions, creating infinite point sets that follow predictable spacing but become extraordinarily difficult to analyze in higher dimensions.

These high-dimensional lattices are packed with hard math problems. One of the most famous is the Shortest Vector Problem (SVP): finding the shortest non-zero vector in a lattice. It sounds simple, but as the number of dimensions explodes, this problem becomes nearly impossible to solve. Think of it like searching for the tiniest puzzle piece in a massive 3D puzzle without knowing what the final picture looks like.

Even quantum computers don't have an efficient way (as far as we know) to solve these problems, which is why lattice-based cryptography is considered quantum-resistant.

Who invented lattice-based cryptography?

The field took shape in the mid-1990s with Miklós Ajtai's breakthrough: the first cryptographic function directly tied to the difficulty of solving lattice problems. This introduced the concept of "worst-case to average-case reduction," meaning breaking certain lattice systems is as hard as solving the toughest lattice problems.

These problems include SVP and the Closest Vector Problem (CVP), which are notoriously hard to solve. Building on this, Cynthia Dwork introduced the Short Integer Solution (SIS) problem, further strengthening the theoretical foundation.

In 1998, NTRU emerged as the first practical lattice encryption scheme. Unlike RSA or elliptic-curve cryptography, which rely on factoring or discrete logarithms, NTRU is based on lattice problems believed to remain hard even for quantum computers.

Then in 2005, Oded Regev introduced the Learning With Errors (LWE) problem, which became the backbone of many modern post-quantum encryption systems.

How lattice-based cryptography enables secure encryption

Lattice-based cryptography protects data and verifies authenticity using mathematical problems that remain hard to solve, even with quantum computers. The core idea is to generate secure keys and ciphertexts from complex, high-dimensional lattice structures that resist known attacks.

Today, it already powers public-key encryption and digital signatures, though most systems still use RSA or elliptic curves. As post-quantum standards roll out, lattice-based methods are expected to see much wider adoption.

These lattice-based cryptographic systems also enable advanced features like homomorphic encryption, which allows data to be processed while still encrypted.

Why is that exciting? Because it means you could, for example, send encrypted data to a cloud service or an AI model, have it perform computations, and get the results back without ever revealing the actual data. This could be game-changing for fields like healthcare, finance, and even large language models (LLMs), where privacy and security are critical but you still need powerful computation.

Other innovations, like private search (finding information in encrypted data without revealing what you're looking for), also build on the flexibility of lattice-based cryptography, showing why it's more than just a quantum-resistant replacement for today's systems.

How lattice-based public key encryption works

At its core, lattice encryption hides messages inside math problems that are easy to create but extremely hard to reverse without the correct key.

A common approach is built on the Learning With Errors problem: solving slightly "noisy" linear equations. Without the secret key, it's like trying to complete a puzzle with missing pieces. The private key acts as a trapdoor, allowing the intended recipient to filter out noise and recover the original message.

Another well-known method is NTRU, which uses polynomial operations instead of matrices. Its public key behaves like a one-way function: simple to compute but very hard to reverse. NTRU is fast, has relatively small key sizes, and has withstood decades of cryptanalysis, making it a strong choice for real-world deployment.

Digital signatures with lattice-based schemes

Digital signatures prove a message came from someone holding a specific secret key without revealing that key. Lattice schemes rely on hard problems like Short Integer Solution, where finding a valid solution without the secret is virtually impossible.

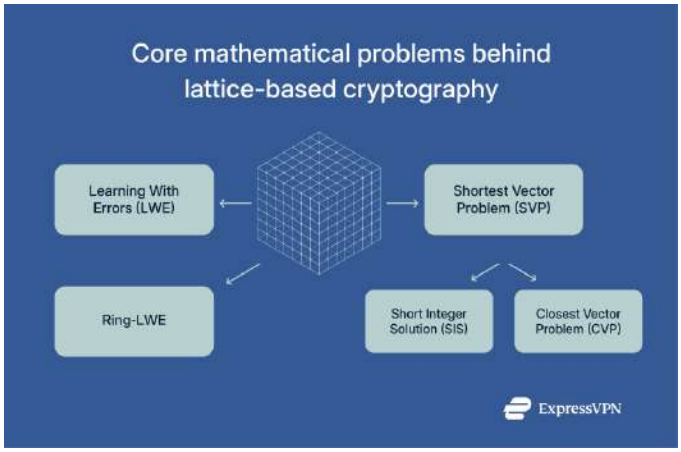
A leading example is CRYSTALS-Dilithium, which generates a short vector tied to both the message and secret key. Anyone with the public key can verify the signature's authenticity, but they still can't learn the secret key itself.

Another prominent scheme, Falcon, generates more compact signatures using trapdoor sampling, but its reliance on floating-point arithmetic makes it harder to implement securely.

Both schemes are quantum-resistant and efficient, even though their keys and signatures are larger than traditional options like RSA or ECDSA (Elliptic Curve Digital Signature Algorithm). They're already being tested in real-world systems (including browsers, TLS libraries, and infrastructure providers like Cloudflare), paving the way for post-quantum digital security.

Hard mathematical problems that ensure quantum resistance

The security of lattice-based cryptography comes from a small set of mathematical problems that are simple to describe but incredibly hard to solve, especially at the scales used in cryptography. These problems are what give lattice-based systems their post-quantum strength, making them resistant to both classical and quantum attacks.



Learning With Errors (LWE)

Introduced by Oded Regev in 2005, LWE is a cornerstone of post-quantum cryptography. At its core, it looks like a simple math challenge: *solving systems of linear equations, but with a twist. Each equation has a small amount of random noise added*.

In formal terms, each LWE sample looks like (A, b = (A·s + e) mod q), where "A" is public, "s" is the secret, and "e" is a small random error (the "noise"). That noise is what makes LWE hard. Without it, you could easily recover "s." With it, solving for "s" becomes incredibly difficult, so much so that even quantum computers don't have a known shortcut.

Regev also proved something powerful: if you can solve random LWE instances efficiently, you can also solve some of the hardest lattice problems in their worst-case form. This "worst-case to average-case reduction" gives LWE a rare kind of provable security, provided the parameters (error size, randomness, etc.) are chosen correctly.

Ring-LWE explained

The Ring Learning With Errors (Ring-LWE) problem is essentially a more efficient version of LWE. Instead of working with large vectors and matrices, it uses polynomials in a special mathematical space called a polynomial ring. This structure allows for faster operations and smaller keys, two major advantages for practical encryption.

How does it work?

- In standard LWE, you multiply vectors and add noise.
- In Ring-LWE, you multiply polynomials with small coefficients, then reduce the result modulo a fixed polynomial (think of it like doing arithmetic in a "wrap-around" polynomial space).

Despite the added structure, Ring-LWE keeps the same fundamental hardness assumptions that make lattice cryptography secure. However, cryptographers must choose parameters carefully because too much structure can sometimes introduce vulnerabilities.

Modern post-quantum algorithms, such as *CRYSTALS-Kyber (encryption)* and *Dilithium (digital signatures)*, use a generalized form called Module-LWE. This strikes a balance: it keeps the efficiency gains of structured lattices while preserving strong, well-analyzed security guarantees.

Shortest Vector Problem (SVP) and related constructs

The Shortest Vector Problem (SVP) sounds simple: find the shortest non-zero vector in a given lattice. In low dimensions, it's straightforward. But in the hundreds of dimensions used in cryptography, even finding a good approximation becomes exponentially harder as the dimension grows.

Many lattice-based cryptosystems rely on this difficulty. For example, recovering a private key often boils down to solving an SVP-like problem, essentially hunting for a specific short vector hidden inside a carefully structured lattice.

Two related problems also play key roles:

- **SIS (Short Integer Solution):** Find a short linear combination of given vectors that equals zero (modulo some value). This is widely used in digital signature schemes and has been proven to be as hard as the worst-case version of SVP.
- **CVP (Closest Vector Problem):** Given a random point, find the nearest lattice point. CVP models error correction in encryption and, like SVP, is believed to be intractable in high dimensions.

Popular lattice-based cryptographic schemes

Some lattice-based cryptographic schemes are already in use. Three that stand out are NTRU (a fast, early encryption scheme), CRYSTALS-Kyber (the NIST-selected key exchange), and CRYSTALS-Dilithium (a standardized digital signature scheme). Each applies lattice techniques differently but is built on the same principle: hiding secrets inside hard mathematical problems.

NTRU encryption

Introduced in 1998, NTRU is one of the oldest lattice-based encryption schemes and remains one of the fastest. It represents both public and private keys as short polynomials, and encryption is simply lightweight polynomial multiplication, much faster than RSA or Diffie-Hellman, especially on low-power devices.

Internally, it hides the message inside a structured lattice using modular polynomial arithmetic, where only someone with the private key can reliably decode it.

NTRU's security comes from a lattice problem similar to finding short vectors in high-dimensional polynomial spaces. While it hasn't been mathematically proven to tie to worst-case lattice problems (unlike LWE-based schemes), it's stood up to decades of cryptanalysis.

In the NIST post-quantum standardization process, NTRU variants like NTRU-KEM and NTRU Prime reached the final rounds, highlighting their resilience and performance.

CRYSTALS-Kyber: Post-quantum key encapsulation

Kyber is a lattice-based key encapsulation mechanism (KEM) selected by NIST as the first post-quantum encryption standard. It's based on the Module-LWE problem, a structured version of the LWE problem that allows for fast and compact encryption.

Kyber enables two parties to establish a shared secret over an insecure connection (similar to RSA or Diffie-Hellman) but with quantum resistance.

The core idea is to embed a shared secret inside a structured mathematical problem, then allow the recipient (armed with a private key) to extract it, even in the presence of deliberate noise. As of now, there's no known method that can break this process.

Its small keys and ciphertexts (around 1–1.5 KB), plus high-speed performance, make it practical for real-world use. Kyber is already being deployed in browsers, TLS libraries, and companies like Cloudflare, helping secure HTTPS traffic with post-quantum protection.

CRYSTALS-Dilithium: Secure digital signatures

Dilithium, another NIST-selected scheme, provides digital signatures built on the Module-LWE and Module-SIS problems. It produces "short" vectors as signatures: proofs that can only be created by someone with the secret key.

These compact outputs serve as mathematical fingerprints that are easy to produce with the key but nearly impossible to forge without it.

Dilithium avoids floating-point arithmetic (unlike Falcon), which simplifies constant-time implementation and reduces the risk of timing-based side-channel attacks, making it easier to implement securely. Its public keys and signatures are a few kilobytes, larger than ECDSA but efficient enough for modern systems.

With its simplicity, robustness, and flexibility across security levels, Dilithium is positioned as a leading candidate to replace traditional signature algorithms in post-quantum environments.

Falcon: Compact Digital Signatures Based on NTRU

Falcon is another standardized signature scheme, based on NTRU lattices. It uses trapdoor sampling to produce highly compact signatures, which are often smaller than Dilithium's. This makes it appealing for applications where bandwidth and storage are at a premium.

However, Falcon's reliance on floating-point arithmetic makes it trickier to implement securely, which is why Dilithium is often recommended as the default choice.

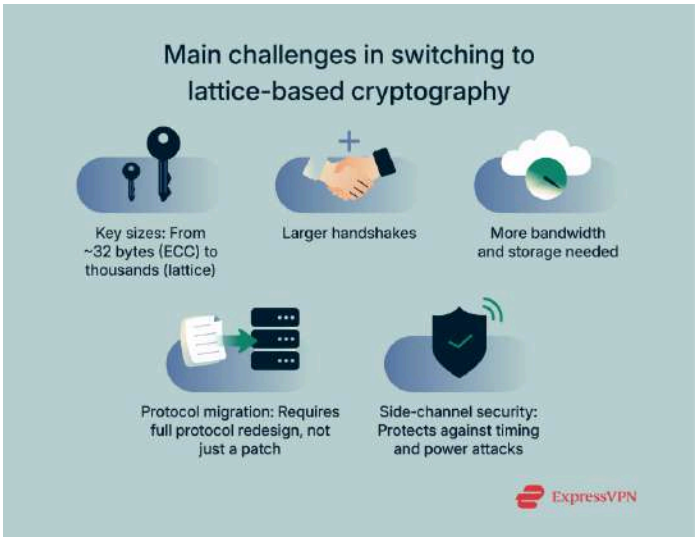
Advantages and practical considerations of lattice-based cryptography

Benefits over traditional cryptography

- **Quantum resilience:** Designed to withstand attacks that would break RSA or ECC.
- **Strong security guarantees:** Many schemes are as hard to break as solving the toughest lattice problems.

- **Efficient in practice:** With the right optimizations, schemes like Kyber and Dilithium often outperform RSA on modern CPUs.
- **Advanced capabilities:** Enables tools like homomorphic encryption and private search.
- **Hardware-friendly:** Structured math operations scale well on modern processors.

Implementation challenges and standardization



- **Larger key sizes:** Switching from ECC to lattice crypto increases storage and transmission requirements.
- **Complex migration:** It's not just swapping libraries. Protocols, hybrid modes, and testing all need updates.
- **Deployment maturity:** While the math is decades old, real-world use is still new.
- **Side-channel risks:** Secure coding practices remain critical.
- **Future agility:** Standards and attacks evolve, so cryptographic agility is essential.

Real-world application examples

- **TLS and HTTPS:** Cloudflare, Google, and Mozilla have tested Kyber in hybrid TLS deployments.
- **VPNs:** ExpressVPN initially integrated Kyber into its Lightway protocol in hybrid mode to protect session keys against future quantum threats. It has since transitioned to ML-KEM (the finalized NIST standard based on Kyber) for stronger post-quantum security.
- **Government use:** Agencies like the NSA are shifting to quantum-safe standards. Though details are classified, lattice schemes are among the top candidates for military and diplomatic encryption.
- **Software signing:** Companies like Microsoft and IBM are testing Dilithium for software update signing.
- **Crypto libraries:** OpenSSL, BoringSSL, and libsodium are integrating lattice algorithms with NIST's parameters. Many cryptographic libraries now support post-quantum algorithms like Kyber and Dilithium, but full integration typically requires protocol updates, hybrid modes, rigorous testing, and security audits to ensure compatibility and security.

Limitations and security considerations

Lattice-based cryptography is grounded in decades of mathematical research, but real-world deployment is still relatively new. As these systems move from theory to widespread use, continued peer review and cautious implementation remain essential.

Core problems like LWE, SVP, and SIS remain solid under current knowledge. Vulnerabilities so far have stemmed from poor parameter choices or flawed implementations, not the math. Several earlier lattice schemes have been broken or weakened due to improperly chosen parameters, reinforcing the need for conservative design and peer-reviewed implementations.

Open research challenges and future directions

- **Key size reduction:** Efforts are underway to reduce storage and transmission overhead.
- **Stronger reductions:** Researchers continue to tighten the connection between lattice schemes and worst-case hardness.
- **Advanced use cases:** Applications in privacy-preserving computation and blockchain are emerging.
- **Quantum monitoring:** Security parameters may need adjusting if future quantum techniques improve.
- **Implementation feedback:** Real-world deployment is helping refine standards and best practices.

13. NIST Finalizes 'Lightweight Cryptography' Standard to Protect Small Devices

by Chad Boutin
https://www.nist.gov/news-events/news/2025/08/nist-finalizes-lightweight-cryptography-standard-protect-small-devices

It's the little things that matter most, as the saying goes, and the NIST has got their back. NIST's newly finalized lightweight cryptography standard provides a defense from cyberattacks for even the smallest of networked electronic devices.

Released as *Ascon-Based Lightweight Cryptography Standards for Constrained Devices* (NIST Special Publication 800-232), the standard contains tools designed to protect information created and transmitted by the billions of devices that form the Internet of Things (IoT) as well as other small electronics, such as RFID tags and medical implants. Miniature technologies like these often possess far fewer computational resources than computers or smartphones do, but they still need protection from cyberattacks. The answer is lightweight cryptography, which is designed to defend these sorts of resource-constrained devices.

"We encourage the use of this new lightweight cryptography standard wherever resource constraints have hindered the adoption of cryptography," said NIST computer scientist Kerry McKay, who co-led the project with her NIST colleague Meltem Sönmez Turan. "It will benefit industries that build devices ranging from smart home appliances to car-mounted toll registers to medical implants. One thing these electronics have in common is the need to fine-tune the amount of energy, time and space it takes to do cryptography. This standard fits their needs."

The standard is built around a group of cryptographic algorithms in the Ascon family, which NIST selected in 2023 as the planned basis for its lightweight cryptography standard after a multiround public review process. Ascon was developed in 2014 by a team of cryptographers from Graz University of Technology, Infineon Technologies and Radboud University. In 2019 it emerged as the primary choice for lightweight encryption in the CAESAR competition, a sign that Ascon had withstood years of examination by cryptographers.

In the standard are four variants from the Ascon family that give designers different options for different use cases. The variants focus on two of the main tasks of lightweight cryptography: authenticated encryption with associated data (AEAD) and hashing.

ASCON-128 AEAD is useful when a device needs to encrypt its data, verify the authenticity of the data, or – crucially – both. A common weakness of small devices is their vulnerability to "side-channel attacks," in which an attacker can extract sensitive information by observing physical characteristics like power consumption or timing. While no cryptographic algorithm is inherently immune to such attacks, ASCON is designed to support side-channel-resistant implementations more easily than many traditional algorithms. Devices that can benefit from its approach include RFID tags, implanted medical devices, and toll-registration transponders attached to car windshields.

ASCON-Hash 256 takes all the data it encrypts and uses it to create a short "hash" a few characters long, which functions like a fingerprint of the data. Even a small change to the original data results in an instantly recognizable change in the hash, making the algorithm useful for maintaining the data's integrity – such as during a software update, to ensure that no malware has crept in. Other uses are for protecting passwords and the digital signatures we use in online bank transfers. It is a lightweight alternative to NIST's SHA-3 family of hash algorithms, which are widely used for many of the same purposes.

ASCON-XOF 128 and ASCON-CXOF 128 are hash functions with a twist: Both algorithms allow the user to change the size of the hash. This option can benefit small devices because using shorter hashes allows the device to spend less time and energy on the encryption process.

The CXOF variant also adds the ability to attach a customized "label" a few characters long to the hash. If many small devices perform the same encryption operation, there is a small but significant chance that two of them could output the same hash, which would offer attackers a clue about how to defeat the encryption. Adding customized labels would allow users to sidestep this potential problem.

McKay said the NIST team intends the standard not only to be of immediate use, but also to be expandable to meet future needs.

"We've taken the community's feedback and tried to provide a standard that can be easily followed and implemented, but we are also trying to be forward-looking in terms of being able to build on it," she said. "There are additional functionalities people have requested that we might add down the road, such as a dedicated message authentication code. We plan to start considering these possibilities very soon."

14. Why the manufacturing industry needs to take action on post-quantum cryptography now

by Joppe W. Bos
https://www.themanufacturer.com/articles/op-ed-why-the-manufacturing-industry-needs-to-take-action-on-post-quantum-cryptography-now/

Smart manufacturing is flourishing. The market is expected to reach $998.99bn by the end of the decade, fueled by growing global populations and product innovations.

At the heart of this sector's success are new technologies powering the industrial internet of things (IIoT) – made up of a huge range of connected devices, from sensors to actuators, logic controllers to 3D printers – alongside advances in cloud computing, robotics, and AI. Together, these tools enable manufacturers to rapidly reconfigure factories based on market needs, bring products to launch faster, and develop more efficient, accurate, and sustainable manufacturing processes.

However, the skyrocketing number of connected devices in the smart manufacturing industry does raise a new challenge when it comes to security. Scalable cyberattacks present a significant concern as the industry evolves, posing monetary, reputational, environmental, and safety threats to manufacturers. In simple terms, as the number of smart devices grows across the manufacturing industry, so too does the potential attack surface.

Adding further complexity, manufacturers must now also prepare for the potential emergence of quantum computers which will see traditional cryptographic technologies made obsolete. Large-scale, fault-tolerant quantum computers may still be years away but the impact could upend security practices across the globe, with particular repercussions on highly-connected industries like manufacturing.

While it's urgent that manufacturers recognize and adequately respond to this emerging risk, the good news is that with the right approach, a more efficient, flexible, and resilient manufacturing sector is in reach.

How quantum computing impacts manufacturing security

Traditional cryptography protects the vast majority of devices today, including those that make up the IIoT. Most of this public-key cryptography is built upon complex algorithms (essentially mathematical problems) that are near-impossible for traditional computers to solve. Quantum computers, however, could theoretically make very short work of such mathematical challenges, thanks to using a different computing paradigm.

The threat of quantum computers to cryptography has long been theorized. In fact, Peter Shor famously proposed a quantum algorithm that, with a quantum computer with sufficient qubits of processing power, could break widespread public-key cryptography schemes back in 1994. Following Google's initial claim of reaching quantum supremacy in 2019 – the point at which a quantum computer can solve problems that are impossible on traditional computers – the risks quantum computers pose to cryptography have quickly moved beyond the theoretical.

In this rapidly changing context, what can manufacturers do to ensure devices, businesses, and the industry as a whole, are secure?

Staying a step ahead: Post-quantum cryptography

While the capabilities of quantum computers are rapidly growing, innovations in cryptographic techniques and IIoT devices – alongside rapidly evolving regulatory frameworks – are helping manufacturers to stay a step ahead of potential bad actors.

While there are issues with fragmentation of post-quantum cryptography (PQC) standards, with many different standards being trialed, put in place, or planned in different regions, the direction of travel is positive. Around the world, agencies such as the USA's NIST are producing algorithm families and guidance on different use cases with the ambition to keep businesses and consumers safe.

For many consumers, and some businesses, this transitional period is less pressing. That's because they'll have updated their devices by the time quantum threats become a reality. But for manufacturers, taking action now is much more urgent. The IoT technology that manufacturers choose today may have a decades-long lifecycle. Companies need to be able to invest today with the confidence their systems will remain both secure and compliant with changing regulations into the 2030s. With the lay of the land still in flux and PQC standards still changing, how will that be possible?

Ensuring cryptographic agility

For manufacturers, cryptographic agility is crucial. This means choosing systems from established and trusted manufacturers that can support multiple algorithms and which can be updated over time. This will make it simpler to adapt to the changing context around PQC. Given this, firmware updateability (something many IIoT devices have traditionally lacked) should be a crucial consideration today – as the alternative may be end-of-life replacement on a shorter timescale than desired.

For manufacturers with thousands of connected devices, this may all seem a daunting – and costly – task. And we should be clear-sighted about the challenges: there's no overnight fix.

Instead, the industry's migration will be gradual, starting with PQC being embedded in crucial use cases like secure boot, updates, TLS connections, and device attestation. Manufacturers will need to monitor changing regulations and work with suppliers to ensure compliance. Hybrid schemes that use both traditional and quantum-safe algorithms will also offer a stepping stone to greater protection (although it can be compute-intensive and so may not be suitable for all IIoT devices, many of which have limited resources).

Change takes time in the manufacturing industry. Today, PQC-readiness and agility are too often considered 'nice-to-haves' or even simply theoretical concerns, yet advances in quantum computing show no sign of slowing. This means that if manufacturers want to stay future-proof and safe, *now* is the time to start building PQC into their security strategy.

15. OPTIA and Patero Launch Post-Quantum-Enabled GPU Compute Platform for Defense and Edge Applications

by Matt Swayne
https://thequantuminsider.com/2025/08/12/optia-and-patero-launch-post-quantum-enabled-gpu-compute-platform-for-defense-and-edge-applications/

OPTIA, a provider of ruggedized, high-performance GPU compute platforms, and **Patero**, a pioneer in post-quantum cryptography, today announced a joint solution that embeds Patero's **CryptoQoR™** encryption suite into OPTIA's NVIDIA-based systems — delivering the **world's first PQC-enabled GPU server** for mission-critical defense and commercial applications.

Designed to support the compute-intensive needs of the U.S. Department of Defense (DoD) and built for deployment in tactical conditions, OPTIA's portable systems are widely used for AI/ML acceleration, tactical edge analytics, and C5ISR workloads. With the integration of Patero's quantum-safe cryptography, OPTIA devices can now protect inbound and outbound data streams against both present-day cyber threats and future quantum attacks.

"This is a first-of-its-kind platform — a tactical NVIDIA GPU server with quantum-resilient protection," said James Elder, BD Director of OPTIA, "A pre-integrated and packaged solution delivers high-performance compute without compromising data security, no matter the threat surface or operating environment."

Defense-Grade Security, Future-Ready Architecture

The combined offering aligns directly with:

- **Executive Order 14028** – Mandating zero-trust cybersecurity architecture for federal and defense systems.
- **National Security Memo 10** – Requiring federal agencies to begin transition to quantum-resistant cryptography.
- **Joint All-Domain Command and Control (JADC2)** initiatives – Demanding secure, interoperable compute at the edge.

"Whether it's battlefield intelligence, secure video feeds, or edge AI inference — when it leaves the OPTIA server, it leaves encrypted with Patero's PQC," said Peter Bentley, COO of Patero. "This isn't future capability — this is real, field-ready quantum security."

Key Features & Market Differentiators

- **1st PQC-Enabled NVIDIA GPU Server** for military, industrial, and public sector use
- **Rugged and Portable** supporting forward-deployable and austere environments
- **End-to-End Encrypted Streams** for AI/ML, ISR, logistics, and robotics workloads
- **Aligned with DoD, DHS, and NSA PQ migration guidance**

Joint Market Execution

OPTIA and Patero is co-developing a portfolio of secure bundles and form factors that jointly address expanding opportunities across:

- **Industrial AI** – Manufacturing, logistics, and autonomous platforms
- **Defense Programs** –C5ISR, AI/ML/LLM model deployment, and situational awareness
- **Secure Infrastructure** – Cities, Smart ports, airports, and energy sectors

16. Utilities, Factories at Risk from Encryption Holes in Industrial Protocol

by Alexander Culafi
https://www.darkreading.com/vulnerabilities-threats/utilities-factories-encryption-holes-industrial-protocol

Despite the promises of OPC UA, a standardized, open source communication protocol often used in industrial settings as a replacement for VPNs, turns out to have a number of vulnerabilities, issues, and potential for exploits.

Last week, Tom Tervoort, principal security specialist for Secura, hosted a session at DEF CON 33 dedicated to OPC UA (short for Open Platform Communications Unified Architecture), which was first introduced in 2006. The protocol includes its own cryptographic authentication and transport security layer, and is interoperable between different vendors.

"That makes it an interesting research target for me, especially because they're not relying on an existing standard protocol like TLS — they implemented their own cryptographic protocol," he said during the session. "I decided to take a look at how these security features work in order [to see if there were] any issues with it."

Tervoort spent time researching the protocol because its use in operational technology (OT) settings (both between OT networks as well as a bridge between OT and IT/cloud environments) makes it a highly attractive target for attackers. If a hacker compromises an OPC UA server, especially in an environment with no VPN, "they might be able to wreak havoc on whatever industrial systems are controlled by it," according to the research.

Probing OPC UA for Security Bugs

According to Tervoort, the cryptographic protocol design of OPC UA, which includes a number of handshakes and includes the use of private keys, session keys, encrypted messages, challenges, and user authentication. It also supports security policies like RSA and AES. In all, Tervoort described the cryptography implementation in the protocol as "redundant" and "not really great design, in my opinion."

Although, as he explained, it could be better to have three times as many cryptographic operations than none at all, and the structure could possibly provide some kind of defense-in-depth, this "expensive" cryptographic design is where the researcher found holes.

For example, Tervoort noticed that regardless of the message being signed from the server to the client or vice versa, they were formatted such that there was no metadata stating a message was specifically intended for a client or server. This enabled him to create a proof-of-concept (PoC) attack where a threat actor could sign one message in a particular context but then use it in a different context. The end result would enable the attacker to trick two different servers into logging in to each other, bypassing most authentication, by feeding each of them challenges generated by the other.

However, this attack requires bypassing the secure channel handshake, the first line of defense. To do so, Tervoort discovered that because of how some configurations of the protocol work, an attacker could set up an HTTPS connection in such a way that the protocol implicitly believes the communication is already encrypted and therefore doesn't require the handshake. The researcher wrote a tool that is capable of doing so automatically.

"You just point it at an HTTPS-based OPC UA server that uses HTTPS with this client authentication feature," he said, which is set up by default in some vendors' implementations. That said, HTTPS variants of the protocol are relatively new, and "almost nobody actually uses [it]," according to Tervoort. He also noted that the tool can't be used to bypass servers with user authentication,

Tervoort then went deeper, to try to attack the standard TCP version of the protocol. Problematically, he found that it supported the PKCS #1 encryption standard, which was broken in the late 1990s by Swiss cryptographer Daniel Bleichenbacher.

Although the standard was eventually deprecated and its use discouraged in OPC UA, some implementations and vendors still enable it by default, and some servers, even when weak ciphers were turned off, could still be exploited by sending an encrypted message using the protocol. The server would only realize it's not supposed to use the standard after decrypting it.

Patch Now: How to Secure OPC UA

Exploiting these issues depends on configuration and implementation details, but they still reflect protocol flaws. After he responsibly disclosed his findings, multiple vendors confirmed they were affected by the researcher's discoveries.

"I found [issues affecting] seven different products, but there are probably going to be many, many more that are affected," he said. Three CVEs representing some of his research have been disclosed: CVE-2024-42512, CVE-2024-42513, and CVE-2025-1468.

Thankfully, because all the vendors using the protocol are in contact with the OPC Foundation that administers the open source protocol, it assisted him with disclosing these issues to the relevant vendors and implementing fixes where possible: "My compliments to the OPC Foundation. That's not how responsible disclosure usually goes in my experience."

Fixes, the researcher said, range from software updates to disabling features to configuration advisories. In many, but not all, cases, disabling HTTPS and Basic128Rsa15 is sufficient. Non-certificate-based user authentication is also not affected. Ultimately, Tervoort advises users and organizations to check their vendor documentation.

As a result of the work, many vulnerabilities have become much more difficult to exploit, particularly if an organization has applied the relevant vendor patches. And although some affected vendors may still be out there, the fixes already done should, in theory, help address any similar problematic implementations that come to light in the future.

As for whether users should go back to VPNs, Tervoort said it depends on whether the organization can easily patch vulnerable servers or not. Even if they can and the organization still wants to go sans VPN, the researcher urged the use of IP allowlisting to allow only authorized connections, particularly if the server contains anything important.

17. Japan quietly built a quantum computer without importing a single part

by Atharva Gosavi
https://interestingengineering.com/innovation/japan-homegrown-quantum-computer

Japan recently launched its superconducting quantum computer built with homegrown components and software. The computer was launched at the University of Osaka's Center for Quantum Information and Quantum Biology (QIQB).

This achievement signifies Japan's technological prowess in quantum computing, demonstrating the nation's capacity to design, manufacture, and integrate a complete quantum system.

How do quantum computers work?

Quantum computers operate in a completely different manner compared to classical computers. They utilize quantum bits, also known as qubits, which use quantum effects like superposition and entanglement. This lets them solve problems that normal computers can't handle.

Quantum computers work in a completely different way from regular computers. Instead of using either 0 or 1 bits, they use qubits, thanks to quantum effects like superposition and entanglement. This lets them solve problems that normal computers can't handle.

Reducing dependencies

The Osaka quantum computer project comprises key components that were developed in Japan. Everything has been manufactured in the country, from the dilution refrigerator that cools the qubits to temperatures near 10 millikelvin to the pulse tube refrigerator that plays a major role in initial cooling stages.

With this step, Japan has reduced its dependence on imported equipment, embracing self-reliance in the process. The project represents a sophisticated amalgamation of engineering disciplines, encompassing cryogenics, microfabrication, electronic control systems, and error-correcting algorithms, all harmonized within an integrated quantum computing architecture.

A robust software ecosystem

Alongside the advanced hardware, there's also a powerful software system. Everything—from the user interface to the control systems—has been built as open-source tools, known as the Open Quantum Toolchain for Operators and Users (OQTOPUS).

This software makes programming, running, and monitoring the quantum computer easy, creating a user-friendly setup for researchers, developers, and enthusiasts. By keeping the software open-source and developed locally, the team in Osaka is promoting collaboration and ongoing improvements in quantum software.

Partners and exhibition

Distinguished institutions and industry leaders like RIKEN, ULVAC, Inc., ULVAC CRYOGENICS INC., e-trees.Japan, Inc., QuEL, Inc., QunaSys Inc., Systems Engineering Consultants Co., Ltd., TIS Inc., and Fujitsu Limited will be backing this project as partners. They have ensured technological self-reliance and created a vibrant ecosystem for quantum innovation within Japan.

The components of this quantum computer will be displayed at the Expo 2025 which will be held in Osaka, Japan, from 14th August to 20th August.

A promising future

Working with Professor Akihiro Kubota from Tama Art University, the exhibit will showcase art created by a quantum computer, blending science with creativity. This Expo aims to make quantum technology easier to understand and spark interest in the next generation of quantum innovators.

Quantum computers have the potential to resolve global challenges, ranging from new material development to optimization of complex systems for mitigating environmental impact.

18. Beyond PQC: Building adaptive security programs for the unknown

by Mirko Zorz
https://www.helpnetsecurity.com/2025/08/07/jordan-avnaim-entrust-pqc-trust/

In this Help Net Security interview, Jordan Avnaim, CISO at Entrust, discusses how to communicate the quantum computing threat to executive teams using a risk-based approach. He explains why post-quantum cryptography (PQC) is an urgent and long-term priority.

Avnaim also outlines practical steps CISOs can take to build crypto agility and maintain digital trust.

From your perspective as a CISO, how do you frame the quantum computing threat to executives and the board?

Complexity can be the enemy of communication in cybersecurity. One of the tools I use when communicating to the Board is the acronym 'KICS' – Keep It Cybersecurity Simple. This reminds you to avoid technical jargon and speak a language that the board understands, namely, the language of risk.

This approach is crucial when framing the quantum threat. In an already highly technical space, speaking the language of post-quantum cryptography to a non-technical board member could lead to a breakdown in communication. Instead, frame the threat as something where we do not have a countdown clock: unlike previous technological advancements and threats, we can only guess at when a scaled quantum computer will arrive. Even the much-feared 'Y2K' had a fixed deadline. 'Y2Q', on the other hand, will arrive one day with no forewarning.

When it does, and if we are unprepared for it, there will be an immediate and overpowering vulnerability for all sensitive information, and this will change everything. This approach speaks directly to the board's language of risk and positions the conversation around what you, as a technical leader, can do to defend against this threat.

Do you see post-quantum cryptography as primarily a long-term risk or a near-term operational challenge?

The lack of a timeline for a post-quantum world means that it doesn't make sense to consider post-quantum as either a long-term or a short-term risk, but both. Practically, we can prepare for the threat of quantum technology today by deploying post-quantum cryptography to protect identities and sensitive data. This year is crucial for post-quantum preparedness, as organisations are starting to put quantum-safe infrastructure in place, and regulatory bodies are beginning to address the importance of post-quantum cryptography.

Establishing post-quantum cryptography in your organization is not just important in safeguarding against an early arrival of quantum technology; it also protects organisations against a particularly malicious threat: 'harvest now, decrypt later'. This is where bad actors, either criminals or those acting on behalf of a nation-state, will steal encrypted information today to decrypt it later when quantum computers are available. This means some organisations could have suffered a significant cyber breach, and they don't even know it yet. Implementing quantum-safe cryptography is the key to preventing this.

As we continue to think in the future, beyond the post-quantum challenges of today, we must recognise there will be new and unprecedented challenges we will face. Undoubtedly, in the post-post-quantum era, there will be threats to post-quantum cryptography that we must anticipate. While implementing the shorter-term solution of post-quantum cryptography solutions to secure enterprise secrets is a necessity, the best organizations will use today's PQC challenges as an opportunity to build agile, adaptive, and responsive organizational security programs that can pivot as necessary to address threats to the enterprise with agility and precision.

What does a realistic post-quantum roadmap look like for CISOs in 2025?

CISOs should take steps now to understand their current cryptographic estate. Many organisations have developed a fragmented cryptographic estate without a unified approach to protecting and managing keys, certificates, and protocols. This lack of visibility opens increased exposure to cybersecurity threats. Understanding this landscape is a prerequisite for migrating safely to post-quantum cryptography.

Another practical step you can take is to prepare your organisation for the impact of quantum computing on public key encryption. This has become more feasible with NIST's release of quantum-resistant algorithms and the NCSC's recently announced three-step plan for moving to quantum-safe encryption.

Even if there is no pressing threat to your business, implementing a crypto-agile strategy will also ensure a smooth transition to quantum-resistant algorithms when they become mainstream. By understanding and implementing quantum-safe cryptography where appropriate, organisations can stay ahead of regulatory requirements and technological advancements, ensuring long-term security in an evolving landscape.

How can CISOs build "crypto agility" into procurement and architecture without overhauling everything?

To enable crypto agility, it requires both a bottoms up and top down approach to be successful. That is, we must select and use products and vendors that have the ability to conform to our desired/selected internal crypto standards, and also provide the internal crypto plumbing (secrets management, PKI, etc) to enable those solutions we procure.

Do you foresee PQC adoption driving wider changes in how CISOs think about digital trust and resilience?

Simply put: The quantum computing threat puts common day digital trust and cyber resilience methods in jeopardy. Adopting PQC is the only way we can ensure we maintain digital trust and resilience in an environment where today's cryptography is broken in seconds. Without strong PQ resistant crypto algorithms, there is no digital trust or resilience.

19. Post-Quantum Cryptography Implementation Considerations in TLS

by Jan Schaumann
https://www.akamai.com/blog/security/post-quantum-cryptography-implementation-considerations-tls

On June 30, 2025, Akamai rolled out support for post-quantum cryptography (PQC) in Ghost to Origin (G2O) connections using Transport Layer Security (TLS) version 1.3. This new feature is currently in limited availability, and early adopters can enable it to protect connections between Akamai and origin servers against the "harvest now, decrypt later" (HNDL) threat.

We are planning to enable this feature on all origin TLS connections with our upcoming general availability release on October 31, 2025. In preparation for that release, let's take a closer look at the implementation.

Our objective is to assist customers in their preparedness and enablement by sharing what considerations come into play as we embark together on this journey to a quantum-secure future.

Libraries and tools

To deploy PQC that interoperates – on the client side or the server side – you'll need a TLS library or framework that supports the latest TLS 1.3 hybrid key exchange using a post-quantum traditional hybrid scheme.

Since common cryptographic libraries like OpenSSL have only recently received support for the newly standardized post-quantum algorithms, Akamai not only developed our own PQC provider, but at the same time invested in platform-wide upgrades, yielding an overall more crypto-agile state.

The resulting flexibility is essential for adopting PQC and defending against the HNDL active threat. Likewise, you will need to assess your infrastructure to identify necessary library updates.

In this blog post we'll share some common implementation challenges for TLS 1.3 hybrid key exchange adoption, using the latest OpenSSL and BoringSSL libraries as examples, to help you prepare for a quantum-secure future.

TLS 1.3 hybrid key exchange

In our previous blog post in this series, we shared:

- How the National Institute of Standards and Technology (NIST) standardized the new post-quantum Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)
- How the Internet Engineering Task Force (IETF) laid the groundwork for adoption in TLS 1.3
- How the IETF adopted a draft specifying hybrid ECDHE-MLKEM key agreement, primarily using the X25519MLKEM768 group

But what does a hybrid key exchange actually look like, and how does it impact client and server behavior? As you adopt PQC, it's important to understand the difference in its behavior, both compared with the classic handshake as well as between client and server.

Sample environment

To observe the TLS packets on the wire, we need an HTTP server that supports PQC. We've already published a simple guide explaining how to set up PQC using nginx on an Ubuntu Linode, which you can reference for exactly that purpose.

Following that guide to configure an example site (https://pqc.example.com), we can then explore the TLS handshake using tcpdump and the openssl s_client command:

```
$ sudo tcpdump -w pqc.pcap host pqc.example.com >/dev/null 2>
$ </dev/null openssl s_client -tls1_2 -connect pqc.example.com:443
[...]
$ </dev/null openssl s_client -connect pqc.example.com:443
[...]
```

Since we are focused only on the TLS handshake here, we don't need to make an actual HTTP request. Having made two successive connections – the first using TLS 1.2 and the second using the default TLS 1.3 – we can now inspect the captured packets for differences in the key exchange.

Key exchange differences in TLS 1.2 vs. TLS 1.3

In a traditional TLS 1.2 handshake, as in the first openssl invocation, the client indicates all supported cipher suites in the TLS ClientHello – including the key exchange algorithms to be used for each cipher suite.

For example, the cipher suite ECDHE-ECDSA-AES256-GCM-SHA384 specifies the use of Elliptic Curve Diffie–Hellman (ECDH) for the key exchange. On the other hand, for example, DHE-RSA-AES256-GCM-SHA384 specifies the use of the original (Finite Field) Diffie–Hellman. The supported_groups extension advertises the appropriate key groups, but only sends the suitable public key in the subsequent Client Key Exchange message (Figure 1).

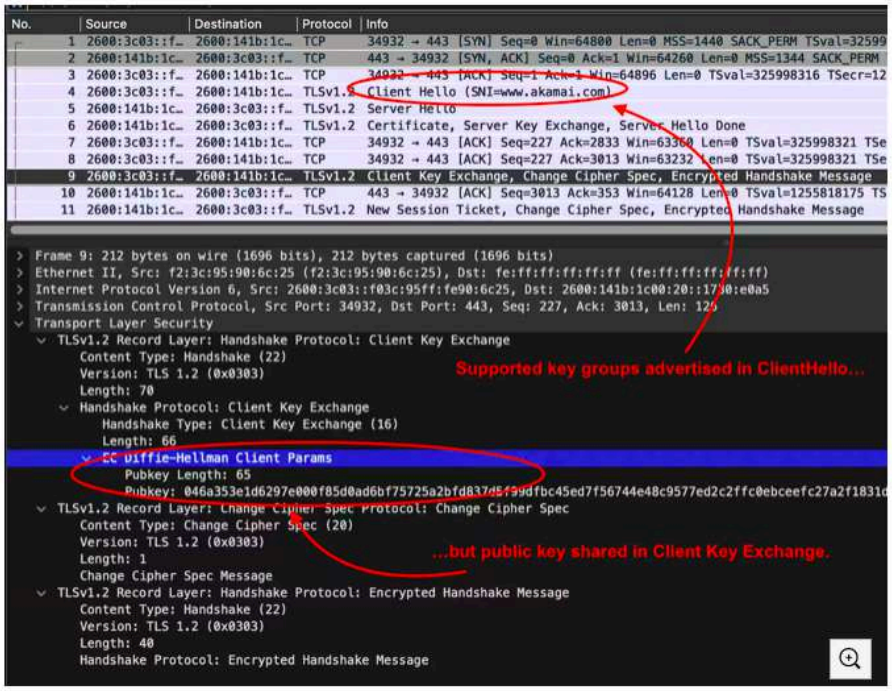
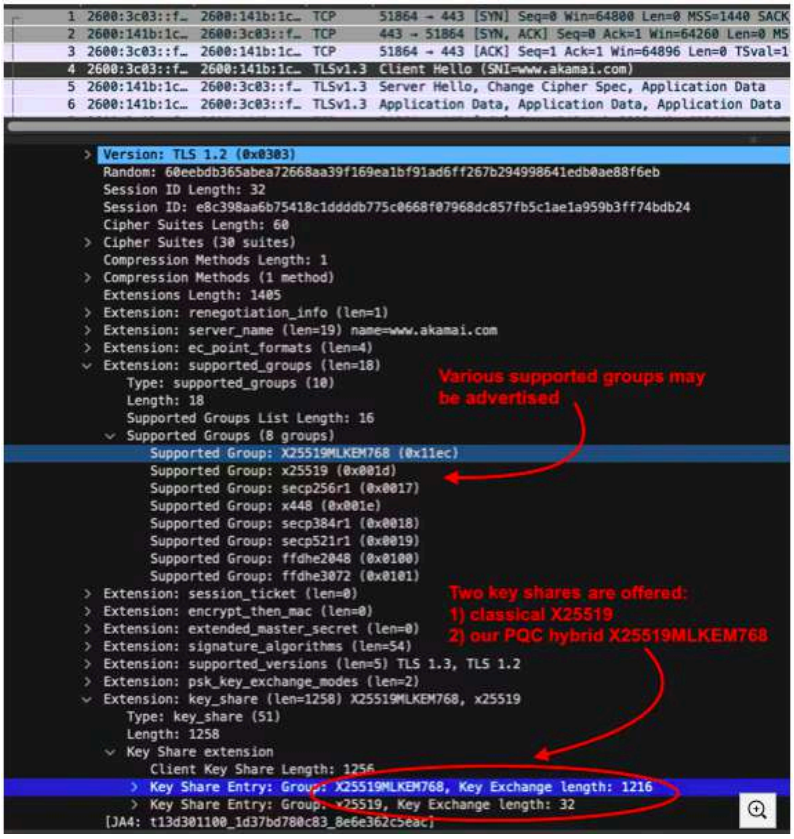


Fig. 1: This Wireshark screenshot shows the details of the Client Key Exchange packets of a TLS 1.2 handshake, highlighting the public key provided by the client

By contrast, in a TLS 1.3 handshake, the key exchange algorithm selection is separated from the authentication algorithms in the cipher suites. The client provides the public key right in the ClientHello as part of the key_hare extension (Figure 2).



TLS ClientHello compatibility

In the packet analysis above, we see that the client supports PQC using X25519MLKEM768and includes *both* a standalone X25519 key and a hybrid key – the latter consisting of the concatenation of a *separate* X25519 public key and the ML-KEM public key. (You can read a more detailed discussion of the hybrid key exchange on my personal blog.)

This combination of keys leads to an increase of bytes in the ClientHello compared with legacy algorithms (Table).

Algorithm	Public key (bytes)
X25519	32
RSA-2048	256
ML-KEM768	1,184
X25519MLKEM768	1,216

This increase in size brings up its own set of challenges. Under certain circumstances, it can cause faulty server implementations to reject the ClientHello. Additionally, generating and sending this larger hybrid key in every ClientHello wastes CPU use and bandwidth if the remote server does not even support PQC.

One option to avoid these inefficiencies is for the client to *advertise* both key groups, but only *include* one key share in the ClientHello. For example, imagine that the client advertises both X25519 and X25519MLKEM768, but only offers the X25519 key share. If the server doesn't speak PQC, it will simply use the offered X25519 key to establish the connection. Otherwise, it would have to initiate a HelloRetryRequest to select X25519MLKEM768, incurring an additional round trip.

Alternatively, if the client offered only the hybrid key share, couldn't a server without support for PQC extract the X25519 component and use that for the classical key exchange? While that may seem like a plausible solution, it would violate cryptographic principles of only ever using a given primitive in the intended context. A server that supports only classic key exchange talking to a client that offers only the hybrid key share would therefore have to trigger a HelloRetryRequest to request the standalone X25519 key from the client.

You can compare both options side-by-side in Figure 3 and Figure 4.

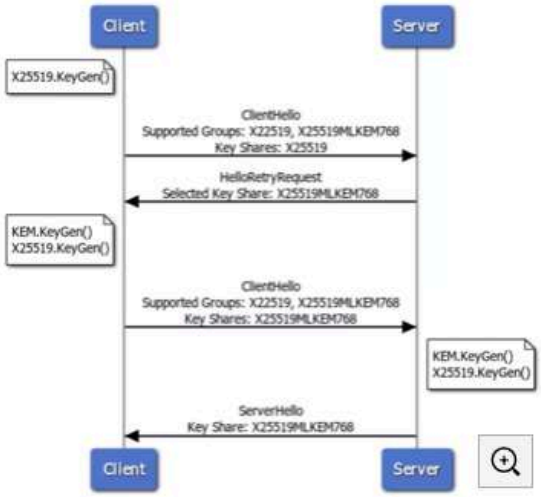


Fig. 3: Client-server communication requiring a HelloRetryRequest to use X25519MLKEM768 after the client only included the X25519 key share

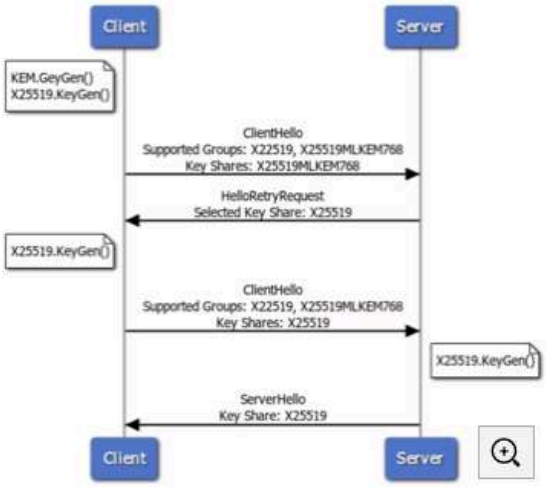


Fig. 4: Client-server communication requiring a HelloRetryRequest to use X25519 after the client only included the X25519MLKEM768 key share

To mitigate these problems, clients must determine the right approach as a trade-off between increased ClientHello size and incurring additional round trips via a HelloRetryRequest. Common clients, such as browsers, favor shorter connection times at the cost of a larger ClientHello, but this may not be the best approach for your application.

For example, if you use long-lived persistent connections but expect few servers to actually support PQC, you may want to only offer the single classic key, but support the hybrid key group if the server initiates a HelloRetryRequest. This will be Akamai's long-term approach for G2O connections for customers who don't explicitly signal PQC support.

Alternatively, if you know the server you're talking to supports PQC, you can immediately and only offer X25519MLKEM768 in the ClientHello. This is Akamai's approach during our limited availability phase, and once PQC support becomes generally available, it will be our approach for customers who explicitly signal PQC support.

While you can simulate these scenarios easily enough using the openssl s_clientcommand, you'll want to carefully read your TLS library's manual page to understand how group preference is specified. For example, OpenSSL's SSL_CTX_set1_curves(3) offers a somewhat unintuitive definition, whereby specifying X25519:X25519MLKEM768 leads to the client only *including* the X25519 key (but *advertising* both), while X25519:*X25519MLKEM768 (note the asterisk) only includes the PQC hybrid key. To include both, you'd have to use *X25519:*X25519MLKEM768.

In BoringSSL, on the other hand, all keys specified in the -curves option are included in the ClientHello. That is, the command-line client does not support advertising multiple key groups but only including a single key share.

To observe the difference, run the following commands:

```
$ sudo tcpdump -w pqc.pcap host pqc.example.com >/dev/null 2>&
$ </dev/null openssl s_client -groups "X25519:X25519MLKEM768"    \
      -connect pqc.example.com:443
$ </dev/null openssl s_client -groups "X25519:*X25519MLKEM768"   \
      -connect pqc.example.com:443
$ </dev/null openssl s_client -groups "*X25519:*X25519MLKEM768" \
      -connect pqc.example.com:443
$ </dev/null bssl client -curves "X25519:X25519MLKEM768"         \
      -connect pqc.example.com:443
```

In the resulting packet capture, you should find a HelloRetryRequest triggered during the first connection, while subsequent connections include the X25519MLKEM768 immediately in the ClientHello. The last two connections will include both key groups.

For a server, the behavior is different once again. Since a server responds to the client and does not need to send any key shares opportunistically, specifying key groups may instead signal its list of preference order to avoid round trips.

As this suggests, a client or server that's uniquely configured for your specific environment may have different priorities and compatibility models than general purpose clients (such as browsers) or servers (such as a CDN edge server).

Verifying the key exchange

With so many configuration options and software/library combinations, you'll want to be able to easily identify whether a given connection uses the hybrid key exchange.

Validating a client

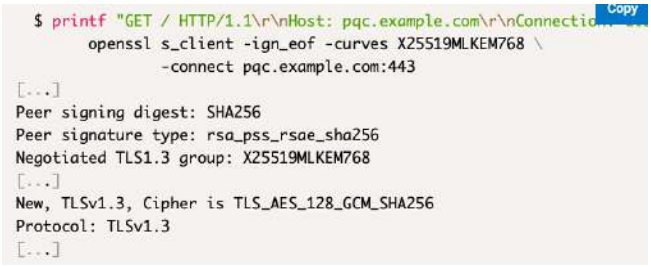
To validate that a client connecting to your server uses the X25519MLKEM768 hybrid key exchange, your server may be able to extract, log, and reflect the key exchange algorithm used. This varies from server to server and further depends on the specific TLS library.

For example, in nginx, you can expose the $ssl_curve parameter to a FastCGI script. For an OpenSSL- or BoringSSL-based server, you might use the SSL_get_negotiated_group(3) function. In some languages, such as Python or Go, however, this information is not always readily available.

Validating a server

The easiest way to verify whether a given server supports PQC is to attempt to make a connection using *only* X25519MLKEM768. This requires a client that supports specifying the key exchange mechanism – for example, via the openssl s_client commands shown above.

In the verbose output, you should see the Negotiated TLS 1.3 Group:



Similarly, the ubiquitous curl command lets you specify which key exchange mechanisms to use via the --curves option, although details of the behavior vary depending on which TLS library curl was built against.

Of course, the easiest way to verify your PQC connectivity may just be to use a browser. As of August 2025, both Firefox and Chrome support, enable, and offer X25519MLKEM768 by default. While Safari does not yet support PQC, Apple recently announced that macOS Tahoe 26 and iOS 26 (expected to be released in fall 2025) will do so.

Moving toward a quantum-secure future

Clearly, there's much to consider as you implement PQC using the new TLS 1.3 hybrid key exchange on client and server applications.

Although you may be able to offload some of these challenges to third-party providers, it's still important to be able to verify and test the new PQC capabilities in your respective environment. The examples we've shared in this post should help protect your and your users' data from current and emerging quantum threats. Akamai is here to support you in onboarding and enabling G2O PQC and help you embark on the journey to a quantum-secure future.

20. VDURA and NMSU Partner to Develop Post-Quantum Cryptography for AI & HPC Data Infrastructure

by Greg Bock
https://thequantuminsider.com/2025/08/05/vdura-and-nmsu-partner-to-develop-post-quantum-cryptography-for-ai-hpc-data-infrastructure/

Quantum computing promises transformative breakthroughs in artificial intelligence and high-performance computing, but it also threatens today's encryption. To stay ahead of that curve, **VDURA** has announced a strategic partnership with **New Mexico State University (NMSU)** to co-develop and commercialize post-quantum cryptographic (PQC) technology that safeguards the petabyte-scale data pipelines powering next-generation AI and HPC workloads.

"AI training sets, model checkpoints, and real-time HPC simulations generate an unprecedented flow of critical data," said Ken Claffey, CEO of VDURA. "Our mission has always been to deliver the most reliable, performance-dense data platform in the industry. By embedding quantum-resilient encryption into VDURA's flash-optimized architecture, we're future-proofing that mission for the AI era."

NMSU, recently elevated to Carnegie R1 status, brings world-class cryptography and cybersecurity research to the collaboration. Together, the teams will integrate NIST-selected PQC algorithms into VDURA's parallel file-system stack, enabling line-rate encryption of GPU-accelerated workloads without sacrificing performance.

"We're excited to work with VDURA to translate our academic innovations into deployable solutions," said Dr. Jay Misra, Associate Dean for Research in the College of Engineering. "This is an excellent example of how research at R1 universities can shape and secure the technological future."

"Industry partnerships are essential to expanding and diversifying NMSU's research portfolio. The VDURA initiative is a high-impact, translational collaboration that positions NMSU as an emerging national leader in cybersecurity," added Dr. Luis Cifuentes, Vice President for Research.

With this alliance, VDURA and NMSU are setting a new benchmark for secure, high-performance data infrastructure—protecting the information that powers discovery today and the quantum-driven breakthroughs of tomorrow.

21. Performance Tests Evaluate Viability of CRYSTALS-Kyber Post-Quantum Cryptography

by Quantum News
https://quantumzeitgeist.com/performance-tests-evaluate-viability-of-crystals-kyber-post-quantum-cryptography/

The looming threat of quantum computers capable of breaking current encryption standards drives urgent research into new cryptographic methods, and Nicolas Rodriguez Alvarez from IES Parquesol and Fernando Rodriguez Merino from the University of Valladolid, along with their colleagues, have investigated the practical performance of one leading solution, CRYSTALS-Kyber. As advances in quantum error correction push the possibility of large-scale quantum computers closer to reality, the cryptographic community must proactively transition to algorithms resistant to these attacks. This study assesses Kyber's viability as a replacement for widely used RSA and ECC encryption, focusing on its performance using standard processor features commonly found in everyday computers. The results demonstrate that Kyber offers strong security without requiring specialised hardware, suggesting it is a feasible option for widespread adoption and mitigating the risks of prolonged vulnerability during the transition to post-quantum cryptography.

Kyber Outperforms ECC and RSA Encryption

This research presents a performance comparison of three cryptographic algorithms, SECP384R1 (Elliptic Curve), Kyber, and RSA, assessing their suitability for securing future communications against the threat of quantum computers. The study demonstrates that Kyber offers significant performance advantages over both SECP384R1 and RSA, particularly in key generation and establishing secure connections, while maintaining acceptable storage requirements. These findings suggest Kyber is a strong candidate for protecting communications in a future where quantum computers could compromise current encryption standards. Kyber consistently outperforms both SECP384R1 and RSA across all tested operations.

In key generation, Kyber is 2. 7 to 3 times faster than ECC and a remarkable 3400 to 20500 times faster than RSA. For establishing shared secrets, Kyber is 41 to 72 times faster than ECC and 1600 to 3200 times faster than RSA. This consistent performance advantage holds true across both x86-64 and ARM64 computer architectures, with ARM64 partially reducing the overhead of traditional schemes but not changing the fundamental performance rankings. Kyber does require slightly more storage space for its data, representing a trade-off for its performance gains.

Kyber Performance on Standard Computer Architectures

Researchers evaluated Kyber's practical viability as a potential replacement for current encryption standards vulnerable to quantum computing attacks. Rather than relying on specialized hardware, the study deliberately used only standard processor acceleration features found in commercially available computers, ensuring the results reflect real-world deployment scenarios and avoiding the costs of bespoke hardware. This approach provides a realistic benchmark for organizations considering adopting post-quantum cryptography. The core of the methodology involved comprehensive performance testing of Kyber across both x86_64 and ARM64 architectures and various implementation scenarios.

To establish meaningful comparisons, Kyber's performance was directly contrasted with that of established cryptographic algorithms, RSA-7680 and SECP384R1, offering equivalent security levels. This comparative analysis clarifies the trade-offs between Kyber and existing standards in terms of speed and efficiency. A key innovative aspect of the study lies in its focus on leveraging existing hardware acceleration capabilities. Researchers utilized features such as Intel's AES-NI and AVX2 instruction sets, alongside ARM's AES and ASIMD extensions, to optimize Kyber's performance. These features, designed to accelerate cryptographic operations, were employed without any modifications or custom implementations, demonstrating that Kyber can benefit from readily available hardware without requiring specialized development. This emphasis on commodity hardware is crucial for facilitating widespread adoption.

Kyber Demonstrates Practical Post-Quantum Cryptographic Security

The increasing power of computers necessitates a continuous evolution of cryptographic methods, particularly with the looming threat of quantum computers capable of breaking widely used encryption standards. Researchers have been actively developing post-quantum cryptography, designed to withstand attacks from both classical and future quantum computers, and recent performance evaluations of a leading candidate, CRYSTALS-Kyber, demonstrate promising results. This study rigorously tested Kyber's practical viability across common computing architectures, revealing significant advantages over existing methods.

Kyber's security relies on the mathematical difficulty of solving problems based on lattices, a fundamentally different approach than traditional cryptography like RSA and Elliptic Curve Cryptography (ECC).

While RSA relies on the computationally intensive task of factoring large numbers, and ECC on solving elliptic curve discrete logarithm problems, Kyber leverages the presumed hardness of lattice-based problems, offering a robust defense against both current and anticipated quantum attacks. The testing involved detailed performance benchmarks on both x86_64 (commonly found in servers and desktops) and ARM64 (prevalent in mobile devices and embedded systems) architectures, utilizing standard processor acceleration features like AES-NI and ASIMD without specialized hardware. The results demonstrate Kyber's exceptional efficiency, particularly in key generation. Across both architectures, Kyber required significantly fewer CPU cycles to generate a key pair compared to both RSA and ECC.

Specifically, Kyber was approximately 2. 7 to 3 times faster than ECC and a staggering 20,500 times faster than RSA on x86_64 systems. Even on the more constrained ARM64 architecture, Kyber remained over 3,400 times faster than RSA. This dramatic improvement stems from the inherent mathematical properties of lattice-based cryptography, which allows for much more efficient key creation processes. The performance benefits extend to the derivation of shared secrets, essential for secure communication.

Kyber consistently outperformed both RSA and ECC in this critical operation, requiring fewer CPU cycles to establish a secure connection. This efficiency is crucial for applications ranging from secure web browsing to encrypted messaging, ensuring minimal performance overhead for users. These findings suggest that CRYSTALS-Kyber represents a viable and efficient solution for securing digital communications in the post-quantum era. Its superior performance, coupled with its robust security guarantees, positions it as a leading candidate for the next generation of cryptographic standards, offering a pathway to maintain secure communications in an increasingly complex and computationally powerful world.

Kyber Outperforms RSA and ECC Significantly

Benchmarking results demonstrate that CRYSTALS-Kyber, a leading post-quantum cryptographic solution, offers decisive computational advantages over traditional schemes like RSA and ECC across both x86_64 and ARM64 computer architectures. Kyber leverages modern CPU features, particularly vectorization instructions, to accelerate core computations, achieving key generation speeds 2. 7 to 3 times faster than ECC and an impressive 3,400 to 20,500 times faster than RSA. Similar speed advantages, ranging from 41 to 72 times faster than ECC and 1,600 to 3,200 times faster than RSA, extend to shared secret derivation, effectively resolving a critical performance bottleneck in receiver-side operations. These gains are consistently observed across different processor types, with ARM64 partially mitigating the overheads of classical cryptography without altering the overall performance hierarchy. While Kyber requires slightly more storage space for its data compared to RSA and ECC, this trade-off is justified by the substantial performance improvements.

22. Fujitsu Starts Development of 10,000-Plus Qubit Superconducting Quantum Computer, Completion Expected in 2030

by Matt Swayne

https://thequantuminsider.com/2025/08/01/fujitsu-starts-development-of-10000-plus-qubit-superconducting-quantum-computer-completion-expected-in-2030/

Fujitsu today announced that it has started research and development towards a superconducting quantum computer with a capacity exceeding 10,000 qubits. Construction is slated for completion in fiscal 2030.

The new superconducting quantum computer will operate with 250 logical qubits and will utilize Fujitsu's innovative "STAR architecture," an early-stage fault-tolerant quantum computing (early-FTQC) architecture also developed by the company. Fujitsu aims to make practical quantum computing possible, particularly in areas like materials science where complex simulations can unlock groundbreaking discoveries, and to this end will focus on advancing key scaling technologies across various technical domains.

As part of this effort, Fujitsu has been selected as an implementing party for the "Research and Development Project of the Enhanced Infrastructures for Post-5G Information and Communication Systems", publicly solicited by the NEDO (New Energy and Industrial Technology Development Organization). Fujitsu will be contributing to the thematic area of advancing the development of quantum computers towards industrialization. The project will be promoted through joint research with Japan's National Institute of Advanced Industrial Science and Technology (AIST) and RIKEN, and will run until fiscal year 2027.

Fujitsu is committed to driving forward the development of practical and industrialized quantum computing solutions. After this 10,000-qubit machine is built, Fujitsu will further pursue advanced research initiatives targeting the integration of superconducting and diamond spin-based qubits from fiscal 2030 and aims to realize a 1,000 logical qubit machine in fiscal 2035 while considering the possibility of multiple interconnected quantum bit-chips.

Vivek Mahajan, Corporate Executive Officer, Corporate Vice President, CTO, in charge of System Platform, Fujitsu Limited, comments: "Fujitsu is already recognized as a world leader in quantum computing across a broad spectrum, from software to hardware. This project, led by NEDO, will contribute significantly to Fujitsu's goal of further developing a Made-in-Japan fault tolerant superconducting quantum computer. We would also be aiming to combine superconducting quantum computing with diamond spin technology as part of our roadmap. By realizing 250 logical qubits in fiscal 2030 and 1,000 logical qubits in fiscal 2035, Fujitsu is committed to leading the path forward globally in the field of quantum computing. Additionally, Fujitsu will be developing the next generation of its HPC platform, using its FUJITSU-MONAKA processor line, which will also power FugakuNEXT. Fujitsu will further integrate its platforms for high-performance and quantum computing to offer a comprehensive computing platform to our customers."

Technology development focus areas

Fujitsu's research efforts will focus on developing the following scaling technologies.

- **High-throughput, high-precision qubit manufacturing technology:** Improvement of the manufacturing precision of Josephson Junctions, critical components of superconducting qubits which minimize frequency variations.

- **Chip-to-chip interconnect technology:** Development of wiring and packaging technologies to enable the interconnection of multiple qubit chips, facilitating the creation of larger quantum processors.
- **High-density packaging and low-cost qubit control:** Addressing the challenges associated with cryogenic cooling and control systems, including the development of techniques to reduce component count and heat dissipation.
- **Decoding technology for quantum error correction:** Development of algorithms and system designs for decoding measurement data and correcting errors in quantum computations.

Background

The world faces increasingly complex challenges that demand computational power beyond the reach of traditional computers. Quantum computers offer the promise of tackling these previously intractable problems, driving significant advancements across numerous fields. While a fully fault-tolerant quantum computer with 1 million qubits of processing power is considered the ultimate goal, Fujitsu is focused on delivering practical solutions in the near term.

Fujitsu's commitment to quantum computing is underscored by its ongoing R&D efforts. In August 2024, in collaboration with the University of Osaka, Fujitsu unveiled its STAR architecture, a highly efficient quantum computing architecture based on phase rotation gates. This architecture paves the way for early-FTQC systems capable of outperforming conventional computers with only 60,000 qubits[1]. On the hardware front, the RIKEN RQC-Fujitsu Collaboration Center, established in 2021 with RIKEN, has already yielded a 64-qubit superconducting quantum computer in October 2023, followed by a world-leading 256-qubit system in April 2025[2].

Scaling to even larger systems requires overcoming challenges such as maintaining high fidelity across multiple interconnected qubit chips and achieving greater integration of components and wiring within dilution refrigerators. In addition to its superconducting approach, Fujitsu is also exploring the potential of diamond spin-based qubits, which use light for qubit connectivity. Fujitsu is conducting research in this area in collaboration with Delft University of Technology and QuTech, a leading quantum technology research institute, which has resulted in the successful creation of highly accurate and controllable qubits.

23. Microsoft CEO Sees Quantum as `Next Big Accelerator in Cloud', Ramps up AI Deployment

by Matt Swayne
https://thequantuminsider.com/2025/07/31/microsoft-ceo-sees-quantum-as-next-big-accelerator-in-cloud-ramps-up-ai-deployment/

Microsoft CEO Satya Nadella said quantum computing will be the next major accelerator in cloud technology, marking a notable shift in the company's long-term strategic focus. The statement, made during the company's fiscal year 2025 fourth-quarter earnings call and posted on Investor.com, signaled

[1] In simulations using 60,000 qubits, the STAR architecture can execute material energy estimation calculations which would take 5 years on conventional computers in about 10 hours.

[2] One of the world's largest superconducting quantum computers available to external users (as of April 2025, according to Fujitsu).

Microsoft's intent to expand beyond traditional cloud and AI infrastructure and invest in technologies with longer time horizons.

"The next big accelerator in the cloud will be quantum and I'm excited about our progress," said Nadella

The remarks came alongside better-than-expected financial results. Microsoft reported $76.4 billion in quarterly revenue, a year-over-year increase of more than 18%. Earnings per share rose to $3.65, beating Wall Street estimates of $3.37. Cloud services, particularly Azure, drove much of the growth, with Azure's annual revenue rising to $75 billion, up 34%, according to the earnings statement.

Quantum Moves into Deployment Phase

Microsoft's commitment to quantum is moving beyond the lab and onto the balance sheet. Earlier in July, the company said it had achieved the first operational deployment of what it described as a "Level 2" quantum computer, in partnership with Atom Computing. A Level 2 quantum computer is often used when describing a quantum system that implements quantum error correction and can preserve logical qubits over time. While details remain limited, this move positions Microsoft as one of the few firms to claim a functional quantum system accessible through commercial infrastructure.

For now, as seen in the earnings report, quantum computing is not contributing meaningful revenue. But Microsoft is positioning it as the next platform wave, one that will reshape infrastructure and workloads. The deployment of the Atom-Microsoft system suggests the company intends to lead in this space, not just participate.

In Nadella's view, quantum should closely follow the same trajectory as past accelerators, such as GPUs and AI models, becoming deeply embedded into Microsoft's growing data center footprint. As Nadella framed it, Microsoft's approach to innovation spans "decade-long arcs," with milestones delivered quarter by quarter.

In fact, in recent quarters, Microsoft appears to be taking direct action to prepare for quantum's contribution to the company's bottom line. Every Azure region is now equipped to support liquid cooling, a necessary feature for advanced computing including quantum. The company has expanded to over 400 data centers in 70 regions globally, and added more than two gigawatts of new computing capacity in the past 12 months – a scale that should accommodate both classical and emerging quantum workloads.

Cloud and AI Workloads Expand

While quantum remains an early-stage bet, AI continues to dominate Microsoft's near-term roadmap and earnings. Azure revenue growth, which includes AI services, reached 37% in constant currency and is expected to maintain that pace in Q1 2026.

Microsoft's AI infrastructure now supports over 500 trillion tokens served annually through its Foundry APIs, a sevenfold increase from the previous year. Foundry enables customers to run AI applications across models from Microsoft, OpenAI, Meta, and others, including emerging players such as Mistral AI. The company said Foundry now supports 14,000 customers, including firms like NASDAQ, which use AI agents to automate tasks such as board meeting preparation.

The company also expanded its Microsoft Fabric platform — a data and analytics engine that integrates SQL, NoSQL, and semantic models — reporting 55% revenue growth and over 25,000 customers. Fabric plays a central role in grounding AI systems with relevant context, a critical requirement for enterprise adoption.

AI Drives Product Adoption

On the application layer, Microsoft's suite of AI-enabled products continues to grow rapidly. Its family of "Copilot" apps now serves over 100 million monthly users, with more than 800 million people using some AI features across Microsoft products. Microsoft 365 Copilot, the AI assistant for Office applications, posted its largest quarter of new seat sales, with customers such as Barclays and UBS committing to company-wide rollouts.

GitHub Copilot, Microsoft's AI assistant for developers, now has 20 million users. Usage increased 75% quarter-over-quarter among enterprise customers. Microsoft said GitHub Copilot has moved from simple code completion to operating in full "agent mode," with asynchronous capabilities that automate development tasks without constant user input.

The momentum extends to specialized markets. In healthcare, Microsoft's ambient AI system recorded over 13 million physician-patient interactions this quarter, helping reduce documentation workloads. In security, Microsoft Defender now protects nearly two million generative AI applications.

Monetization Strategy Reflects AI Complexity

During the Q&A portion of the call, analysts pressed Microsoft leadership on how it plans to monetize the surge in AI use, particularly for SaaS applications like Microsoft 365 and Dynamics 365. Nadella and CFO Amy Hood said they expect a mix of per-user pricing and consumption-based models to evolve, depending on the complexity and frequency of AI interactions.

Microsoft executives emphasized that AI tools are becoming deeply embedded in workstreams and applications, no longer just add-ons. Nadella cited GitHub Copilot as a model, noting that its evolution from basic code suggestions to full-fledged agents points to broader adoption patterns across all business software.

AI workloads are also reshaping Microsoft's infrastructure. Hood reported that Microsoft Cloud gross margins declined slightly to 68%, driven by the costs of scaling AI systems. Yet operating income for the quarter still grew 17% year-over-year, thanks to demand in cloud services and tight control on expenses.

Market Response and Forward Guidance

Investors responded favorably to the results. Microsoft shares rose 0.29% during regular trading and gained another 0.47% after hours, pushing the stock to $515, closing in on its 52-week high. The company now holds a market capitalization of close to $4 trillion.

Looking ahead, Microsoft expects double-digit growth in revenue and operating income for fiscal 2026. The company projects continued Azure strength and estimates Q1 Azure revenue growth of 37%. Capital

expenditures will moderate slightly, though Microsoft still expects to spend over $30 billion next quarter, with more than half of that directed toward long-lived infrastructure.

Executives warned that AI infrastructure demand is likely to outpace supply through at least the first half of fiscal 2026. But they expressed confidence in the company's ability to scale — and to define the architecture of a new era of computing shaped by AI and quantum technologies.

24. Karnataka launches Rs 1,000 crore Quantum Mission, to set up Q-city near Bengaluru

https://indianexpress.com/article/cities/bangalore/karnataka-launches-rs-1000-crore-quantum-mission-10162150/?utm_source=substack&utm_medium=email

The Karnataka government Thursday (31 July 2025) unveiled a Rs 1,000-crore Quantum Mission with a vision to transform the state into a $20 billion quantum economy by 2035 and establish it as the "quantum capital of Asia". As part of this mission, it announced the establishment of Q-City (Quantum City) near Bengaluru – a futuristic integrated hub for quantum technology innovation, manufacturing, research, and talent development.

The announcement was made during the inauguration of the Quantum India Summit 2025 held in Bengaluru, co-organised by the Department of Science & Technology (DST) and the Indian Institute of Science (IISc). Chief Minister Siddaramaiah and Minister for Science & Technology N S Boseraju laid out the government's roadmap to foster quantum innovation and infrastructure across the state.

"By 2035, we aim to create 10,000 high-skilled jobs and establish Karnataka as the quantum capital of Asia," Chief Minister Siddaramaiah said.

He added that a Quantum Technology Task Force will be constituted to guide policy frameworks, while the government will also launch a Quantum Venture Capital Fund to back more than 100 startups and generate at least 100 patents in the sector. The overall initiative is expected to create over 2 lakh direct jobs.

Minister Boseraju said, "As part of this effort, our government will establish Q-City where world-class facilities will be provided. This city will integrate academic institutions, innovation centres, manufacturing clusters for quantum hardware, processors, ancillary units, and R&D hubs supported by quantum high-performance computing (HPC) data centres."

The minister said the state is already home to India's first commercially deployable quantum computer, built locally in Bengaluru by a team of Kannadigas. "This computer is not just a proof of concept but a testimony to determination. Developed indigenously, it is already delivering commercial services," he added.

The state has already set up a Quantum Research Park at IISc Bengaluru, which has supported over 55 research and development (R&D) projects and 13 startups, while training more than 1,000 quantum professionals annually. To boost its activities, the state has sanctioned an additional Rs 48 crore in funding. Karnataka Thursday also announced plans to establish India's first Quantum Hardware Park, along with four innovation zones and a dedicated quantum chip fabrication facility, expected to be operational by the end of this year.

"Quantum chip fabrication capability will be operational by the year-end. This will enable domestic production of advanced quantum components and devices," Boseraju said. The minister also emphasised the need for policy flexibility from the Centre to enable state-level innovation.

"The Government of India has launched the National Quantum Mission with an outlay of Rs 6,000 crore. For its successful implementation, the Centre must allow Karnataka to lead with innovative and decentralised approaches," he said, addressing DST Secretary Abhay Karandikar.

To develop talent across the state, the science and technology minister said, Karnataka will roll out a quantum curriculum at the higher secondary level in both English and Kannada under its Stream Labs initiative. The state will also introduce quantum skilling programmes in 20 colleges, expand DST-funded PhD fellowships to 150 students, and take these programmes to tier-2 and tier-3 cities and over 20 universities. The roadmap is structured around five strategic pillars: talent development, R&D pilots, infrastructure, industry support, and global partnerships.

Karnataka also aims to develop 1,000-qubit quantum processors and pilot real-world applications in healthcare, cybersecurity, governance, agriculture, and early disease detection.

25. Citrix adds post-quantum cryptography to boost enterprise data security

by Ben Wodecki
https://www.sdxcentral.com/news/citrix-adds-post-quantum-cryptography-to-boost-enterprise-data-security/

Citrix added a handful of offerings to its NetScaler platform designed to strengthen enterprise data security.

Chief among the updates is support for post-quantum cryptography (PQC). Initially teased to customers back in April, the offering is designed to shore up enterprise applications with quantum computer-proof encryption capabilities.

Available via NetScaler version 14.1.51, Citrix's PQC solution is compatible with existing client browsers. The vendor said it will help users prepare for the eventual wider use of quantum computing, citing ISACA findings that just 5% of organizations have a roadmap to address the emerging technology.

Beyond future-proofing encrypted enterprise workloads, Citrix touts its PQC support as a way to shore up defenses against existing attacks, like harvest now-decrypt later, in which threat actors steal encrypted data now with the intention to wait for decryption technologies capable of breaking today's cryptography methods to become available.

"PQC support gives organizations a clear path to start their PQC transition now with full control of their timeline rather than waiting for quantum computers in the hands of bad actors to force their hand, all through a single platform," the NetScaler parent said in a statement.

Citrix also unveiled its latest long-term service release (LTSR), CVAD 2507, which the vendor claims adds more than 400 new features, improvements, and security updates.

Citrix's latest NetScaler update adds support for a wider range of operating systems, offers improved performance for graphically intensive workloads, with improvements also made to provisioning across cloud and virtualization platforms. Users can also obtain deeper insights into network conditions metrics, such as endpoint health and reconnect behaviors.

Update CVAD 2507 marks the first in a new cadence for Citrix's LTSRs, with one major update dropping every year, while CVAD releases will come three times per year.

The NetScaler updates come after Citrix issued a patch addressing critical flaws in the platform, only for the fix to break login functionality for some users. The patch ended up disrupting some legitimate authentication processes, particularly for users in environments using third-party identity providers or custom login scripts.

26. French National Quantum Update: July 2025

by Matt Swayne
https://thequantuminsider.com/2025/07/31/french-national-quantum-update-july-2025/

Executive Summary

In July 2025, it's become more evident that all echelons of French society are beginning to not just understand the impact of quantum technology, but act on that understanding to cement French leadership in what is becoming the quantum era.

French President Emmanuel Macron is raising national defense targets amid geopolitical uncertainty, while doubling down on leadership in disruptive technologies like AI and quantum. His administration has reaffirmed support for deeptech through the launch of a Franco-British engineering lab and by maintaining the integrity of the €54 billion France 2030 investment plan.

French quantum firms, including Quandela, Pasqal, and Quobly, are expanding partnerships across Europe and North America to build scalable, sovereign, and application-ready technologies. Research efforts continue to break new ground, including record-setting carbon qubit coherence and a roadmap to quantum advantage co-authored by IBM and Pasqal. Meanwhile, France is promoting scientific excellence through awards and events like the France Quantum 2025 conference, which drew over 1,000 participants to Paris.

Links to these stories – and more – are below.

Policy

Macron to boost French defence targets, citing rise of global threats

French President Emmanuel Macron is set to announce new French defence budgetary targets on Sunday, in the face of a menacing Russia and a potential US disengagement from Europe, his office said. France's

defence budget has already increased sharply since Macron took power, and is projected to rise from 50.5 billion currently to 67 billion euros in 2030. In an interview, Defence Minister Sebastien Lecornu said France was mostly worried about falling behind in "disruptive technologies" including artificial intelligence and quantum technology.

President Macron launches Imperial-CNRS joint engineering laboratory

The President of France, Emmanuel Macron, celebrated the launch of a new joint engineering laboratory between Imperial and France's CNRS. President Macron visited Imperial's South Kensington campus to meet the engineers who will lead the new laboratory and spoke about the growing UK-French scientific partnerships. The event formed part of the schedule of the state visit for the French President.

France 2030: There Will Be New on Space and Quantum

France's 2030 54 billion euro investment plan appears relatively untouched by recent budget cuts. The Planning Department has even just announced a new research program.

Business

Quandela and Mila Develop Hybrid Artificial Intelligence and Quantum Computing Technologies

Quandela, a European leader in photonic quantum computing, and Mila, the Quebec Artificial Intelligence Institute, announce a partnership to explore the potential of hybrid technologies combining machine learning and quantum computing. This strategic collaboration will focus on the development and evaluation of innovative quantum machine learning (QML) models, positioning both organizations at the forefront of this new technological frontier.

How Quandela Is Racing to Make Quantum Computing Practical

While quantum computing giants build massive and costly systems, Quandela Co-Founder and COO Valérian Giesz explains why the French startup's photonic approach is more efficient. Quandela has already sold quantum computers to European clients and is partnering with NVIDIA on AI integration.

Quobly and Inria Partner on Integrated, Scalable Silicon Qubit Architecture

Quobly, a pioneer in quantum microelectronics, and Inria, France's national institute for research in digital science and technology, announce a strategic partnership to align silicon-based quantum hardware with advanced control software. This alliance aims to structure a sovereign value chain by combining software excellence with hardware engineering. By expanding its R&D to include low-level software layers – such as those found in embedded, industrial, and operating systems – Quobly reaffirms its ambition to build a fully integrated, fault-tolerant, and scalable quantum computing architecture.

French-German Cooperation Advances Europe's Quantum Computer Lucy

Two leading technology companies from Germany and France are joining forces to help shape Europe's future in quantum computing: attocube systems GmbH, a company of the WITTENSTEIN group and specialist in nanotechnology, and Quandela, a pioneer in photonic quantum computer technology. The

companies have been working together on the development of the European quantum computer Lucy. Representatives of the owners, Management Board and senior management of the WITTENSTEIN group took advantage of a visit to Paris to meet with the Quandela team and assess the status of the joint project.

Pasqal, IBM Researchers Offer a Measured Path Toward Quantum Advantage

A new study from IBM and Pasqal outlines a rigorous framework for defining and demonstrating "quantum advantage" – which is often defined as the point at which quantum computers perform useful tasks more efficiently or accurately than classical systems. The paper doesn't claim this milestone has been reached but lays out a practical and testable roadmap to get there.

From resonances to quantum sensors: the medicine of the future starts today

In Thales laboratories in Palaiseau, quantum physics promises diagnostic devices hundreds of times more accurate, as small as a pen, capable of reading electrical discharges in the brain.

HiQuTe Diamond raises 7.5M€ to bring technological diamonds into the industrial era

French deeptech HiQuTe Diamond, specialist in the manufacturing of very high quality diamonds for technological applications, announces a fundraising of 7.5 million euros. This strategic financing, in particular from the Ile-de-France Reindustrialization Fund (initiated by the Île-de-France region and operated by Innovacom), from the French Tech Seed fund managed on behalf of the State by Bpifrance as part of France 2030, TF Participations, Socadif and iXcore, will allow the company to industrialize its production in Île-de-France and meet growing needs in power electronics, quantum computing and new generation sensors.

Research

Carbon Qubits Break Record for Longevity in Quantum Circuits

A team of researchers report they have demonstrated microsecond-scale coherence times in a carbon nanotube circuit driven by cavity photons—showing longer-lived quantum states than any previously recorded for carbon quantum dots and surpassing similar systems built with silicon.

The study, published in Nature Communications by a team that included scientists from C12 Quantum Electronics and several French research institutions, reports coherence times of 1.3 microseconds in a suspended carbon nanotube double quantum dot setup integrated within a microwave cavity. That figure represents a roughly 100-fold improvement over previous carbon-based implementations and a tenfold improvement over similar silicon quantum dot devices.

The PEPR Quantum congratulates its award-winning members

The PEPR Quantum congratulated its award-winning members. Igor Ferrier-Barbut won CNRS Bronze Medal 2025. Ferrier-Barbut is a CNRS researcher at the Charles Fabry Laboratory (LCF, CNRS/Institut d'Optique Graduate School). He and his team are working to create devices capable of storing or transforming quantum information carried by light. Christopher Bäuerle won an ERC Advanced Grant 2024.

Bäuerle is CNRS Research Director at Institut Néel and coordinator of the PEPR Quantique project eQubitFly, aimed at developing a new quantum architecture by exploiting electronic flying qubits.

Alain Aspect, Nobel Prize in Physics and member of the Académie des Sciences, joins the Académie française

The French Academy of Sciences welcomes the election of one of its members to the French Academy. Physicist Alain Aspect, director of research emeritus at the CNRS Charles Fabry Laboratory(CNRS/ Institut d'optique Graduate School), winner of the 2022 Nobel Prize in Physics for his experimental work on quantum entanglement, contributing to today's quantum technological revolution, and a member of the Académie des Sciences since 2001, joins the thirty-three "Immortals" in the chair of Mr. René de Obaldia, French playwright, novelist and poet (F22).

Education qnd Events

Video Highlights of Quantum of France Quantum 2025 – After Movie

Organizers of France Quantum Conference 2025 published an After Movie in July that featured some highlights of the event. The conference, held in June, at Station F in Paris, is a major event focused on internationalizing quantum technologies. It's the fourth edition of the conference and drew more than 1,000 participants and 60 international experts.

Pushing quantum limits: A Canada–France collaboration on nonlocal boxes

What began as a master's thesis has grown into a dynamic international collaboration that pushes the boundaries of quantum research. Led by Professor Anne Broadbent, this Canada–France partnership is advancing science while offering students transformative global experiences.

27. Crypto-agility: The unsung hero in the quantum security race

by Marco Pereira
https://www.capgemini.com/crypto-agility-the-unsung-hero-in-the-quantum-security-race/

In the global race to secure digital infrastructure against quantum threats, post-quantum cryptography (PQC) often takes the spotlight – and rightly so. Quantum computing has the potential to break the cryptographic systems that currently protect our data, communications, and national infrastructure.

But there's another capability that deserves equal attention – crypto-agility. Quietly, but powerfully, it is emerging as the foundational layer upon which a truly quantum-resilient future will be built.

What is crypto-agility – and why it matters

Just as security by design and, more recently, privacy by design have become essential principles in the development of modern IT solutions, it's time to embrace a new imperative: crypto-agility by design. In a

world where cryptographic algorithms can become obsolete overnight – due to advances in computing power, quantum threats, or newly discovered vulnerabilities – crypto-agility is no longer optional.

Crypto-agility is the ability to swiftly switch between cryptographic algorithms – whether in response to a new vulnerability or to adopt an emerging standard – without disrupting operations. It's not about replacing cryptography once; it's about building the flexibility to respond again and again as threats evolve, and standards mature.

This proactive approach ensures long-term resilience and trustworthiness, much like how security and privacy are now embedded from the ground up. As digital ecosystems grow more complex and interconnected, crypto-agility must become a foundational design principle – not an afterthought.

Quantum computing isn't the only threat. The recent vulnerabilities in widely used libraries like OpenSSL are stark reminders of how brittle our current cryptographic landscape can be. Yet, our recent CRI research reveals a troubling picture:

- Only 35% say their organizations maintain a centralized inventory of all cryptographic keys, algorithms, and certificates in use.
- 54% of organizations operate on legacy infrastructure that lacks compatibility with modern cryptographic standards.
- Just 40% are prepared to respond effectively to the discovery of a critical vulnerability in a widely used cryptographic library.

These are not just technical blind spots – they are business risks.

Building crypto-agility: What it takes

Crypto-agility isn't a feature you can simply buy off the shelf. It must be intentionally designed into your systems, processes, and organizational culture. Here's what that journey looks like:

- **Maintain a live cryptographic inventory:** Know which algorithms, keys, and certificates are in use – and where they reside.
- **Automate key and certificate management:** Manual processes cannot keep up with today's evolving threat landscape.
- **Design modular, update-ready systems:** Avoid hard-coded cryptography. Use configuration files and CI/CD pipelines for rapid updates.
- **Rotate keys regularly:** Annual key rotation should be the baseline – automated rotation is even better.

The barriers are real – but so are the rewards

Crypto-agility is not just a technical challenge; it's an organizational shift. Our CRI research shows that:

- 67% of organizations struggle with dedicated budget and personnel for crypto transitions.
- 59% lack the expertise to assess, plan, and implement crypto-agility.
- 54% operate on legacy infrastructure that's incompatible with modern standards.

These numbers reflect inertia – but they also highlight the opportunity for leaders to act before the curve. As Bernd Meurer, Field CTO at BT Group, notes:

"Many of our customers have done a high-level assessment of systems and communication interfaces, but a full impact analysis for post-quantum readiness is still in draft in many cases."

This is the reality for many large enterprises – and a call to action for all.

Some early adopters are embedding crypto-agility into their PQC pilots through hybrid cryptography, which combines classical and quantum-safe algorithms. This allows them to test emerging standards without breaking existing systems.

A strategic advantage in the post-quantum era

Crypto-agility is the bridge between today's encryption and tomorrow's post-quantum world. It enables resilience not just against quantum, but also against the unknowns that lie ahead in our increasingly complex threat landscape.

At Capgemini, we believe that crypto-agility is no longer a "nice to have." It's a core business capability, and a marker of forward-thinking leadership. Organizations that build it now will gain the flexibility to evolve, adapt, and thrive – no matter how the future unfolds.

The quantum era is coming. Crypto-agility will define who's ready.

28. Researchers Define Path to Quantum Advantage

by Berenice Baker
https://www.iotworldtoday.com/quantum/researchers-define-path-to-quantum-advantage

Researchers from IBM and quantum startup Pasqal have published a white paper that establishes criteria for determining when quantum advantage, the point at which quantum computers outperform classical systems, has truly arrived.

The paper, on arXiv, addresses how to recognize quantum advantage as the first claims emerge.

The collaborative research tackles the question of how to identify genuine quantum advantage. According to the authors, quantum advantage isn't a single breakthrough moment but rather a series of validated hypotheses that will collectively demonstrate quantum computing's capabilities.

"We define quantum advantage as the ability to execute a task on a quantum computer in a way that satisfies two essential criteria," the authors wrote.

"First, the correctness of the quantum computer's output can be rigorously validated. Second, it is performed with a quantum separation that demonstrates superior efficiency, cost-effectiveness or accuracy over what is attainable with classical computation alone."

The researchers predict that by the end of 2026, the quantum community will have uncovered the first definitive quantum advantages. They emphasize that the advantages will come from hybrid approaches where quantum systems augment classical workflows rather than quantum computers working alone.

Three problem areas are identified as the most likely to yield the first quantum advantage claims: Sampling problems, variational problems and calculating expectation values of observables. Variational problems and expectation value calculations are considered particularly promising because their results can be more easily validated.

The white paper outlines the technical requirements for achieving quantum advantage: Performant quantum hardware, infrastructure for synchronized classical-quantum computing and methods for running accurate quantum circuits. Error mitigation techniques, which reduce the effects of noise in quantum circuits, are described as necessary for achieving quantum advantage before full error correction becomes available.

Several real-world examples already hint at quantum computing's business potential. Startup Kipu Quantum recently reported that its quantum algorithms solved complex business optimization problems faster than traditional computing methods, potentially offering companies quicker solutions to scheduling, logistics, and resource allocation challenges. Q-Ctrl has shown how quantum computing can tackle constrained optimization problems, which are common in supply chain management and operational planning.

Meanwhile, researchers are making progress with quantum techniques that could revolutionize materials science and chemical research.

These approaches, with names like "sample-based quantum diagonalization" and "Krylov quantum diagonalization," allow scientists to model complex molecular structures more accurately than ever. For pharmaceuticals, manufacturing, and materials development businesses, this could mean faster discovery of new drugs, catalysts, and advanced materials with significant cost savings compared to traditional trial-and-error methods.

The IBM-Pasqal collaboration establishes a common framework for evaluating quantum advantage claims. As quantum hardware improves—Pasqal's neutral-atom platform has demonstrated 100+ qubits and is expected to reach 250 qubits by 2026—the evaluation of quantum advantage claims continues.

"Quantum advantage won't be a single moment in time," the researchers note. "Rather, we'll see several hypotheses tested until eventually the community determines that quantum advantages have been realized."

This approach to defining and validating quantum advantage provides a roadmap for the field as it transitions from theoretical potential to practical superiority over classical computing methods. The researchers emphasize that even after the first quantum advantages are established, the search for new quantum algorithms will continue, similar to how classical computing algorithms continue to evolve today.

29.Random Number Enhancement Boosts Security of ChaCha Encryption Algorithm

by Quantum News
https://quantumzeitgeist.com/random-number-enhancement-boosts-security-of-chacha-encryption-algorithm/

The widespread use of the ChaCha algorithm in secure communication and data streaming faces increasing threats from advances in artificial intelligence and computing power, prompting researchers to seek ways to bolster its defences. Chao Liu, Shuai Zhao, and Chenhao Jia, from multiple institutions including institution, lead a team that addresses this challenge with a new variant, Random Number Enhanced ChaCha, or QRE-ChaCha. This improved algorithm strengthens ChaCha by incorporating quantum random numbers, both during initial setup and periodically throughout the encryption process, to enhance the diffusion of information and resist attack. The team's analysis demonstrates that QRE-ChaCha exhibits significantly improved resistance to differential attacks while maintaining the speed and efficiency of the original ChaCha, and its generated keystream successfully passes rigorous statistical randomness tests, ensuring its suitability for demanding cryptographic applications.

ChaCha Cipher Enhanced by Quantum Randomness

This research details an improvement to the ChaCha stream cipher by incorporating Quantum Random Number Generation (QRNG). The team aimed to strengthen the cipher against potential attacks that exploit weaknesses in traditional random number generators. Key findings demonstrate that integrating QRNGs enhances security, and the research includes a comprehensive review of existing cryptography, stream ciphers, QRNGs, and cryptanalysis techniques. The authors rigorously tested the improved algorithm, employing statistical tests and security analyses to validate its performance. This work contributes to the ongoing effort to enhance cryptographic security by leveraging the benefits of true randomness provided by QRNGs, potentially leading to more robust and secure communication systems.

Quantum Randomness Enhances ChaCha Encryption Security

To strengthen the ChaCha cipher against modern threats, researchers developed QRE-ChaCha, which integrates quantum random numbers into the encryption process. This approach addresses vulnerabilities in existing ciphers susceptible to attacks like differential cryptanalysis and key-recovery attacks, while maintaining high performance. The core innovation lies in incorporating quantum random numbers directly into the ChaCha algorithm by XORing initial constants with these random numbers, effectively randomizing the encryption's starting state. Furthermore, the team periodically injects additional quantum random numbers into selected parts of the cipher's internal calculations during odd rounds, increasing the diffusion of randomness. Rigorous evaluation involved theoretical analysis, automated vulnerability searches, and extensive statistical testing using the NIST statistical test suite and the GM/T 0005-2021 standard. Results confirm that QRE-ChaCha maintains the efficiency of the original ChaCha cipher.

Quantum Randomness Enhances ChaCha Encryption Security

Researchers have developed an enhanced version of the ChaCha cipher, a widely used encryption algorithm, by integrating quantum random numbers into its core operations. Unlike methods that modify the cipher's internal structure, QRE-ChaCha leverages the inherent unpredictability of quantum mechanics to bolster its defenses. The team injected quantum random numbers into two critical stages: the initial seed and the round function. Testing demonstrates that QRE-ChaCha exhibits significantly improved resistance to differential cryptanalysis and successfully passes stringent statistical randomness tests, including those defined by the NIST statistical test suite and the GM/T 0005-2021 standard. Importantly, this increased security is achieved without sacrificing performance, maintaining the high speed and efficiency that have made ChaCha popular in applications like real-time communication and data streaming. This research represents a promising step towards strengthening symmetric encryption algorithms in the face of emerging threats and extends the practical applications of quantum random number generators.

Quantum Randomness Boosts ChaCha Cipher Security

The research presents QRE-ChaCha, a new stream cipher that builds upon the widely used ChaCha algorithm. The key innovation lies in incorporating quantum random numbers into the encryption process, both during initialization and periodically throughout the encryption rounds. Results demonstrate that QRE-ChaCha significantly improves resistance to differential cryptanalysis compared to the original ChaCha cipher, with substantially lower upper bounds of differential trail probabilities. Furthermore, keystreams generated by QRE-ChaCha successfully passed rigorous statistical randomness tests using both the NIST Statistical Test Suite and the GM/T 0005-2021 standard. Importantly, these security enhancements were achieved without compromising performance, with encryption speeds remaining comparable to those of the original ChaCha cipher. QRE-ChaCha also functions as a quantum randomness expansion scheme, potentially offering broader applications beyond encryption.

30. India Opens Rolling Call for Quantum Startups Under National Mission

by Matt Swayne
https://thequantuminsider.com/2025/07/24/india-opens-rolling-call-for-quantum-startups-under-national-mission/

India's Department of Science and Technology is inviting startups to apply for research support under its National Quantum Mission, marking a key move to accelerate the country's push into quantum technology.

The call for proposals, which opened on July 15, 2025, is part of a broader government strategy to build a strong domestic quantum ecosystem through sustained support for early-stage innovation. According to the Department of Science and Technology (DST), the initiative focuses on four main areas of quantum technology: sensing and metrology, communication, computing, and materials and devices.

Startups developing technologies in these areas are eligible to apply. Each startup must choose one domain and submit its proposal to the corresponding Thematic Hub, a government-backed center of excellence housed at a leading Indian academic institution. These include IISc Bengaluru for quantum computing, IIT

Madras for quantum communication, IIT Bombay for sensing and metrology and IIT Delhi for materials and devices.

Unlike fixed-deadline grant cycles, this call is open on a rolling basis. This allows companies to apply whenever they are ready, providing a flexible path to access government backing as they reach technical milestones.

The program is open to Indian startups and for-profit institutions. Proposals are expected to demonstrate clear potential for technological impact, as well as a feasible plan for reaching commercial or applied readiness. Each Thematic Hub manages its own intake and review process, and applicants must apply directly through the relevant hub's portal.

The hubs are designed to serve as more than just funding channels. Each one offers scientific mentorship, infrastructure support, and access to academic networks that can help early-stage companies move more quickly through the research and development phase. According to DST, these hubs are intended to serve as innovation nodes—connecting companies to top-tier researchers, lab space, and testing infrastructure in a highly specialized environment.

Launched in 2023, the National Quantum Mission is one of India's most ambitious science and technology efforts to date. It was created to position the country as a competitive force in quantum research and commercialization, a field seen as increasingly strategic to economic growth and national security. DST leads the initiative, with support from several of India's most prominent technical institutions, including IITs and the Centre for Development of Telematics (C-DOT).

The initiative is part of a broader global race to build quantum capabilities. While the U.S., China, and European nations have made multi-billion-dollar bets in this space, India's approach is to build a long-term foundation by focusing on early research, talent development, and local industry partnerships. The startup support call is one piece of that plan, intended to create viable commercial pathways for quantum technologies developed in India.

The mission's structure also reflects a bet on decentralization. Rather than placing all activity under a single authority, DST has distributed responsibilities across domain-specific hubs to create focus and depth in each area. That approach could allow for faster iteration and better alignment between startups and the specific technical challenges they aim to solve.

With the rolling call now open, DST hopes to attract a new wave of quantum entrepreneurs who can contribute to India's next phase of scientific development – while helping the country compete in a field increasingly seen as critical to the global technology landscape.

More information and application details are available through the individual websites of the four Thematic Hubs.

31. WhatsApp is refused right to intervene in Apple legal action on encryption 'backdoors'

by Bill Goodwin
https://www.computerweekly.com/news/366627911/WhatsApp-is-refused-right-to-intervene-in-Apple-legal-action-on-encryption-backdoors?utm_campaign=20250724_WhatsApp+is+refused+right+to+intervene+in+Apple+legal+action+on+encryption+%E2%80%98backdoors%E2%80%99&utm_medium=email&utm_source=MDN&source_ad_id=366627911&asrc=EM_MDN_316969553&bt_ee=G3x1at47aybLWHXxVkwnvwU9iVtq8JEp2jpEEalT4WvZPgBviTRQ5OjcwOpyGEsu&bt_ts=1753352971831

A court is to hear legal challenges against a secret order issued by the Home Office that requires Apple to give British law enforcement and intelligence agencies the ability to access users' encrypted data stored on iCloud in a public hearing in 2026.

The Investigatory Powers Tribunal (IPT) ruled on 23 July that it would hear five legal challenges, brought by Apple, Privacy International, Liberty and two individuals, in open court over seven days at the "earliest opportunity" next year.

The court refused to allow encrypted messaging service WhatsApp the right to intervene and submit evidence in the case brought by campaign groups Privacy International and Liberty. Apple is bringing its own case, which will be considered alone.

WhatsApp CEO Will Cathcart submitted evidence to the tribunal in June, raising concerns that the move by the UK government would undermine the security of people using encrypted communication and cloud services.

He said the technical capability notice (TCN) would set a "dangerous precedent for security technologies that protect users around the world".

Next year's hearing will test the ability of technology companies to use encryption to secure their customers' data without being ordered to create "backdoors" to provide access to UK law enforcement and intelligence services.

The Home Office argues that it needs the capability to access encrypted data stored by Apple users anywhere in the world on its iCloud service to fight terrorism and child abuse.

Technology companies and security experts have repeatedly warned that government attempts to weaken encryption will inevitably be exploited by cyber criminals and rogue nation states, impacting the security of internet users worldwide. They argue that there are ways to fight crime without weakening encryption.

The Home Office's decision to issue a TCN against Apple in January has raised tensions between US lawmakers and the UK government over what the US sees as unwelcome interference in US "big tech" companies.

President Donald Trump and US intelligence chief Tulsi Gabbard have criticised the Home Office's move against Apple. Gabbard warned that any attempt by the UK to create a backdoor that would allow the UK to access the data of Americans would be a "clear and egregious violation".

Court permits Home Office NCND

Although the existence of the order became public knowledge when it was leaked to the *Washington Post*, the IPT found that the Home Office should be allowed to continue its policy of "neither confirming nor denying" (NCND) the existence of the order against Apple.

Judges rejected arguments from Privacy International and Liberty that the court should hear legal arguments over whether the Home Office should be allowed to continue with its NCND policy, as this would delay hearing Apple's case against the Home Office.

The court will proceed based on "assumed facts" rather than "actual facts". This will enable the hearing to be held in public without requiring the Home Office or Apple to disclose details of the order, which could only be heard in a private court session.

In April, the IPT dismissed attempts by the Home Office to require all legal arguments to be heard in a secret "closed" court that would exclude the public, press and Apple's lawyers, following the intervention of a consortium of 10 media organisations, including Computer Weekly, the BBC, the *Guardian*, the *Telegraph* and *Reuters*.

NCND policy `absurd'

Caroline Wilson Palow, legal director and general counsel of Privacy International, said she welcomed the court's decision to hear Apple's case, and that of Privacy International and Liberty, in largely public hearings.

But she said the UK government's insistence on maintaining its "neither confirm nor deny" policy, when the existence of the order has been widely leaked, reported and discussed, was "absurd".

"We are being forced to sustain the fiction that the order does not exist, which may hinder our ability to grapple fully with its legal ramifications," she said.

The Privacy International lawyer said the tribunal's refusal to allow WhatsApp to intervene in the case "denied the largest provider of end-to-end encrypted services in the world a chance to defend itself and its users".

"There should be no mistake – the fight over the Apple order is ultimately about end-to-end encryption and whether the UK government can dictate if this vital form of digital security should exist for users worldwide," she added.

WhatsApp warned in June that the case could undermine the security of people's private communications and expose them to attacks from hackers and hostile nation states.

"We've applied to intervene in this case to protect people's privacy globally. Liberal democracies should want the best security for their citizens. Instead, the UK is doing the opposite through a secret order," said Cathcart.

"This case could set a dangerous precedent and embolden nations to try to break the encryption that protects people's private communication," he added.

WhatsApp will continue to oppose moves to break encryption

A WhatsApp spokesman said last night that the company was disappointed at not being allowed to present its arguments in the Investigatory Powers Tribunal but would continue to oppose attempts by governments to weaken encryption.

"This is deeply disappointing, particularly as the UK's attempt to break encryption continues to be shrouded in layers of secrecy. We will continue to stand up to governments that try to weaken the encryption that protects people's private communication," the spokesman added.

Apple withdrew its Advanced Data Protection (ADP) service from UK users in February 2025, rather than comply with the Home Office's order. "As we have said many times before, we have never built a backdoor or master key to any of our products or services, and we never will," Apple said in a statement at the tim

The legal challenges to the Home Office are being brought by Privacy International; Liberty; Gus Hosein, executive director of Privacy International, and Ben Wizner, director of the ACLU's Speech, Privacy and Technology Project. Apple is bringing a separate legal challenge.

32. Three-in-one post quantum cryptography PQC block saves area, power

by Nick Flaherty
https://www.eenewseurope.com/en/three-in-one-post-quantum-cryptography-pqc-block-saves-area-power/

UK chip designer EnSilica has developed a combined PQC hardware encryption accelerator IP block that cuts the silicon area by two thirds.

The licensable eSi-CRYSTALS PQC accelerator supports the full CRYSTALS post-quantum cryptography (PQC) suite approved by the NIST, Integrating three IP blocks for the Dilithium (FIPS-204), Kyber (FIPS-203) and SHA-3 (FIPS-202) algorithms saves silicon area, power and cost.

After several years of competition, NIST released its first three finalised PQC standards to address the threat of quantum computers cracking the existing AES encryption standards in the future. However the first implementations have been for enterprise and networking systems where the silicon area is less important.

- Ensilica to build fully integrated ASIC for resilient satellite navigation
- IoT ASIC deal with Danish chip designer

EnSilica previously announced separate Dilithium, Kyber and SHA-3 algorithms licensed for use by a major semiconductor company for a 5 nm networking ASIC. The new IP offers a more compact implementation than separate cores. EnSilica also has a full suite of classical cryptographic accelerators including ECC, ECDSA, RSA, AES, ChaCha20, and Poly1305. In addition, the company offers a NIST-compliant true random number generator (TRNG).

Combining the three PQC accelerators into a single block allows PQC algorithms to be used in a wider range of chips, including edge processing.

Harvest now, decrypt later

"The emerging PQC threat is not just theoretical. Security analysts warn that adversaries can already capture encrypted data today, with the intention of decrypting it in the future when quantum capabilities become available, a tactic known as 'harvest now, decrypt later'," said Ian Lankshear, CEO of EnSilica. "The implications are profound for those relying on today's cryptographic schemes, which is why EnSilica's PQC offering delivers future-proof hardware protection at the silicon level with minimal silicon area for mature and advanced technology nodes."

Dilithium is used for digital signatures, providing authentication and data integrity, while Kyber is a key encapsulation mechanism that enables secure key exchange. Integrated into the block is also a hardware-optimised implementation of the cryptographic SHA-3 hash function that creates a digital fingerprint of data allowing for robust integrity verification. Together, these algorithms form the foundation for quantum-resistant security in modern systems, ensuring long-term protection of sensitive information.

33. UK may be seeking to pull back from Apple encryption row with US

by Bill Goodwin
https://www.computerweekly.com/news/366627928/UK-may-be-seeking-to-pull-back-from-Apple-encryption-row-with-US?utm_campaign=20250722_UK+may+be+seeking+to+pull+back+from+Apple+encryption+row+with+US&utm_medium=email&utm_source=MDN&source_ad_id=366627928&asrc=EM_MDN_316871013&bt_ee=3LDH4s9FgD%2BhlO%2BwwLnivaKsTlPX95eNm8ceBajy0FUKQ4xgU5d26CczOxMwCUXI&bt_ts=1753180156786

The government may be seeking to pull back from a diplomatic row with the US over UK demands to require Apple to give the UK access to secure data stored by Apple users.

UK government officials have told the *Financial Times* that pressure from senior US officials, including vice-president JD Vance could force the UK to retreat from the plan.

Home secretary Yvette Cooper issued a notice against Apple under the Investigatory Powers Act in January, requiring the company to provide law enforcement with the capability to access encrypted data stored by Apple users on Apple's iCloud service. The move has attracted opposition from both Democratic and Republican law makers in the US, and has been criticised by president Trump and JD Vance, who object to the UK interfering with US technology companies.

Two government officials, believed to be from the Department of Science Innovation and Technology (DSIT), told the *Financial Times* that the UK's decision to force Apple to break its end-to-end encryption could disrupt technology agreements with the US.

"One of the challenges for the tech partnerships we're working on is the encryption issue," one official said. "It is a big red line in the US: they don't want us messing with their tech companies. This is something that the vice-president is very annoyed about and which needs to be resolved. The Home Office is basically going to have to back down."

A second official said that the Home Office had "its back against the wall" and that the problem was of the "Home Office's own making".

The government maintains that it needs access to Apple customers' secure files in order for law enforcement to investigate terrorism and child sexual abuse. The government order, known as a Technical Capability Notice, however, led Apple to withdraw its secure Advanced Data Protection (ADP) service from UK customers. The company is now challenging the lawfulness of the Home Office's order in the Investigatory Powers Tribunal.

Computer Weekly previously reported that WhatsApp, the encrypted messaging service owned by Meta, has agreed to provide legal submissions in support of Apple. Civil Society groups, Amnesty and Privacy International have filed a separate claim to the Investigatory Powers Tribunal challenging the Home Office. A third senior British official told the *Financial Times* that the UK government was reluctant to push "anything that looks to the US vice-president like a free-speech issue".

The US vice-president attacked Europe and the UK in February for opposing free speech on social media and more generally in a speech at the Munich Security Conference. "In Britain, and across Europe, free speech, I fear, is in retreat," he said.

The US director of national intelligence Tulsi Gabbard said in a letter published in the same month that she shared concerns raised by US Congress over reports that the UK has issued an order against Apple that could "undermine Americans' privacy and civil liberties".

President Donald Trump confirmed in an interview with *The Spectator* that he had raised the Apple TCN with prime minister Keir Starmer during his visit to Washington, comparing the UK's actions to the conduct of China: "We actually told him [Starmer]...that's incredible. That's something, you know, that you hear about with China."

Ben Collier, chair of the Foundation for Information Policy Research, a think tank for internet policy which today published a report on the Apple affair, said that it was not surprising that the Home Office's attempt to compel Apple to undermine the security of its products is facing resistance from the US.

"Tactics like issuing encryption removal orders to tech companies will only make every iPhone user in the UK less secure," said Collier. "As the UK government's own guidance for companies and the public makes clear, strong encryption is at the heart of keeping the services we all use safe and secure. There is no way to undermine encryption which doesn't leave huge weaknesses that criminals and hostile state actors can exploit.

"Law enforcement have much more effective tactics – ones which don't involve undermining our shared security – to investigate and disrupt serious criminal activity where encryption is being used. The government would be sensible to step back and retract this notice, and instead focus on the important work of renewing the UK's basic infrastructure, digital security and privacy protections," he added.

34. The dawn of quantum advantage

by Ryan Mandelbaum, Jay Gambetta, Borja Peropadre, and Olivia Lanes
https://www.ibm.com/quantum/blog/quantum-advantage-era

Quantum computing is about to enter an important stage – the era of quantum advantage. The first claims of quantum advantage are emerging, and over the next few years, we expect researchers and developers to continue presenting compelling hypotheses for quantum advantages. In turn, the broader community will either disprove these hypotheses with cutting-edge techniques – or the advantage holds.

Put simply, quantum advantage means that a quantum computer can run a computation more accurately, cheaply, or efficiently than a classical computer. Between now and the end of 2026, we predict that the quantum community will have uncovered the first quantum advantages. But there's more to it than that.

We have arrived already at a place where quantum computing is a useful scientific tool capable of performing computations that even the best exact classical algorithms can't. We and our partners are already conducting a range of experiments on quantum computers that are competitive with the leading classical approximation methods. At the same time, computing researchers are testing advantage claims with innovative new classical approaches.

So, how will we know if and when we've achieved quantum advantage?

We've published a new white paper with startup Pasqal that lays out the definition of quantum advantage, how we can scientifically validate claims, and potential ways to achieve it.

What is quantum advantage?

In our white paper, we define quantum advantage as the ability to execute a task on a quantum computer in a way that satisfies two essential criteria. First, the correctness of the quantum computer's output can be rigorously validated. Second, it is performed with a *quantum separation* that demonstrates superior efficiency, cost-effectiveness, or accuracy over what is attainable with classical computation alone.

This definition has several implications. The first is that we don't expect quantum advantages to be achieved by quantum computers acting alone. Instead, they will emerge from use cases where we leverage quantum computers to augment a classical workflow. So, quantum advantage really means that "quantum plus classical" can outperform classical alone.

The ideal benchmark we strive for is an *unconditional quantum separation*—a clear, provable gap in algorithmic performance between quantum and classical computers. These separations are typically grounded in complexity theory-based assumptions or derived from direct comparisons with the best-known

classical algorithms. In certain specific cases, researchers have already identified the potential existence of such separations. However, most existing results so far do not demonstrate the exponential performance advantage that quantum computers are poised to deliver.

Given that definition, we expect the first quantum advantage claims to arise in one of three problem areas: sampling problems, variational problems, and calculating expectation values of observables.

At the same time, it can be challenging to rigorously confirm when an advantage has occurred unless the result can be checked classically or uses the variational principle, which is not always the case. Instead, we will need to rely on verifying each part of the computation on its own, which can be done using trusted methods of error detection and mitigation.

The requirement for rigorous validation implies that, in practice, research groups will hypothesize that they've demonstrated a quantum advantage, and then attempt to validate the result. At the same time, the community will respond with attempts to support or falsify the hypothesis. This back-and-forth will continue until we reach a consensus. We also believe that it positions variational problems and calculating expectation values as likely delivering the first proven advantages, given our ability to validate these kinds of problems.

That leads to a critical point: quantum advantage won't be a single moment in time. Rather, we'll see a number of hypotheses tested until eventually the community determines that quantum advantages have been realized.

And that's only the start, because the search for quantum advantages doesn't end after the first claims are accepted. We must continue developing the algorithms that will bring useful quantum computing to the world. That search will continue even after the release of the first large-scale, fault-tolerant quantum computers, in much the same way that computer scientists push the field of classical computing forward today.

So, let us be clear: By the end of next year, we predict that the community will coalesce around an agreement over the first demonstrations of quantum advantages. From that point forward, we will continue searching for new algorithms that extract further value from quantum computers.

A clear path to quantum advantage

IBM has long promoted a clear, incremental path to quantum advantage. We are driving innovations in quantum computing hardware to extract accurate, valuable outputs from quantum circuits. At the same time, domain experts and developers from IBM and the quantum community are searching for valuable quantum computing algorithms.

Back in 2023, IBM achieved a critical milestone along this path with quantum utility. Quantum utility demonstrated that a quantum computer could perform reliable computations at a scale beyond brute force classical simulations of quantum circuits. But now, advantage means outperforming all classical methods.

Pushing forward along that path requires that we improve three key hardware and infrastructural elements to achieve advantage: Performant quantum hardware, infrastructure to run programs synchronized across

classical and quantum resources, and methods for running accurate quantum circuits. For that third piece, our partners are providing valuable help.

Near-term error mitigation to achieve long-term advantage

Fully-realized fault-tolerant quantum computing will require implementing error correction – but in the meantime, a new set of techniques have arisen that can reduce and eliminate bias in expectation value calculations caused by noise in quantum circuits. We call these error mitigation techniques – they "mitigate" the effects of noise. Error mitigation is crucial for achieving quantum advantage before the end of 2026, and is likely to play an important role in early fault-tolerant regimes.

Some of today's error mitigation techniques use classical post-processing, and those require exponential computational overhead. However, for near-term demonstrations, they scale far more favorably than classical simulation methods, and that scaling will continue to improve alongside improving hardware.

A number of our partners are building powerful error mitigation methods, which can be accessed as a service via our Qiskit Function Catalog. For example, Algorithmiq's Tensor Network Error Mitigation (TEM) circuit function manages noise in software post-processing, while lowering quantum processing unit usage. As we move along the IBM Quantum roadmap towards increasingly large quantum systems, incorporating error mitigation services such as Algorithmiq's TEM function demonstrates the use of classical HPC to extend the reach of current quantum computers, an architecture we call quantum-centric supercomputing. We expect that techniques like TEM will help the research community discover quantum algorithms that will unlock new computational territory and facilitate the push towards quantum advantage.

Another example of error-mitigation's success is Qedma's Quantum Error Suppression and Error Mitigation (QESEM) circuit function – also available in the Qiskit Functions Catalog. QESEM combines quantum error suppression and error mitigation to reduce hardware-level errors, and provides a resource-efficient service to improve quantum computation reliability. For QESEM users, this means it improves accuracy for executing utility-scale circuits and beyond, enabling researchers to unlock greater value from near-term quantum computation.

These are just two examples among many that highlight how improving and simplifying the use of error mitigation techniques is the key to realizing useful quantum computing in the near term. As the capabilities of the Qiskit Functions Catalog expand, so too will the ways error mitigation can help solve more complex problems between now and 2029.

With errors accounted for, we must now run algorithms on these systems that demonstrate a quantum separation.

The seeds of advantage

Researchers using quantum computers are already uncovering potential paths toward achieving quantum advantage. These algorithms are using quantum as a computational tool for research investigating applications beyond what classical computing can achieve alone.

In other words, our users are sowing the seeds of quantum advantage: drafting and presenting the first hypotheses of advantage to the community.

Just recently, researchers at the startup Kipu Quantum claimed a runtime quantum advantage, where their quantum algorithm ran faster than specific-purpose classical solvers for dense, higher-order unconstrained binary (HUBO) optimization problems. They identified instances that were challenging for methods like CPLEX and simulated annealing, and found that running their BF-DCQO quantum algorithm on ever-improving quantum hardware reported faster approximate solutions. They expect their runtimes to be soon orders of magnitude faster as hardware continues to advance. In addition, the Kipu team tested BF-DCQO against Quantum Annealing and LR-QAOA. They found that BF-DCQO outperformed both alternative methods in accuracy, runtime and resources — specifically in terms of qubit overhead for Quantum Annealing and circuit depth for LR-QAOA — in the tested instances.

Startup Q-CTRL has also benchmarked IBM Quantum systems against classical, quantum annealing, and trapped-ion technologies for optimization — unlocking a more than 4 × increase in solvable problem size and outperforming commonly used classical local solvers; capability that is available through their Optimization Solver application function. And in a recent collaboration with Network Rail on a scheduling solution, Q-CTRL's Performance Management circuit function, which powers the Optimization Solver function, enabled the largest demonstration to date of constrained quantum optimization, accelerating the path to practical quantum advantage. In another demonstration, they generated a 75-qubitentangled state. This was achieved with the help of a new method for performing the entangling CNOT gate, plus a lightweight error-detection scheme. The result was an impressive feat of long-range quantum entanglement and computational gains (85%+ fidelity over 40 qubits).

Meanwhile, one family of algorithms combines quantum and classical computing resources to return solutions with comparable accuracy to the leading classical approximation methods for chemistry and materials science. These algorithms follow the variational principle, the principle that allows us to understand a system by calculating the minimum or maximum of a function.

Variational principle: a promising direction for advantage

Techniques for solving problems obeying the variational principle are bringing practical quantum advantage tantalizingly close in the fields of chemistry and materials science. Solutions to these problems can be ranked and compared against classical methods. Therefore, if a quantum solution offers a better accuracy or lower energy, that indicates a possible quantum advantage that can be rigorously validated.

One such technique is sample-based quantum diagonalization (SQD), which aims to find a simpler way to express a quantum system's Hamiltonian — the mathematical object used to calculate the total energy of the system. Starting with an educated first guess, a quantum computer and classical computer work together to find an appropriate subspace that the Hamiltonian can be projected onto. It is as if the quantum computer is taking a picture of the Hamiltonian, and the subspace is the photographic film.

Last month, RIKEN and IBM demonstrated the use of SQD to simulate molecular nitrogen and two species of iron-sulfur clusters, 2Fe-S and 4Fe-2S. Their experiments used up to 77 qubits of the IBM Quantum Heron processor running up to 3,500 two-qubit gates alongside the supercomputer Fugaku to simulate the molecules. These quantum-centric computations went beyond the limit of exact classical simulability, operating at what we call "utility scale." Crucially, the expectation value of the Hamiltonian emerges as an accuracy metric, allowing researchers to rank the outputs of SQD against classical-only methods, as published in *Science Advances*.

RIKEN isn't the only group employing variational methods in the search for advantage. Researchers at the University of Tokyo are pursuing a similar method to SQD called Krylov quantum diagonalization, or KQD. As published in *Nature Communications*, the IBM and the University of Tokyo teams showed how KQD similarly begins by creating a subspace on a quantum computer and projecting a Hamiltonian of interest onto it, one more appropriate for materials science calculations. However, KQD has a powerful benefit: given some assumptions about the spacing of solutions, KQD is guaranteed to converge to the best answer for a wide range of initial guesses.

Advantage is just the start

This is a marathon, not a sprint. While IBM continues to release more performant quantum computers, it is essential that the quantum community keeps developing new algorithms – all in the name of creating the applications that will bring useful quantum computers to the world.

We believe that realizing advantage will also require the community to adopt a set of best practices. These are, first, the definition of standardized benchmarking problems with the help of classical experts to ensure that problems are relevant and fair. Second, teams must publish detailed methodologies and datasets so that they can be reproduced. And third, we must maintain open-access leaderboards to track improving computational performance.

We hope the community will work together to create and adopt these best practices while continuing their explorations to realize advantage and useful quantum computing. There's never been a better time to get started.

35. Shor's Algorithm Breaks 5-bit Elliptic Curve Key on 133-Qubit Quantum Computer

by Quantum News
https://quantumzeitgeist../shors-algorithm-breaks-5-bit-elliptic-curve-key-on-133-qubit-quantum-computer/

The security of modern digital communication relies on complex mathematical problems that are difficult for conventional computers to solve. Still, a new demonstration showcases the potential of quantum computers to break these safeguards. Tippeconnic from Arizona State University and colleagues successfully break a 5-bit elliptic curve cryptographic key, a fundamental component of many security systems, using a 133-qubit quantum computer. The team achieves this breakthrough by implementing a quantum algorithm that exploits the unique properties of quantum interference to reveal the secret key without directly encoding it within the computation, a significant step towards assessing the real-world threat posed by quantum computers to current encryption methods. This experiment, performed on an IBM quantum processor, demonstrates the ability to solve a cryptographic problem with a relatively small number of qubits and a surprisingly deep circuit, paving the way for further research into quantum-resistant cryptography.

Shor's Algorithm Breaks 5-Bit Cryptographic Key.

The experiment successfully broke a 5-bit elliptic curve cryptographic key using a quantum attack based on Shor's algorithm, executed on IBM's 133-qubit IBM_Torino processor. A key innovation lies in the method's ability to extract the secret key without directly encoding it into the quantum circuit, enhancing security against certain attacks. The approach focuses on interfering over a specific subgroup of the elliptic curve, allowing researchers to reveal key information through quantum measurement, which manifests as a distinct pattern in the quantum data. The methodology begins by mapping the points of the elliptic curve to integers, simplifying calculations while preserving the necessary mathematical relationships.

Quantum registers then represent parameters of the equation, including the exponent and a point index, initialised in a superposition of states using carefully timed pulses. A specifically constructed quantum oracle performs a reversible transformation, linking these registers through a function related to the secret key, designed to avoid directly referencing the key itself. Following the oracle's operation, the algorithm isolates a specific register, focusing on the phase relationship between registers rather than absolute values. A Quantum Fourier Transform is then applied, transforming the data into a frequency domain where the interference pattern becomes more apparent, revealing the modular phase relation and ultimately the secret key.

Classical post-processing analyses the measurement results, identifying the most likely key candidates based on the observed interference pattern. The success of the attack is demonstrated by the consistent appearance of the correct key within the top results, even in the presence of quantum noise. The experiment highlights the power of quantum interference to reveal hidden information and the potential for quantum computers to break commonly used cryptographic algorithms. Researchers emphasise that the observed interference pattern is a physically real phenomenon exploitable for cryptographic attacks.

Summary

Researchers successfully demonstrated a quantum attack on elliptic curve cryptography by breaking a 5-bit key using a modified Shor's algorithm on IBM's 133-qubit quantum processor. Despite the extreme complexity of the quantum circuit (over 67,000 layers deep), the system maintained sufficient quantum coherence to produce valid interference patterns. Classical post-processing of the quantum results correctly identified the secret key (k=7) within the top 100 candidate solutions.

The experiment validates that Shor's algorithm remains effective even with very deep quantum circuits, suggesting potential scalability for attacking larger cryptographic keys. The approach used modular arithmetic techniques to encode the problem without directly referencing the secret key, and visualization of the results confirmed the expected quantum interference patterns.

36. Quantum code breaking? You'd get further with an 8-bit computer, an abacus, and a dog

by Thomas Claburn
https://www.theregister.com/2025/07/17/quantum_cryptanalysis_criticism/

The US NIST has been pushing for the development of post-quantum cryptographic algorithms since 2016.

"If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use," NIST explains in its summary of Post-Quantum Cryptography (PQC).

Peter Gutmann, a professor of computer science at the University of Auckland New Zealand, thinks PQC is bollocks – "nonsense" for our American readers – and said as much in a 2024 presentation, "Why Quantum Cryptanalysis is Bollocks."

Gutmann's argument is simple: to this day, quantum computers – which he regards as "physics experiments" rather than pending products – haven't managed to factor any number greater than 21 without cheating.

Quantum computers and PQC are both enormously complex. But the common process for cracking RSA public key encryption is relatively straightforward. Given a key pair modulus n, you have to factor it into two prime numbers, p and q, such that $n = p \times q$.

When n is 21, p could be 3 and q could be 7, for a not very secure 5-bit RSA implementation. But when n is a 1024-bit or 2048-bit number, finding two prime factors requires a tremendous amount of computational power.

NIST's concern, raised by many computer scientists, is that a quantum computer might one day be capable of running Shor's algorithm, which is essentially a shortcut to find the prime factors of a large integer. Were that to happen, data protected by insufficiently complex encryption keys would be at risk of exposure. To avoid that purported possibility, the US standards organization has been shepherding the development of various quantum-resistant encryption algorithms, such as HQC (Hamming Quasi-Cyclic), CRYSTALS-Kyber, CRYSTALS-Dilithium, Sphincs+, and FALCON. These are being positioned as replacements for current algorithms like RSA.

NIST, which did not immediately have someone available for comment, says some engineers claim quantum code-cracking could be a thing within two decades. Since that's about as long as the deployment of modern public key infrastructure has taken, the standards body argues it's time to start preparing.

Judging by the present state of quantum computers, the case for new algorithms looks less compelling. In a tongue-in-cheek paper released in March, Gutmann and co-author Stephan Neuhaus, senior lecturer of computer science at the Zurich University of Applied Sciences, argue that it's possible to replicate the code-cracking capabilities of current quantum computers with a VIC-20 8-bit home computer from 1981, an abacus, and a dog.

The paper notes that IBM in 2001 implemented Shor's algorithm in a seven-qubit quantum computer, demonstrating the factorization of the number 15. A decade later, researchers managed to use a quantum

computer to factor the number 21. IBM tried to factor 35 in 2019 but basically failed – the algorithm worked 14 percent of the time due to rampant qubit errors.

Researchers affiliated with Shanghai University claim to have used a quantum computer from D-Wave, which specializes in quantum annealing computers tuned for specific optimization problems, to have factored a 2,048-bit RSA integer.

But according to Gutmann and Neuhaus, the RSA number evaluated was the product of two prime factors that were too close together.

As with a parlor magician's card deck that's been stacked for a card trick, the computer scientists explain in their paper: "Quantum factorization is performed using sleight-of-hand numbers that have been selected to make them very easy to factorize using a physics experiment and, by extension, a VIC-20, an abacus, and a dog."

"Since n (public key) $= p \times q$, the square root of n will give you p and q to within one or two bits if there's only one or two bits difference between them," Gutmann told *The Register*. "This is why standards for RSA, like FIPS 186 which the paper references, require that they differ by at least 100 bits, i.e. that they're 2^{100} (1.3×10^{30}), which Google tells me is called a nonillion) or more apart so you can't get an approximation to them using a square root operation."

An analog in the AI world would be touting the benchmark testing prowess of an AI model trained on the questions in benchmark tests.

Trevor Lanting, chief development officer at D-Wave, told *The Register*: "Based on our assessment, this research does not represent a new fundamental breakthrough in capability, it's an exploration of some previous work in using annealing QC to factor small numbers. The research explores factoring capability, which we've long said is a problem set that both annealing and gate model quantum systems could address.

"Breaking modern encryption would require quantum processors many orders of magnitude larger than today's scale: there will be no threat to encryption for many years. Moreover, there are post-quantum encryption protocols available. D-Wave does not specifically focus on cryptography, but our technology has been used to power intrusion and threat detection applications."

Amid claims of "quantum supremacy" by Google, Microsoft's disputed Majorana breakthrough, University of Illinois computer science professor Daniel Bernstein's arguments that quantum computers shouldn't be written off, and University of Texas computer scientist Scott Aaronson's view that quantum computing "is on the threshold of becoming real," Gutmann remains skeptical that anyone will be doing any meaningful code cracking with "physics experiments" any time soon.

The Register asked Gutmann to elaborate on when the implausibility of quantum cryptanalysis became apparent.

"There wasn't really any specific time, although it has become more and more obvious over time, with the failure of any genuine (non-sleight-of-hand) quantum cryptanalysis to appear, that it's about as real as fusion-powered electricity too cheap to meter and all the other decades-old tech pipe dreams," Gutmann explained.

"I'm an empirical gnostic, and with standard crypto that works well, it's based on mathematics and engineering, we can look at the math and look at the engineering (computing power and so on) and draw a line through the data points on a graph and say 'this will be good until about this time.'

"PQC on the other hand isn't mathematics or engineering, it's augury: 'A great machine shall arise, and it will cast aside all existing cryptography, there shall be Famine, Plague, War, and a long arable field.'

"The Bollocks talk drew a line through the two PQC data points we have which indicate that we'd get to the same level of code breaking that we have today with standard computers in about 2,000 years' time, but even those data points are from sleight-of-hand factorizations, not legitimate applications of Shor's algorithm to recover two unknown factors as needed to break RSA (this is why in the paper we suggest evaluation criteria for quantum cryptanalysis claims that should be resistant to sleight-of-hand tricks).

"In practice we have zero data points, which is pretty good evidence that we're not getting anywhere with physics experiment-based cryptanalysis."

Gutmann added as an aside that we also have the same number of data points for faster-than-light space travel, Star Trek-style transporters, and any number of other high-tech dreams.

Asked whether his skepticism of PQC extends to quantum computers in general, Gutmann said The Australian Strategic Policy Institute addressed the matter better than he could:

Contrary to popular claims, quantum algorithms don't 'try all solutions at once.' Instead, they carefully manipulate qubits to amplify the probability of measuring a useful answer at the output, while suppressing the probability of measuring any other answer. It's roughly similar to a magician's card trick: rather than checking every card in the deck for the one that was chosen, the magician uses a clever sequence of steps to make the chosen card more likely to appear without actually knowing what it is.

Compared to classical algorithms, quantum algorithms can more effectively scale with problem size. This means that for a sufficiently large problem, they may be able to compute an answer more efficiently – in time, energy or cost – than classical alternatives. For smaller problems, it is likely that classical computers will retain a clear comparative advantage for the foreseeable future due to the overheads in quantum computing.

We inquired how IT security professionals should interpret the move to "Post-Quantum Cryptography" and whether there's anything to be gained from the transition.

"No, in fact there's a lot to be lost," Gutmann replied. "We currently have a multibillion-dollar global cybercrime industry that's built on the failure of encryption to provide the protection that it's supposed to, and instead of fixing that problem we're investing a vast amount of effort into swapping out our crypto for new stuff that's inefficient and difficult to work with and that offers no more protection than the old stuff (there's a reason why it had been ignored for decades before quantum cryptanalysis came along to give it a reason to exist, it's really not very practical or usable). Switching to PQC is just a distraction from having to fix the actual hard problem."

37. The future of encryption in a post-quantum world

by Ian Barker
https://betanews.com/2025/07/17/the-future-of-encryption-in-a-post-quantum-world/

As **quantum** computing speeds edge closer to practical use, the 'harvest now, decrypt later' approach is already in motion with adversaries collecting encrypted data today, anticipating they'll be able to crack it tomorrow. But is enough being done to prevent it?

New research from Forescout highlights the urgent need for organizations to prepare for a future where quantum-capable adversaries can break widely used cryptographic protocols.

The report finds that only about six percent of all 186 million SSH servers on the internet already use quantum-safe **encryption**. Three quarters of OpenSSH versions on the internet still run versions released between 2015 and 2022 that do not support quantum-safe encryption. In addition less than 20 percent of TLS servers use TLSv1.3, which is the only version that supports PQC.

If, as seems likely, regulators mandate quantum-safe encryption in the near future, organizations will face serious gaps. Current quantum migration roadmaps throughout the world mandate transitioning to PQC between 2030 and 2035, especially for critical assets. Outdated infrastructure will become a compliance and security risk, and upgrading later may be slower, more expensive, and more disruptive than acting early.

Rob McNutt, chief strategy officer at Forescout, writes on the company's blog, "Today's encryption standard, PKI, still matters and will continue to matter in the future but it will diminish in its ability to be trusted. Certificates, certificate authorities, and TLS will still rely on PKI but other technologies like SKA or post-quantum key exchange platforms will likely become a trend. PKI updates to the key exchange and the signature algorithms will be needed to ensure they are quantum safe, which is a tall task for the 10B+ connected devices in the world."

You can read more on the Forescout blog. The company has also launched the Forescout 4D Platform which continuously identifies, protects and ensures the compliance of all managed and unmanaged cyber assets -- IT, IoT, IoMT and OT -- without business disruption. It delivers comprehensive capabilities for network security, risk and exposure management, and extended detection and response.

38. Post-Quantum Cryptography Plugin Secures DNSSEC Against Future Attacks

by Rusty Flint
https://quantumzeitgeist.com/post-quantum-cryptography-plugin-secures-dnssec-against-future-attacks/

The security of the internet's fundamental infrastructure faces an evolving threat as quantum computers become increasingly powerful, potentially breaking the cryptographic algorithms that underpin secure communications. Julio Gento Suela, Javier Blanco-Romero, and Florina Almenares Mendoza, all from the Telematic Engineering Department at the University Carlos III of Madrid, alongside Daniel Díaz-Sánchez

and colleagues, address this challenge by integrating quantum-resistant cryptographic algorithms into CoreDNS, a widely used DNS server. Their work demonstrates the first practical implementation of post-quantum DNSSEC, enhancing the security of the Domain Name System against future attacks. By developing a plugin supporting multiple new signature schemes, the researchers show it is possible to upgrade existing DNS infrastructure and maintain compatibility while preparing for a post-quantum world, even though this introduces performance trade-offs that require careful consideration.

Quantum Threat Drives Post-Quantum Cryptography Transition

The internet relies on secure communication, and cryptography is fundamental to that security. Current cryptographic methods, like RSA and ECC, face a potential threat from future quantum computers, which could compromise online security within the next decade.

This vulnerability demands a proactive shift towards post-quantum cryptography (PQC), developing new algorithms resistant to attacks from both conventional and quantum computers. Organizations like the National Institute of Standards and Technology (NIST) are leading this transition, standardizing new PQC algorithms to ensure continued data security.

A critical component of internet infrastructure is the Domain Name System (DNS), which translates website addresses into numerical addresses computers use. DNSSEC adds a layer of security to DNS, authenticating data and protecting against manipulation.

Integrating PQC into DNSSEC is crucial given the vulnerabilities of current implementations. Integrating PQC into DNSSEC presents challenges, particularly concerning the increased size of PQC signatures and keys compared to traditional methods. This larger size impacts data transmission efficiency and server memory requirements.

Researchers are addressing this challenge by integrating PQC algorithms into CoreDNS, a widely-used DNS server often deployed in modern containerized environments. Their work focuses on implementing several PQC signature algorithm families, including FALCON, ML-DSA, SPHINCS+, MAYO, and SNOVA, within CoreDNS, extending its functionality while maintaining compatibility with existing DNS resolution processes.

This allows for on-the-fly signing of DNS data using quantum-resistant signatures, paving the way for a more secure DNS infrastructure. The research demonstrates that while PQC algorithms introduce operational overhead, several candidates offer viable compromises for transitioning DNSSEC to quantum-resistant cryptography.

By testing these algorithms within a real-world DNS server environment, the team provides valuable empirical data for algorithm selection and deployment planning, helping to ensure a smooth and secure transition to a post-quantum internet.

DNSSEC Transition, Increased Signature and Key Sizes

Experimental support for Post-Quantum (PQ) algorithms is currently limited in widely-used DNS software like BIND9. This presents unique challenges for the transition to post-quantum cryptography in DNSSEC, particularly regarding the size of post-quantum signatures and keys.

These signatures and keys can be significantly larger than those generated with traditional algorithms, impacting the efficient transmission of data and increasing memory requirements for servers and DNS resolvers, often necessitating the use of TCP, which introduces additional latency. Before large-scale deployment, testing tools are needed to evaluate the performance and compatibility impact of integrating these new algorithms into real systems.

Controlled testing environments help identify potential issues and ensure that migration to PQ algorithms does not compromise system security or operability. This paper describes the integration of standard and candidate algorithms from the second NIST round for signatures, of post-quantum algorithm families (FALCON, ML-DSA, SPHINCS+, MAYO, and SNOVA) into CoreDNS, a widely-used DNS server in Kubernetes environments developed in Go.

This implementation extends existing work by providing empirical performance data across a broader range of PQC algorithms, enabling comparative analysis for algorithm selection and deployment planning in containerized DNS environments.

Viable Quantum-Resistant DNSSEC Algorithms Identified

Results indicate that several PQC candidates offer viable compromises for transitioning DNSSEC to quantum-resistant cryptography. The performance evaluation demonstrates that these algorithms, despite their computational demands, present feasible options for enhancing DNS security and achieving quantum resistance.

This work contributes to the ongoing effort of securing digital signatures and critical internet infrastructure against future quantum computing threats.

Post-Quantum DNSSEC Plugin for CoreDNS

Traditional algorithms like RSA and ECDSA are being evaluated alongside post-quantum candidates to determine the best path forward for secure DNS resolution. A dnssec_pqc plugin was developed for CoreDNS to integrate post-quantum cryptographic algorithms, extending the existing DNSSEC plugin while maintaining compatibility and minimizing interference.

This plugin leverages the liboqs library through Go bindings, enabling access to a range of post-quantum primitives. Eighteen algorithms were evaluated, including 13 post-quantum (Falcon-512, ML-DSA-44, SPHINCS+-SHA2-128s-simple, MAYO-1, Falcon-1024, ML-DSA-65, SPHINCS+-SHAKE-128s-simple, MAYO-3, Falcon-padded-512, ML-DSA-87, Falcon-padded-1024, SNOVA_24_5_4, SNOVA_24_5_4_SHAKE) and 5 traditional (RSA-2048, RSA-4096, ECDSA-P256, ECDSA-P384, Ed25519), measuring signing time, resolution latency, CPU usage, memory consumption, and DNS response size.

Testing was conducted on an Ubuntu 24.04.2 LTS system with an Intel Core i7-10870H processor and 16 GB of RAM. Functional tests confirmed correct DNS response generation with post-quantum signatures. Key findings include: SNOVA, MAYO-1, and ML-DSA-44 exhibited competitive signing times (below 25 ms), while SPHINCS+ variants were significantly slower, reaching up to 2.6 seconds for SPHINCS+-SHAKE-128s-simple.

All post-quantum algorithms required TCP due to exceeding UDP size limits, resulting in latencies around 101.5 ms, with SPHINCS+ algorithms exhibiting the highest latencies. ECDSA-P256 and Ed25519 demonstrated the lowest CPU consumption, while SPHINCS+ variants were the most CPU-intensive.

Post-quantum algorithms increased memory consumption by approximately 3-4 MB compared to traditional algorithms. SNOVA produced the smallest responses, followed by Falcon-512 and MAYO-1, while ML-DSA-87 and Falcon-1024 generated the largest responses. This work demonstrates the feasibility of integrating post-quantum cryptography into a widely used DNS server.

Algorithms like SNOVA, MAYO-1, and Falcon-512 offer a balance between performance and security, while SPHINCS+ variants present significant performance challenges. The need for TCP due to increased response size is a critical consideration for deployment.

Future research should focus on algorithm optimization to reduce signing time, CPU usage, and response size, investigating hybrid cryptographic schemes, conducting comprehensive network impact analysis, exploring hardware acceleration, and contributing to standardization efforts.

39. Post-Quantum Cryptography Algorithms Deployed on Resource-Constrained IoT Devices

by Quantum News
https://quantumzeitgeist.com/post-quantum-cryptography-algorithms-deployed-on-resource-constrained-iot-devices/

The increasing power of computers presents a growing danger to the encryption methods that currently secure much of our digital world, especially for the billions of connected devices in the Internet of Things. Jesus Lopez, Viviana Cadena, and Mohammad Saidur Rahman, from the University of Texas at El Paso, and their colleagues, address this challenge by evaluating whether new, quantum-resistant cryptographic algorithms can run effectively on devices with limited processing power and energy. Their work demonstrates the practical feasibility of implementing these next-generation algorithms – specifically BIKE, CRYSTALS-Kyber, and HQC – on a standard Raspberry Pi platform. This research is significant because it confirms that it *is* possible to safeguard future IoT networks against the threat of quantum computers, paving the way for resilient security in the next generation of connected devices.

The proliferation of Internet of Things (IoT) devices introduces significant security vulnerabilities, as current cryptographic methods are increasingly threatened by the rapid advancement of quantum computing. A powerful quantum computer could compromise the confidentiality and integrity of data transmitted by these devices, particularly as many have limited processing power, memory, and energy. Researchers are therefore focused on post-quantum cryptography (PQC) – developing algorithms resistant to attacks from both classical and quantum computers.

Recent work has systematically evaluated three promising PQC algorithms – BIKE, CRYSTALS-Kyber, and HQC – on Raspberry Pi-based platforms to assess their feasibility for resource-constrained devices. The team measured execution time, power consumption, memory usage, and device temperature to determine

performance characteristics. Results indicate that CRYSTALS-Kyber offers the most favorable balance of these metrics, making it a strong candidate for securing future IoT deployments.

While BIKE demonstrated the lowest memory usage, it incurred substantial latency and power costs at higher security levels, and HQC demanded significant memory and generated considerable heat. These findings highlight the trade-offs inherent in different PQC algorithms and provide valuable guidance for developers building quantum-resistant IoT devices. The National Institute of Standards and Technology (NIST) has been actively involved in standardizing these new algorithms, recently releasing its first three finalized post-quantum encryption standards – a crucial step towards securing future communications.

Research has focused on adapting the Transport Layer Security (TLS) protocol to incorporate post-quantum security, with Kyber emerging as a leading candidate due to its promising performance. Demonstrations of practical implementations confirm that integrating PQC algorithms on constrained hardware is indeed feasible, reinforcing the urgent need for quantum-resilient cryptographic frameworks in next-generation IoT devices. This work contributes to the growing body of knowledge surrounding quantum-secure communication and its application to resource-limited devices, and the implementation is publicly available to facilitate further research and development.

Ultimately, balancing cryptographic strength with system-level constraints is critical when selecting PQC algorithms for future deployments at scale.

40. How CISOs can prepare for the quantum cybersecurity threat

by Kyle Johnson
https://www.techtarget.com/searchsecurity/feature/How-CISOs-can-prepare-for-the-quantum-cybersecurity-threat

Quantum computing will mark a revolutionary change in modern computing, as well as a pivotal shift in cybersecurity. As these powerful machines make their way from theory to reality, they threaten to unravel the encryption algorithms that organizations have relied on for years to protect their data and communications systems.

Industry experts and government agencies, such as NIST, the U.S. Department of Homeland Security and the U.K.'s National Cyber Security Centre, have all sounded the alarm: CISOs, the time to start preparing for quantum computing is now.

Let's look at how quantum computing threatens cybersecurity and how CISOs should start their post-quantum migration.

How quantum computing disrupts traditional cybersecurity

While quantum computers won't replace classical computers, per se, they will complement them and excel at certain tasks. For example, due to a fundamental principle of quantum mechanics called superposition, qubits -- unlike classic bits -- can be both 1 and 0 at the same time or anything in between until measured.

This enables quantum computers to solve complex mathematical problems much faster than classical computers.

Currently, however, qubits are fragile and error-prone because they are vulnerable to heat, vibrations and even cosmic radiation. However, scientists are on their way to developing more resilient and capable quantum computers. While the exact date is unknown, experts estimate it to be between 2030 and 2050.

The benefits of quantum computing's speed and power come at a price: security.

Long-relied-upon cryptographic algorithms that have kept business-critical and personal data safe for decades will soon be broken. A cryptographically relevant quantum computer -- one capable of cracking cryptographic algorithms -- can compromise asymmetric cryptography, also known as public key encryption. Specifically, using Shor's algorithm -- a quantum algorithm that finds the prime factor of an integer -- will make it possible to break this type of encryption in a matter of hours or even minutes if the quantum computer is large enough.

With asymmetric algorithms, such as the commonly used Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC), becoming vulnerable, organizations face the following threats:

- **Weakened secure communications.** Secure communications that use asymmetric encryption, such as TLS, HTTPS and VPNs, will become vulnerable to eavesdropping and interception.
- **Increased difficulty securing IoT devices.** Many IoT and embedded devices don't have the memory or compute power to accommodate post-quantum cryptography (PQC) algorithms, leaving them vulnerable to attack.
- **Impersonated digital signatures.** Digital signatures that rely on asymmetric cryptography can be forged, enabling malicious actors to create fraudulent documents and transactions.

Another threat presented by quantum computing is harvest now, decrypt later attacks. These involve malicious actors exfiltrating encrypted data now with the intent of decrypting it when quantum computers are more readily available.

CISO action plan: A post-quantum computing roadmap

Quantum preparedness isn't achieved overnight. Ideally, CISOs should start the process now and roll it out in three key phases.

Short-term: Preparation

Over the next one to three years, CISOs should assess their current IT systems and cryptographic use. This involves the following steps:

- **Create a migration team.** Build a team and appoint a team leader to manage the PQC migration. Include relevant stakeholders from business units beyond cybersecurity. This team is responsible for ensuring the migration remains on time and within budget.
- **Inventory and classify data.** Conduct an inventory of all data held by the organization. Classify data based on how it is currently encrypted and whether it requires encryption in the future. Not all data

requires quantum-safe encryption. Consider which data needs to remain protected in five to 10-plus years, i.e., the data susceptible to harvest now, decrypt later attacks.

- **Determine cryptographic use.** Review where and what types of cryptographic algorithms are in use. Create a cryptographic bill of materials (CBOM) to inventory cryptographic algorithms within hardware, firmware and software components.
- **Understand potential future exposure.** Use the CBOM to identify the assets using asymmetric cryptographic algorithms that will be exposed. Analyze the following:

  ★ How PQC will affect current systems.
  ★ Which legacy tools and systems aren't capable of switching to PQC algorithms.
  ★ Whether new tools need to be adopted.
  ★ Which existing software needs to be deprecated.

Perform a risk assessment to discern which data, systems, controls and policies to prioritize and protect first during the transition. This risk assessment also affects which PQC algorithms to choose.

- **Select and test PQC algorithms.** Research and select the most suitable PQC algorithms based on the inventory and assessments. NIST has vetted and approved the following PQC algorithms:

  A. **ML-KEM.** Module-Lattice-Based Key-Encapsulation Mechanism is a lattice-based algorithm based on the CRYSTALS-Kyber algorithm.
  B. **ML-DSA.** Module-Lattice-Based Digital Signature Algorithm is a lattice-based algorithm for securing digital signatures based on CRYSTALS-Dilithium.
  C. **SLH-DSA.** Stateless Hash-Based Digital Signature Algorithm, based on the Sphincs+ stateless hash-based signature scheme, is intended as a backup for ML-DSA.
  D. **FALCON.** Fast Fourier Lattice-Based Compact Signatures Over NTRU is a lattice-based algorithm for digital signatures.
  E. **HQC.** Hamming Quasi-Cyclic, which has not been finalized, is a code-based algorithm for key exchange for both classical and quantum computers that is intended to be a backup for ML-KEM.

- **Finalize budget and tool needs.** CISOs should estimate PQC migration costs and determine a realistic budget. Allocate resources to secure the most at-risk data first, with the longer-term goal of migrating all systems.

- **Educate users organization-wide.** With initial efforts for a post-quantum journey complete, educate employees on quantum computing's impact on cybersecurity. Cover how corporate policies and procedures will be updated to mitigate quantum computing threats and outline changes to expect over the coming decade.

Mid-term: Planning and execution

Where the short-term phase focused on inventorying data and encryption use, the mid-term phase covers the start of implementation. In the next three to five years, CISOs should do the following:

1. **Assess vendor PQC capabilities.** Vet the quantum computing security efforts of current and potential vendors. Evaluate how they currently protect data and what their roadmap is for the next five to 10-plus years. Many vendors are already rolling out quantum-safe tools and systems.

2. **Determine supply chain risk.** Evaluate how third parties with access to the organization's data are preparing for PQC to determine future needs and relationships. For example, consider cutting ties with third parties that are not conducting post-quantum migration efforts.

3. **Update security policies and plans.** Create or update policies and procedures to account for PQC needs. These might include data security policies, incident response plans and disaster recovery plans.

4. **Update infrastructure based on risk.** Begin migrating to the chosen PQC algorithms and secure data according to the quantum risk assessment. Consider a layered strategy that uses PQC algorithms and quantum-safe systems and tools alongside existing cryptographic standards.

Other key quantum computing security strategies to research include the following:

- **Quantum key distribution.** QKD enables the exchange of encryption keys for secure communications. It uses quantum mechanics to protect keys from interception and eavesdropping.

- **Quantum random number generators.** QRNGs use quantum mechanics to create unpredictable encryption keys. They enhance the security of communications, transactions and data.

Crypto-agility. Becoming crypto-agile involves systems and infrastructure dynamically shifting between PQC algorithms. It enables systems to switch PQC algorithms in the event one becomes compromised.

Long-term: Monitoring and evaluation

At this point, the most critical data and cryptography systems should be updated. Now it's time for CISOs to implement a multiyear quantum-safe infrastructure strategy across the entire organization.

PQC migrations are complex and time-consuming. They will be a long-term focus for organizations. The goal is to adopt quantum-safe tools and infrastructure across all systems -- something that might take more than 10 years to complete.

Long term, plan for the following:

- **Migrate low-risk systems.** Continue the migration process for all systems, data and processes.
- **Assess migration efforts.** The migration team should monitor and measure the effectiveness of the migration. Is everything going according to the planning stages? Or does the team need to adjust something?
- **Update inventories and CBOMs.** Continue to update the data inventory and CBOMs as new systems and tools are migrated or adopted.
- **Monitor security threats.** Stay apprised of emerging quantum computing threats and create mitigation plans.
- **Maintain compliance.** Review relevant standards and regulations for PQC requirements to meet compliance mandates.

41. The Quantum Imperative: Securing Digital Trust in a Post-Quantum World

by Amaanie Hakim
https://www.thefastmode.com/expert-opinion/43236-the-quantum-imperative-securing-digital-trust-in-a-post-quantum-world

In June 2024, the United Nations declared 2025 as the International Year of Quantum Science and Technology, placing the spotlight on a domain poised to redefine science, security, and global systems. This global recognition affirms the accelerating relevance of quantum advancements and the urgency with which governments, industries, and society must prepare for a quantum-enabled future.

Among the most transformative aspects of this shift is the rise of quantum computing. According to McKinsey, quantum technologies could generate as much as $1.3 trillion in value by 2035. Yet, alongside this promise lies a pressing dilemma: how to protect the foundational structures of today's digital security – particularly cryptography – from the disruptive power of quantum capabilities.

The present threat – post-quantum security realities

The threat posed to cryptographic systems, which currently secure everything from financial transactions to national infrastructure, should not be underestimated. As quantum computing matures, the timeline to address post-quantum cryptographic risks continues to compress. A growing body of research underscores the urgency to act now to ensure sensitive data and transactions remain protected both today and into the quantum future. Among the most critical concerns to be addressed in today's cryptographic systems are:

- **Harvest now, decrypt later**: malicious actors are already storing encrypted data today, with the expectation that quantum computing will enable them to decrypt it. This strategy poses risks to both current and historical data privacy.
- **Breakage of current cryptographic standards**: Most public-key encryption methods in use today, such as RSA and ECC, could be rendered obsolete by large-scale quantum computers.
- **Long-lifespan device exposure**: IoT devices like payment terminals, connected vehicles, and smart meters may remain operational for a decade or more. If deployed without quantum-resilient protection, these devices could become critical security liabilities in the near future.
- **Lack of crypto-agility**: Many systems lack the flexibility to quickly and securely upgrade to new cryptographic protocols, leaving them exposed during the transition to post-quantum security.

Addressing these concerns requires urgent, coordinated action from both public and private sectors. As telecom and financial systems grow more interconnected and digitized, the need to safeguard digital transactions from future quantum threats becomes paramount.

Across the digital trust ecosystem, key innovators are already investing in forward-looking technologies, from crypto-agility frameworks to quantum-safe transaction protocols, to futureproof against the looming risks. Notable recent developments include the release by IDEMIA Secure Transactions of next-generation crypto-agility solutions, participation in large-scale collaborative quantum security initiatives, and the world's first demonstration of a quantum-resistant offline central bank digital currency (CBDC) payment.

These advances not only demonstrate technical feasibility but also set the stage for a proactive transition into the post-quantum era.

From theory to tangible solutions: post-quantum cryptography in action

In recent years, the focus has shifted from theoretical debates to practical implementations of quantum-safe cryptography. Organizations at the forefront of digital trust are deploying cryptographic tools that can withstand both classical and quantum attacks, ensuring business continuity and data security in a changing threat landscape.

Notable recent developments include:

- **Crypto-agility solutions**: Newly launched tools enable secure and scalable migration from classical to post-quantum cryptographic algorithms. These systems are designed to ensure uninterrupted transaction security, even as cryptographic standards evolve.
- **Quantum-resistant CBDC demonstration**: A world-first demonstration of an offline CBDC transaction protected against quantum threats illustrates how central banks and digital finance ecosystems can innovate securely in a post-quantum world.
- **Cross-industry quantum security collaboration**: Participation in international consortia and joint R&D efforts reflects a growing recognition that no single entity can tackle this challenge alone. Shared knowledge and standards, through partnerships and collaborations with universities or through the development of global standard algorithms with the US National Institute of Standards and technology (NIST), will be vital for large-scale adoption.

These initiatives are essential building blocks for a secure digital future. They demonstrate that quantum security is not just a theoretical ideal, but an attainable and increasingly necessary reality.

A call for proactive action

The post-quantum era is fast approaching, and with it, a decisive opportunity to build more secure, trustworthy digital ecosystems. A strategic roadmap for innovation, such as those focusing on the future of communications, payments and digital identity, highlights the priorities that must guide this transformation: crypto-agility, cross-sector collaboration, and continuous investment in scalable, quantum-safe solutions.

Organizations, especially those handling high-value or sensitive digital transactions, must act now. Governmental agencies around the world are already encouraging this transition, recognizing the long-term threat quantum computing poses to current cryptography methods. Integrating post-quantum cryptographic tools, investing in future-ready infrastructure, and participating in global standard-setting efforts will be critical steps in this journey.

The ability to adapt cryptographic systems swiftly and securely will define the resilience of tomorrow's digital platforms. But more than a defensive necessity, the transition to post-quantum security represents a chance to fundamentally strengthen the privacy, reliability, and inclusiveness of digital services for all.

It is not just about reacting to a future threat, but seizing a present opportunity to secure digital trust for generations to come.

42. MeitY and CERT-In Launch Quantum Cyber Readiness Whitepaper: What It Means for India's Digital Future

https://the420.in/meity-certin-quantum-cybersecurity-whitepaper-encryption-readiness-india/

India, a global leader in digital payments and online public services, faces an urgent new challenge—preparing for the cybersecurity risks posed by quantum computing. Recognizing that conventional encryption methods such as RSA and ECC may soon become obsolete, the Ministry of Electronics and Information Technology (MeitY), the Indian Computer Emergency Response Team (CERT-In), and SISA have launched a whitepaper titled "*Transitioning to Quantum Cyber Readiness*".

This whitepaper offers a roadmap for organizations, especially in sectors like BFSI, healthcare, civil infrastructure, and defense, to begin transitioning toward quantum-resilient encryption models before traditional algorithms are compromised.

Anticipating the Inevitable: Bringing Forward the Risk Horizon

The whitepaper warns that advancements in quantum computing will soon make it possible to break traditional encryption. As digital-first economies like India become increasingly reliant on online data exchanges and financial transactions, the implications of quantum threats are severe.

The document lays out practical steps for public and private organizations to assess their current cryptographic systems and begin migrating to post-quantum cryptography. It emphasizes proactive preparedness by aligning compliance, operational continuity, and cybersecurity risk management with the evolving digital landscape.

Voices of Leadership: Strategic Imperatives from MeitY and CERT-In

Shri S. Krishnan, Secretary of MeitY, emphasized during the launch, *"Quantum readiness is a strategic imperative as we prepare for the disruptive potential of quantum technologies, especially in cybersecurity. This whitepaper provides the right ingredients to build resilience in India's digital and AI-driven future."*

Dr. Sanjay Bahl, Director General of CERT-In, highlighted the collaborative nature of the initiative, stating, *"CERT-In recognizes that quantum computing will fundamentally change the threat landscape. We must evolve our security frameworks to protect India's expanding digital infrastructure. Our partnership with SISA showcases the importance of strategic public-private collaboration in building national preparedness."*

The whitepaper serves not only as a technical guideline but also as a learning document, combining strategic foresight with real-world application. It aims to foster a culture of cybersecurity maturity in regulated sectors while equipping organizations to face the quantum horizon with agility and confidence.

43. How Post-Quantum Cryptography Affects Security and Encryption Algorithms

by Oleksii Borysenko
https://blogs.cisco.com/developer/how-post-quantum-cryptography-affects-security-and-encryption-algorithms

The advent of quantum computing represents a fundamental shift in computational capabilities that threatens the cryptographic foundation of modern digital security. As quantum computers evolve from theoretical concepts to practical reality, they pose an existential threat to the encryption algorithms that protect everything from personal communications to national security secrets. Post-quantum cryptography is changing cybersecurity, exposing new weaknesses, and demanding swift action to keep data safe.

The quantum threat is not merely theoretical; experts estimate that cryptographically relevant quantum computers (CRQCs) capable of breaking current encryption may emerge within the next 5-15 years. This timeline has sparked the "Harvest Now, Decrypt Later" (HNDL) strategy, where threat actors collect encrypted data today with the intention of decrypting it once quantum capabilities mature. The urgency of this transition cannot be overstated, as government mandates and industry requirements are accelerating the timeline for post-quantum adoption across all sectors. The US government has established clear requirements through NIST guidelines, with key milestones including deprecation of 112-bit security algorithms by 2030 and mandatory transition to quantum-resistant systems by 2035. The UK has similarly established a roadmap requiring organizations to complete discovery phases by 2028, high-priority migrations by 2031, and full transitions by 2035.

The Quantum Threat Landscape

Understanding Quantum Computing Vulnerabilities

Quantum computers operate on fundamentally different principles than classical computers, utilizing quantum mechanics properties like superposition and entanglement to achieve unprecedented computational power. The primary threats to current cryptographic systems come from two key quantum algorithms: Shor's algorithm, which can efficiently factor large integers and solve discrete logarithm problems, and Grover's algorithm, which provides quadratic speedup for brute-force attacks against symmetric encryption.

Current widely-used public-key cryptographic systems including RSA, Elliptic Curve Cryptography (ECC), and Diffie-Hellman key exchange are particularly vulnerable to quantum attacks. While symmetric cryptography like AES remains relatively secure with increased key sizes, the asymmetric encryption that forms the backbone of modern secure communications faces an existential threat.

Impact on Cryptographic Security Levels

The quantum threat manifests differently across various cryptographic systems. Current expert estimates place the timeline for cryptographically relevant quantum computers at approximately 2030, with some

predictions suggesting breakthrough capabilities could emerge as early as 2028. This timeline has prompted a fundamental reassessment of cryptographic security levels:

Algorithm	Based On	Classical Time (e.g., 2048 bits)	Quantum Time (Future)
RSA	Integer Factorization	~10^{20} years (secure)	~1 day (with 4,000 logical qubits)
DH	Discrete Log	~10^{20} years	~1 day
ECC	Elliptic Curve Log	~10^{8} years (for 256-bit curve)	~1 hour

*Note: These estimates refer to logical qubits; each logical qubit requires hundreds to thousands of physical qubits due to quantum error correction.

Current Security Protocols Under Threat

Transport Layer Security (TLS)

TLS protocols face significant quantum vulnerabilities in both key exchange and authentication mechanisms. Current TLS implementations rely heavily on elliptic curve cryptography for key establishment and RSA/ECDSA for digital signatures, both of which are susceptible to quantum attacks. The transition to post-quantum TLS involves implementing hybrid approaches that combine traditional algorithms with quantum-resistant alternatives like ML-KEM (formerly CRYSTALS-Kyber).

Performance implications are substantial, with research showing that quantum-resistant TLS implementations demonstrate varying levels of overhead depending on the algorithms used and network conditions. Amazon's comprehensive study reveals that post-quantum TLS 1.3 implementations show time-to-last-byte increases staying below 5% for high-bandwidth, stable networks, while slower networks see impacts ranging from 32% increase in handshake time to under 15% increase when transferring 50KiB of data or more.

Advanced Encryption Standard (AES)

Quantum computers can use Grover's algorithm to speed up brute-force attacks against symmetric encryption. Grover's algorithm provides a quadratic speedup, reducing attack time from 2^n to roughly $\sqrt{(2^n)} = 2^{(n/2)}$.

AES Key Size	Grover's Effective Attack	Effective Key Strength
AES-128	~2^{64} operations	Equivalent to 64-bit key
AES-256	~2^{128} operations	Equivalent to 128-bit key

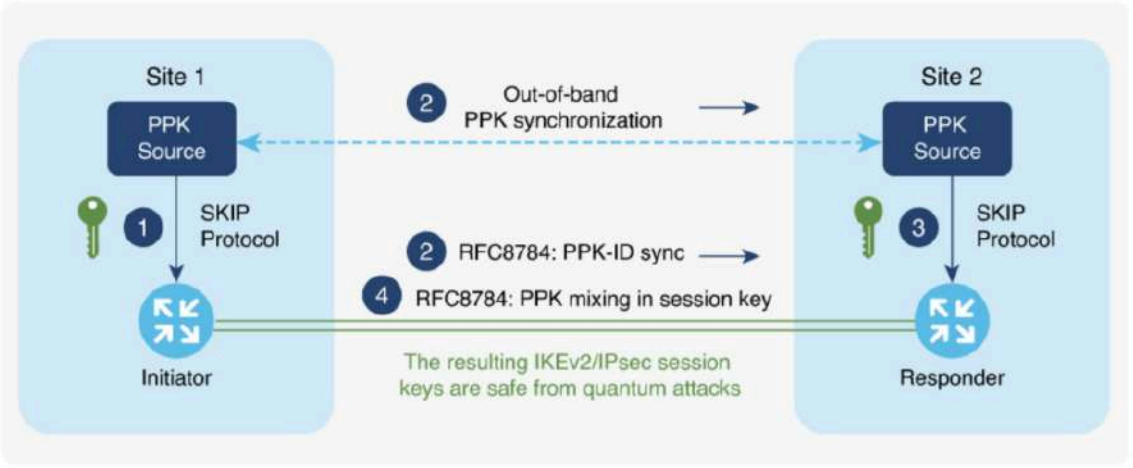
The practical implication is that quantum computers effectively halve the security strength of symmetric encryption algorithms.

IPSec and VPN Technologies

IPSec protocols require comprehensive quantum-resistant upgrades across multiple components. Key exchange protocols like IKEv2 must implement post-quantum key encapsulation mechanisms, while authentication systems need quantum-resistant digital signatures.

Cisco Secure Key Integration Protocol (SKIP) represents a significant advancement in quantum-safe VPN technology. SKIP is an HTTPS-based protocol that allows encryption devices to securely import post-quantum pre-shared keys (PPKs) from external key sources. This protocol enables organizations to achieve quantum resistance without requiring extensive firmware upgrades, providing a practical bridge to full post-quantum implementations.

Quantum-Safe IKEv2/IPsec Session Keys with Dynamic PPK



SKIP uses TLS 1.2 with Pre-Shared Key – Diffie-Hellman Ephemeral (PSK-DHE) cipher suite, making the protocol quantum-safe. The system allows operators to leverage existing Internet Protocol Security (IPSec) or Media Access Control Security (MACsec) while integrating post-quantum external sources such as Quantum Key Distribution (QKD), Post-Quantum Cryptography (PQC), pre-shared keys, or other quantum-secure methods. Cisco supports SKIP in IOS-XE.

Vulnerable Cryptographic Algorithms

RSA Encryption

RSA security relies on the difficulty of factoring large semiprime integers (products of two large primes). It is widely used for secure web communication, digital signatures, and email encryption. Asymmetric key exchange systems face significant risk from future quantum threats, as a quantum computer with sufficient quantum bits, along with improvements in stability and performance, could break large prime number factorization. This vulnerability could render RSA-based cryptographic systems insecure within the next decade.

Diffie-Hellman (DH) / DSA / ElGamal

These algorithms are based on the hardness of the discrete logarithm problem in finite fields using modular arithmetic. They are used in key exchange (DH), digital signatures (DSA), and encryption (ElGamal). Shor's algorithm can break discrete logarithm problems as efficiently as integer factorization. Current estimates suggest that DH-2048 or DSA-2048 could be broken in hours or days on a large quantum computer using approximately 4,000 logical qubits.

Post-Quantum Cryptography Standards

NIST Standardization Process

The National Institute of Standards and Technology (NIST) has finalized three initial post-quantum cryptography standards:

FIPS 203 (ML-KEM): Module-Lattice-Based Key-Encapsulation Mechanism, derived from CRYSTALS-Kyber, serving as the primary standard for general encryption. ML-KEM defines three parameter sets:

- ML-KEM-512: Provides baseline security with encapsulation keys of 800 bytes, decapsulation keys of 1,632 bytes, and ciphertexts of 768 bytes
- ML-KEM-768: Enhanced security with encapsulation keys of 1,184 bytes, decapsulation keys of 2,400 bytes, and ciphertexts of 1,088 bytes
- ML-KEM-1024: Highest security level with proportionally larger key sizes

FIPS 204 (ML-DSA): Module-Lattice-Based Digital Signature Algorithm, derived from CRYSTALS-Dilithium, intended as the primary digital signature standard. Performance evaluations show ML-DSA as one of the most efficient post-quantum signature algorithms for various applications.

FIPS 205 (SLH-DSA): Stateless Hash-Based Digital Signature Algorithm, derived from SPHINCS+, providing a backup signature method based on different mathematical foundations. While SLH-DSA offers strong security guarantees, it typically involves larger signature sizes and higher computational costs compared to lattice-based alternatives.

Implementation Challenges and Considerations

The transition to post-quantum cryptography presents several significant challenges:

Performance Overhead: Post-quantum algorithms typically require more computational resources than classical cryptographic methods. Embedded systems face particular constraints in terms of computing power, energy consumption, and memory usage. Research indicates that while some PQC algorithms can be more energy-efficient than traditional methods in specific scenarios, the overall impact varies significantly based on implementation and use case.

Key Size Implications: Many post-quantum algorithms require significantly larger key sizes compared to traditional public-key algorithms. For example, code-based KEMs like Classic McEliece have public keys that are several hundred kilobytes in size, substantially larger than RSA or ECC public keys. These larger key sizes

increase bandwidth requirements and storage needs, particularly challenging for resource-constrained devices.

Integration Complexity: Implementing post-quantum cryptography requires careful integration with existing security protocols. Many organizations will need to operate in hybrid cryptographic environments, where quantum-resistant solutions are integrated alongside classical encryption methods during the transition period.

44. Post-quantum cryptographic inventory – the latest PQC buzzword and why you need to know it

by Stefanie Schappert
https://cybernews.com/security/post-quantum-encryption-transition-cryptographic-inventory-q-day-explainer/

As the security industry braces itself for a post-quantum world – and the dreaded changeover of pretty much every piece of encrypted technology in existence – there's a new buzzword coming to town, and it's called "cryptographic inventory." Cybernews explains what it is and why you'll be hearing about it for the next 10 years.

Have you heard of Q-day? It's the day when quantum computers will be able to break even the most secure encryption algorithms in use today – algorithms such as RSA-2048 and ECC-256, that are currently protecting a large portion of the nearly 200 zetabytes of sensitive digitally stored data all over the world.

As scientists continue to get a handle on how to successfully stabilize qubits, the building blocks of quantum computers, leading experts have predicted Q-day could come anytime in the next three to fifteen years.

Security insiders warn of a quantum playground filled with savvy hackers and nation-state threat actors who have been diligently hoarding reams of encrypted data in anticipation – a tactic known as "harvest now, decrypt later." A cryptographically Relevant Quantum Computer (CRQC) attack could not only expose critical secrets but also result in a loss of trillions of US dollars.

And, citing the IBM roadmap released last month, many quantum researchers now estimate the "quantum apocalypse'"will happen less than a decade from now, by the early 2030s.

These predictions have got the Western world up in arms, with the White House and the European Union scrambling to put together their own post-quantum cryptography (PQC) roadmaps to guide government agencies, critical infrastructure, the financial and crypto sectors, as well as private and public organizations.

In fact, it was only last year that the NIST released not only the first official PQC standards guideline (Transition to Post-Quantum Cryptography Standards), but also the first three ready-to-deploy PQC algorithms, with a fourth standardized algorithm said to be on its way.

Created under a new label known as FIPS, or Federal Information Processing Standard, the finalized algorithms were chosen from 82 submissions in a process started by NIST in 2016.

So, where does cryptographic inventory fit in?

One of the core tenets of creating any cybersecurity strategy worth its salt is to start with knowing what you have.

Unless a company has a full and detailed list of its digital assets, how can it know what it needs to protect? Well, the same concept applies here.

The US, UK, and EU member states have put forth timelines where the transition to PQC algorithms must be completed for highly sensitive organizations by 2030 and all others by 2035, essentially making all current public key cryptography methods obsolete.

And, until an organization creates a comprehensive cryptographic inventory, it can not begin to prepare for a successful quantum-safe environment.

> *Cryptographic infrastructure serves as the cornerstone of the global digital ecosystem, underpinning the very essence of digital trust.* -- Cryptographic Inventory: Deriving Value Today, Preparing for Tomorrow

"Many organizations don't realize how tremendous this transition is," said Vladimir Soukharev, Vice President of Cryptographic Research and Development at InfoSec Global, a Keyfactor Company.

In a collaboration with HSBC and Thales, Soukharev is also one of the authors of the freshly published July whitepaper, "*Cryptographic Inventory: Deriving Value Today, Preparing for Tomorrow.*"

Shared exclusively with Cybernews before its formal release this week, the 31-page insider report delves into the intricacies of how a company can best tackle "today's cryptographic shortcomings while ensuring compliance and prioritising the reduction of business risk" – all within the given timeframes.

The entire process is expected to present technical challenges, impact all partners within the value chain, require substantial resources, and even then, some existing digital systems may not be able to transition to quantum-safe status, the paper states.

"Realistically, it should be done as soon as possible," Soukharev explains.

"Cryptographic transitions themselves take years to achieve. Thus, if one needs to ensure that their chances of completing it by 2030 are high, they should finish the inventory task no later than the end of 2026," he says.

Preparing for the advent of quantum computing is a major undertaking, according to the authors. By providing specific goal dates, Soukharev says companies increase their chances of completing the entire transition in time.

"If they only have the final date as their guidelines, they are very likely to underestimate the time and resources needed, leading to delays," Soukharev says.

CISOs need to start – yesterday

Designed specifically to help technology leaders such as Chief Information Officers (CIOs), Chief Technology Officers (CTOs), and Chief Information Security Officers (CISOs) understand the inventory's strategic value to overall business success, the authors say that cryptography itself can now be classified as critical infrastructure.

Besides harvest now, decrypt later threats, the research states CRQC attacks could severely impact encrypted network traffic, digital signatures and certificates, all layers of software and hardware systems, most applications, the cloud, Internet of Things (IoT), 5G, robotics, AI, blockchain, and Web3.0.

One of the more interesting aspects of the complicated process will be the need for automation, as discussed in the whitepaper.

The authors say that there will be some level of automated cryptographic discovery due to inefficient manual processes and the continuous changes occurring within an organization's infrastructure.

However, they say human management will also be required.

Very few automated platforms can handle discovery across "on-premises, cloud-native, and hybrid environments, especially with most organizations' mix of legacy systems, cloud services, and third-party applications involving a vast number of keys, certificates, algorithm instances, and protocols," it said.

The paper further explains that automation tools often have limited coverage or compatibility, may ignore some artifacts they don't understand, thus creating blind spots in the overall cryptographic visibility.

Additionally, while automation is expected to play a critical role in inventory discovery, Soukharev is less convinced that artificial intelligence can be used the same way.

"AI might possibly be able to help in the future by speeding up some subprocesses. However, cryptography is a very complicated topic, and currently, AI often provides improper, outdated, and wrong expertise around it," he says.

As for cybersecurity concerns related to the collected data, Soukharev says, "most of the time, cryptographic inventory would contain highly sensitive items, so sharing it with AI could be dangerous or possibly even out of compliance."

Furthermore, with most security leaders already aware of the risks associated with the inventory getting into the wrong hands, Soukharev says it would be imperative to only "perform data collection on premises, rather than using a SaaS approach."

45. Nearly two-thirds of organizations consider quantum computing as the most critical cybersecurity threat in 3–5 years

https://www.capgemini.com/us-en/news/press-releases/nearly-two-thirds-of-organizations-consider-quantum-computing-as-the-most-critical-cybersecurity-threat-in-3-5-years/

A Capgemini Research Institute report published today, *'Future encrypted: Why post-quantum cryptography tops the new cybersecurity agenda,'* highlights that rapid progress of quantum computing threatens to render current encryption algorithms obsolete. 'Harvest-now, decrypt-later[3]' attacks, together with tightening regulations and the evolving technology landscape, have elevated the importance of quantum safety. However, despite increasing awareness within the industry, many organizations still underestimate the risks surrounding quantum computing, which could lead to future data breaches and regulatory penalties.

According to the report, around two-thirds (65%) of organizations are concerned about the rise of 'harvest-now, decrypt-later' attacks. One in six early adopters[4] believe that 'Q-day[5]' will be within five years, while around six in ten believe it will arrive within a decade.

"Quantum readiness isn't about predicting a date–it's about managing irreversible risk. Every encrypted asset today could become tomorrow's breach if organizations delay adopting post-quantum protections. Transitioning early ensures business continuity, regulatory alignment, and long-term trust," said Marco Pereira, Global Head of Cybersecurity, Cloud Infrastructure Services at Capgemini. *"Quantum safety is not a discretionary spend but a strategic investment, which can turn a looming risk into a competitive advantage. The organizations that recognize this fact early will best insulate themselves against future cyber-attacks."*

While current quantum computers cannot break widely used encryption yet, high-risk industries such as defense and banking are leading the adoption of quantum-safe solutions. In contrast, consumer-focused sectors like consumer products and retail sectors are showing less urgency.

Post-quantum cryptography migration preferred over other quantum-security solutions

Most organizations surveyed (70%) are protecting their systems against emerging quantum threats by adopting the appropriate mix of post-quantum cryptographic (PQC) algorithms.

They view PQC as the best option to address near-term quantum security risks because it provides a comprehensive approach to securing data. Nearly half of early adopters are already exploring, assessing

[3] 'Harvest-now, decrypt-later' attacks rely on the acquisition of currently unreadable data with the possibility of decrypting it after 'Q-Day'

[4] "Early adopters," who make up 70% of our survey respondents, are organizations that are either currently working on or planning to implement quantum-safe solutions within the next five years.

[5] 'Q-Day' is the hypothetical future date when quantum computers will become powerful enough to break the crypto-graphic algorithms that currently secure most of the world's digital data and communications.

feasibility, or piloting PQC solutions. For 70% of organizations, regulatory mandates are a key driver behind the shift to PQC.

While the early adopters are working towards quantum safety, a few organizations (30%) are still ignoring the quantum threat. They are struggling to allocate sufficient budget and personnel to cryptographic transition.

Report Methodology

The Capgemini Research Institute conducted a survey of 1,000 organizations with annual revenue of at least $1 billion across 13 sectors and 13 countries in Asia–Pacific, Europe, and North America. The global survey was carried out in April–May 2025. Around 70% of the sample in this report are referred to as 'early adopters'. This segment is either working on or planning to work on quantum-safe solutions in the next five years. The survey findings were supplemented through in-depth interviews with sixteen industry executives.

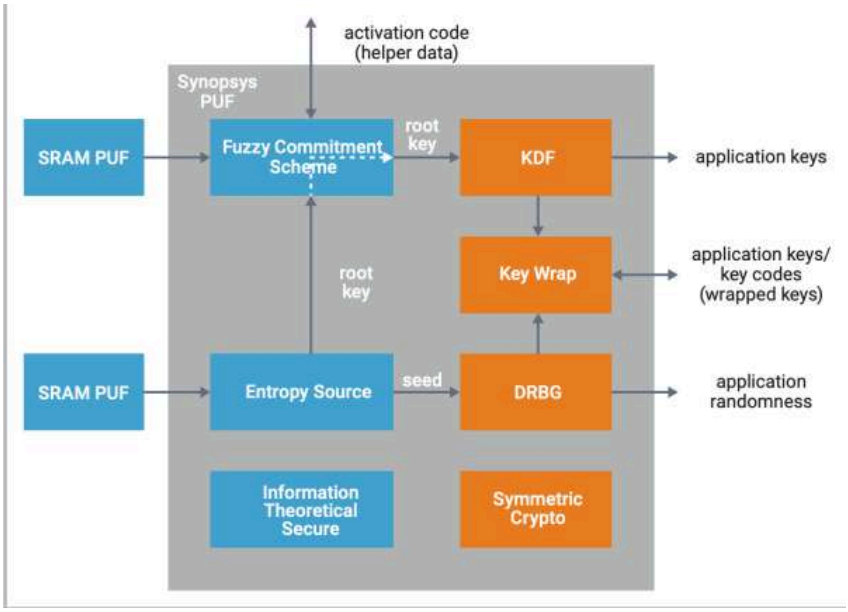
46. PUFs in a Post-Quantum World

by SYNOPSYS
https://semiengineering.com/pufs-in-a-post-quantum-world/

With the looming threat of quantum computing on the horizon, the security landscape is changing. Explore the emerging threat and its implications for current cryptographic standards. This white paper provides an in-depth analysis of quantum computing's impact on security and explains how PUF technology can help you maintain robust security in the quantum era.

Why Read This?

- **Quantum Computing Insights:** Gain a clear understanding of how quantum computers work and their potential to disrupt existing cryptographic methods.
- **Informed Decision-Making:** Discover whether you should be concerned about transitioning to post-quantum cryptography and how it impacts your systems.
- **Future-Proof Your Security:** Explore the status of PUF products in a post-quantum world and how they ensure robust security against emerging threats.



Key Takeaways:

- **Quantum Threat:** Quantum computing poses a threat to asymmetric cryptographic algorithms.
- **Sense of Urgency:** In certain cases, there can be a need to transition now to post-quantum cryptography.
- **PUF:** PUF products remain secure against quantum attacks, providing a strong starting point for your system's security.

47. Samsung One UI 8 debuts with AI-powered privacy and quantum encryption for next-gen smartphone security

by Kanika Budhiraja
https://www.livemint.com/gadgets-and-appliances/samsung-one-ui-8-debuts-with-ai-powered-privacy-and-quantum-encryption-for-next-gen-smartphone-security-11751958885891.html

The new One UI 8 update for Galaxy smartphones, which Samsung has announced, brings powerful security and privacy tools. Packed with on-device AI protections and future-ready encryption, this release is designed to help users stay safe as digital threats become more advanced and harder to detect.

One of the most important changes here is the introduction of quantum-resistant encryption across Galaxy devices. This technology is designed to protect files, messages, and passwords from hacking attempts as computers become more powerful.

The update also makes it easier to manage your data and adds stronger threat detection with Knox Matrix. Together, these improvements will help Samsung users see how their information is used and keep Galaxy devices better protected against new kinds of online threats.

The Samsung One UI 8 update also includes enhanced on-device protections that monitor for suspicious activity and help block harmful apps and phishing attempts. By running security checks directly on the device, personal information can stay under tighter control.

Knox enhanced encrypted protection secures your data

Knox Enhanced Encrypted Protection, known as KEEP, is a new system that isolates personal app data inside encrypted containers. Let me explain in a simple way: KEEP acts like a locked, secure vault inside your smartphone where all your sensitive information is stored safely. This makes it much harder for anyone to gain unauthorised access or tamper with your information.

KEEP is also closely integrated with Knox Vault, Samsung's hardware-based secure environment that protects your sensitive credit card information, passwords, and biometric data, even if the main operating system is compromised. Together, these elements allow features such as Now Brief and Smart Gallery search to work without sending user information to external servers.

In addition, KEEP also covers more tools on your phone, like Smart Suggestions. Samsung explains that this keeps your personal information stored only on your device rather than shared elsewhere. The company sees privacy as a core part of the phone's design, not just an optional setting.

Knox Matrix and Secure Wi-Fi upgrades

Samsung's Knox Matrix was originally designed to synchronise and secure multiple Galaxy devices. It has now been updated to respond to high-risk scenarios with improved detection and containment of threats across connected products like phones, tablets, and wearables. If an issue arises on one device, Knox Matrix will work to protect the rest automatically.

Secure Wi-Fi gets advanced encryption

Secure Wi-Fi has also been upgraded with advanced encryption methods designed to resist attacks, including those that could emerge with the arrival of quantum computing. This means your Wi-Fi now has much stronger security. Even if someone tries to use a powerful quantum computer in the future, they will have a hard time breaking into your connection. For example, if a hacker attempts to crack your Wi-Fi password using advanced tools, this upgrade helps keep your data secure.

System safeguards remain central

One UI 8 still includes Samsung's main security tools. Knox Vault keeps personal details like passwords and fingerprints separate from the main system. Auto Blocker stops unwanted apps and commands, and Enhanced Theft Protection adds extra checks if your phone is stolen. New Advanced Intelligence Settings let you turn off online data use for AI features. Altogether, these updates highlight Samsung's strong focus on privacy, security, and personalisation as AI becomes part of everyday life.

48. What is the future of cybersecurity?

by Karen Scarfone
https://www.techtarget.com/searchsecurity/feature/What-is-the-future-of-cybersecurity

Cybersecurity concerns continue to dominate corporate agendas, as a multitude of challenges, including generative AI-enabled attacks, ransomware extortion, supply chain risks, chronic talent shortages and security staff burnout, compound the difficulty of protecting enterprises from malicious threats.

Below are five cybersecurity trends enterprises must understand and address as they move forward.

Trend 1: AI is a double-edged sword in cybersecurity

AI technologies are already having both positive and negative effects on cybersecurity:

- **Negative effects.** Cybercriminals have been using artificial intelligence and machine learning technologies for years to help them craft increasingly sophisticated, highly customized phishing attacks, deepfake video and audio, and ransomware attacks. AI-generated attacks are much more difficult for security technologies to detect than previous attacks were. These attacks are also more likely to succeed because the use of AI can make them seem legitimate and believable.

- **Positive effects.** Although cybercriminals have a head start on defenders, organizations are starting to catch up by expanding their use of AI technologies in support of cybersecurity. Many of today's security measures employ AI to improve their capabilities, such as strengthening authentication mechanisms and access controls, detecting and analyzing cyberthreats and anomalies more quickly and accurately, and automating responses to security incidents so incidents are stopped faster, reducing damage and lessening recovery time.

Organizations should act swiftly to ensure that their technology workforces are brought fully up to speed on the capabilities of AI technologies and how they can be leveraged for positive and negative purposes. Most importantly, employees need to be trained on two things: how to identify potentially malicious uses of AI technologies against the organization, and how to effectively and safely use AI technologies in support of the organization's cybersecurity objectives, including an emphasis on the importance of human oversight and validation of AI outputs. The workforce's understanding of AI should be maintained through frequent training updates as AI technologies rapidly evolve.

Trend 2: Addressing the cybersecurity skills gap

Some pundits are declaring that the cybersecurity workforce is in decline, anticipating rapid replacement of skilled workers by AI technologies and other forms of security automation. It remains to be seen how much of this is hype and how much the security workforce will actually decline in the future, if at all. Today, it's obvious that most cybersecurity skills and tasks can't yet be performed competently by technologies instead of people.

However, it's also obvious that there's currently a significant cybersecurity skills gap. A few decades ago, the discipline of cybersecurity was small enough that a single person could understand just about all of it:

hardening OSes, configuring firewalls to reduce network attack surfaces, deploying a VPN for secure access for remote employees and using badge readers to restrict access to the data center. Today, the field of cybersecurity has become incredibly vast, with countless specialties, technologies and standards. Even the greatest cybersecurity experts can't credibly claim to be well versed in all of its niches.

Organizations should develop a plan for addressing their cybersecurity skills gap. For many organizations, employing a combination of strategies will provide the best results. Here are some examples:

- Use AI and other security automation technologies to reduce the workload on people in those cases where the technologies perform as well or better than people would.
- Outsource some cybersecurity functions to third parties. This might be particularly beneficial for skills that an organization needs only occasionally, like forensic analysis.
- Offer a variety of skills-building opportunities to the cybersecurity workforce, such as standard training courses and short refresher courses, team exercises, and job shadowing and rotation.

Trend 3: Quantum computing and post-quantum cryptography

Researchers around the world continue to push the boundaries of quantum computing technologies. We don't know when these technologies will become powerful enough to thwart today's encryption technologies, but experts expect us to pass that threshold in the coming years. At that time, all organizations with quantum computers will be able to access all of the data currently protected by cryptographic algorithms, effectively creating the world's largest data breach.

Organizations should start preparing now for what's called post-quantum cryptography (PQC), which means using cryptographic algorithms that won't be vulnerable to quantum computing. Several post-quantum algorithms have been finalized and standardized recently, and various technologies are adding support for them.

Organizations should inventory their current cryptographic usage, plan how to migrate all of those technologies to their post-quantum counterparts, and then start executing on that plan. Waiting is dangerous because, once quantum computing becomes sufficiently advanced, data that was encrypted months and years ago using today's algorithms will all be accessible. It will be far too late to protect it.

For more information on the latest developments in post-quantum cryptography, see the PQC website hosted by NIST.

Trend 4: Improving response capabilities

It's become painfully obvious that most organizations need to improve their response capabilities. Attacking organizations through ransomware has become an actual business, with attackers effectively locking users out of their systems and data, then demanding -- and receiving -- large ransoms to restore access. At the same time, these attackers are conducting large data breaches, collecting enormous amounts of sensitive data and demanding ransoms to prevent its release or sale.

Organizations need to be prepared to respond to large-scale ransomware incidents, and that means incident responders working closely with not just security experts but also system administrators, legal

counsel, public affairs and others to ensure the response goes smoothly and services are restored quickly. Prepare to handle ransom demands before they're made.

Trend 5: Recognizing the risks from supply chains

We typically trust what our vendors and service providers give us. The SolarWinds incident illustrated just how risky that trust in our supply chains is. A single company can be successfully infiltrated by a nation-state, and that company might then provide compromised technology products or services to thousands of other companies. Those companies, in turn, might not only be compromised themselves; they could also expose their own customers' data to the original attackers or provide compromised services to their customers. Thus, what started with a single infiltrated company could expand to millions of organizations and individuals being compromised.

There's no easy answer to addressing this. Organizations could improve many aspects of their security strategy and technology, but what's most important at this time is for organizations to recognize and acknowledge the risks from supply chains and to demand increased vigilance from everyone. Whether that means holding vendors accountable for poor security practices that lead to compromises, requiring more transparency into vendors' security practices before renewing contracts or adding requirements to new procurements, individual organizations can raise awareness of these issues and put pressure on vendors and service providers to do better.

49. The cloud's role in PQC migration

by George Lawton
https://www.techtarget.com/searchcloudcomputing/tip/The-clouds-role-in-PQC-migration

Q-Day -- when quantum computers start cracking existing public key cryptography schemes -- is still a few years away. Cloud providers are making progress to support the integration of post-quantum cryptography into existing infrastructure to ensure secure data and application protection, while maintaining business continuity.

Nigel Gibbons, director and senior advisor at NCC Group, a cybersecurity consultancy, said: "Post-quantum cryptography migration is not simply a cryptographic upgrade; it is a foundational shift in enterprise security architecture." Cloud and edge computing play a vital role in enabling this shift, offering both platforms for experimentation and infrastructure for scaled deployment.

With this new technology, enterprises will need to navigate numerous challenges to successfully undergo post-quantum cryptography (PQC) migration. But cloud providers are already adopting various migration strategies that can help.

How cloud can meet PQC migration challenges

Various PQC algorithms have been around for decades, all of which suffer performance, key size and security tradeoffs. In late 2024, NIST finalized the first Federal Information Processing Standards for PQC algorithms. These aim to improve interoperability and drive adoption.

"Cloud hyperscalers are moving in the right direction, offering PQC-ready services in key areas like [Transport Layer Security], VPNs and key management. But, right now, it's more about experimentation and readiness testing than full-scale enterprise deployment," said Mukesh Ranjan, vice president at Everest Group.

Across all the scenarios, the cloud can be useful in isolating PQC risks, testing hybrid crypto models and validating interoperability across systems. Cloud-native systems will be the most straightforward for PQC migration because of their centralized nature. However, this remains a complex endeavor since numerous crypto systems are spread across each cloud service.

"It's the best environment to run controlled pilots before scaling changes across the enterprise," Ranjan said.

Enterprises face additional risks and complexities in PQC migration efforts for legacy, on-premises and embedded systems. On-premises support is mostly limited to toolkits and documentation, Ranjan said. Embedded systems are lagging, often left to chipmakers and OEMs.

PQC migration challenges

PQC migration presents numerous challenges. Organizations can improve their security for the quantum era by proactively addressing these challenges.

Consider the volume of infrastructure a business uses. Each of these has its own crypto implementation, often hardcoded and undocumented.

"Enterprises today rely on decades' worth of infrastructure -- from mainframes and [programmable logic controllers] to cloud VMs and containerized microservices," said Rebecca Krauthamer, co-founder and CEO at QuSecure, a quantum cybersecurity vendor.

Another issue with PQC migration is the lack of standardization in implementation. For example, at the network level, some providers use post-quantum preshared keys instead of PQC directly. Ultimately, this challenge lies with software developers.

"While there is general agreement on PQC algorithms, there's no single way to apply them," said Carl Dukatz, global lead for quantum at Accenture.

The primary challenges with PQC migration are deeply rooted in the operational and architectural complexity of existing systems, Gibbons said. Some of the areas that create the most challenges are the following.

Legacy systems

Older systems often rely on hardcoded cryptographic libraries or unsupported protocols. These might not be compatible with larger key sizes or entirely new algorithm structures that PQC could introduce. Legacy systems also typically lack crypto-agility, which makes it hard to plug in PQC algorithms.

Visibility and inventory

Enterprises often lack full visibility into where and how cryptography is used across their environments. Additionally, without a comprehensive cryptographic inventory, identifying what needs to be updated for PQC is a substantial hurdle.

"Without that, any attempt at PQC migration is like flying blind," Krauthamer said.

Dependency management

Dependencies like legacy libraries or closed source vendor software can become roadblocks. Many enterprise applications rely on third-party libraries, hardware security modules (HSMs) or external APIs that might not support PQC. Updating or replacing these dependencies can be expensive and time-consuming.

Integration and update issues

New cryptographic primitives require updates across the entire software stack, from firmware to APIs to application layers. Integration is particularly difficult in tightly coupled systems where cryptography is embedded deeply.

Common approaches exist for application development, such as using APIs or standardizing on the Transport Layer Security (TLS) cryptographic protocol. Still, there is no universal pattern or guide for building IT systems. This means that each system that requires PQC must be updated carefully and thoughtfully.

"It's the diversity and customization of solutions that make this transition challenging," Dukatz said.

Even if the business doesn't patch systems, cloud providers will likely include this in a product upgrade or new release. Otherwise, nonupdatable systems should be protected by another safety measure.

"Creating and deploying these updates takes time, and each step requires education and testing," Dukatz said.

Cloud provider options

Dukatz shared that many cloud providers have begun providing their customers with access to PQC. In fact, AWS, Google and Cloudflare rolled out prestandardized PQC schemes before the NIST standards.

However, this doesn't mean that these providers are selling the same offerings.

"Each cloud provider is following a slightly different path to the same goal, and this differentiation fosters innovation," said Dr. Ja-Naé Duane, academic director at Brown University School of Engineering and MIT Research Fellow.

Consider the following PQC offerings from AWS, Google and Cloudflare:

- **AWS.** AWS provides PQC support for its Transfer Family service to securely move data to and from its cloud. It is taking a phased approach, focusing first on TLS connections and core libraries, like AWS Libcrypto, to secure data in transit across internet-facing services.

- **Google.** Google uses key encapsulation mechanisms to protect against steal now, decrypt later attacks. It is also heavily investing in cryptographic services, like Cloud Key Management Service (KMS) and Cloud HSM.

- **Cloudflare.** Cloudflare secures over 35% of its human-generated internet traffic connected to its networks. It is providing immediate quantum-safe tunnels for TLS traffic without requiring customers to upgrade individual libraries.

Dukatz said different ways of accessing the cloud can also lead to different experiences for users upgrading to PQC. For example, with SaaS, most users can upgrade to PQC transparently, as major web browsers already enable these protections. PaaS providers can update their base images and key management capabilities so that users have PQC packages when they deploy new systems.

"However, it's still the customer's responsibility to bring on and enforce these updates, which can be just as complex as an on-premises PQC upgrade," Dukatz said. The same patterns apply to embedded systems managed by the cloud.

3 migration support areas

While cloud-native environments are getting better support first, the transition for on-premises and embedded systems will require more custom work and longer timelines. Gibbons said that cloud service providers (CSPs) are largely focusing on three strategic areas to help enterprises use the cloud to support migration efforts:

1. **Cloud-native support.** For workloads running in the cloud, CSPs are introducing PQC support through their managed services, such as TLS in load balancers, KMS integrations and secure storage. These are often easier to update and provide the quickest path to PQC readiness.

2. **Hybrid and on-premises support.** Recognizing the hybrid nature of many enterprises, CSPs are beginning to offer toolkits and SDKs that extend PQC support to on-premises systems. Microsoft's open source PQCrypto-VPN and AWS' integration of PQC into TLS libraries like s2n are examples of this cross-environment strategy.

3. **Embedded systems and edge devices.** The edge could also play an important role in supporting migration efforts using local cryptographic processing, supporting a gradual transition and firmware and cryptographic update distribution. Support here is still in early development. Cloud providers are collaborating with hardware manufacturers and IoT vendors to test and validate lightweight PQC implementations. Google and Microsoft are contributing to open standardization efforts to ensure compatibility in constrained environments.

Where should you start?

Organizations should start with a cryptographic asset inventory, evaluate their risk exposure to quantum threats and collaborate closely with CSPs to implement early-stage protections and transition pathways.

Dr. Ali El Kaafarani, CEO of quantum security vendor PQShield, recommended enterprises speak to their cloud providers to understand the crypto roadmap for each service. Major providers, like AWS, Microsoft and Google, have clear transition plans and can help businesses prepare theirs.

Karl Holmqvist, founder and CEO at identity security vendor Lastwall, recommended enterprises explore how cloud infrastructure can be used as a low-risk sandbox environment to pilot PQC transitions. This can help understand performance impacts or interoperability issues before broad enterprise deployment.

"I would encourage leaders to think of what types of fast experimentation they can do in cloud environments to prove PQC capabilities can work before deploying," he said.

Ultimately, the decision-making and strategic initiatives necessary to undergo migration must come from knowledgeable teams invested in the success of their business.

"While cloud providers are beginning to offer tools and services to support PQC migration, the road ahead requires strategic planning, technical agility and collaboration across IT, security and business teams," Gibbons said.

50. What's Europe's Quantum Strategy? Breaking Down Europe's Coordinated Plan for Global Quantum Leadership

by Matt Swayne
https://thequantuminsider.com/2025/07/03/whats-europes-quantum-strategy-breaking-down-europes-coordinated-plan-for-global-quantum-leadership/

The European Commission has unveiled a sweeping plan to consolidate Europe's position as a global leader in quantum technologies, laying out a multi-decade industrial roadmap that aims to turn scientific strength into economic scale. The *Quantum Europe Strategy* details a coordinated investment and policy framework to overcome fragmentation, accelerate commercial applications, and secure Europe's technological sovereignty in a field seen as critical for competitiveness, cybersecurity, and national defense, said Henna Virkkunen, Executive Vice-President for Tech Sovereignty, Security and Democracy, in a statement.

"With Quantum science advancing rapidly, we are on the verge of some of the most transformative scientific and technological breakthroughs," Virkkunen said in a statement. "Europe has always been at the forefront of quantum science, with a strong record of innovation and discovery. We have everything we need to become a leading quantum continent, from a highly skilled workforce to a robust research infrastructure. As the global quantum race intensifies and moves from lab to real-world application, Europe must maintain its leadership. That's why we are launching the Quantum Europe Strategy – to bring together Member States, industry, academia and society to unlock the full potential of quantum technologies."

The strategy marks a turning point in Europe's approach to quantum, shifting focus from scattered research efforts to unified industrial deployment. Despite leading the world in quantum talent and publications, Europe lags in patent filings, private investment, and quantum hardware manufacturing. The Commission warns that without a stronger commercialization pipeline and sustainable support for startups, the region risks losing ground to the United States and China, both of which have committed billions to scaling quantum platforms.

Quantum Strategy Institute's Head of Government and Consortium Relations, Petra Soderling, and primary drafter of the EU Quantum Strategy writes in a Substack post that Europe has all the requirements needed to be a quantum leader.

"The EU Quantum Strategy is being written in the midst of a heated global race that is dividing interest lines and regrouping camps," Soderling writes in the post. "Europe has the strength and the potential of being competitive in many of the quantum sectors, but now is the time to develop the ecosystem; build infrastructures, educate the workforce, develop problem solving solutions, establish supply chains (=friends) and ensure funding for the future."

Five-Point Framework Anchors The Strategy

At the heart of the plan is a five-pronged approach:

1. **Research and Innovation** – aligning public and private research across member states through a new Quantum Europe Research and Innovation Initiative.
2. **Quantum Infrastructures** – expanding shared computing, communication, and sensing facilities under public control.
3. **Industrial Ecosystem Support** – bolstering startups, building pilot production lines, and increasing private capital flow.
4. **Space and Security Integration** – embedding quantum in EU space, defense, and intelligence programs.
5. **Skills Development** – launching a pan-European training system to produce applied quantum engineers and technicians.

Each area will be supported by a coordinated implementation plan, with new legislation – the upcoming *Quantum Act* – expected in 2026 to formalize governance structures and funding instruments.

Technology platform	Superconducting	Ion traps	Cold atoms	Photonics	Spin qubits
EU machines	17	6	8	5	3
UK machines	4	**6**	0	**5**	2
USA machines	26	7	4	2	0
Canada machines	13	0	0	1	0
China machines	2	0	0	0	0
ROW[29] machines	1	0	0	1	**3**

From Research to Market: Closing the Commercialization Gap

The strategy acknowledges that Europe's existing €11 billion in quantum investment over the past five years has delivered scientific results but has not translated into global market leadership. While approximately one-third of the world's quantum companies are based in the EU, and European firms supply nearly half of hardware and software components used globally, the lack of scale, fragmentation across national programs, and limited industrial demand have stifled growth.

To address this, the EU will establish six quantum pilot lines under the Chips Joint Undertaking, each co-funded by member states and the Commission. These facilities will enable early prototyping, process development, and industrial validation of quantum chips – which remain largely handcrafted and proprietary. *A Quantum Chips Industrialisation Roadmap* is due in 2026, alongside a *Quantum Standards Roadmap* to drive interoperability.

Public procurement will also be used to stimulate demand, with hospitals, infrastructure agencies, and government departments acting as early customers for quantum-enabled tools. The Commission plans to coordinate this through targeted financial incentives and innovation-oriented procurement schemes.

Building Quantum Infrastructure for Computing, Communications, and Sensing

A key element of the strategy is scaling up shared quantum infrastructure. Through the EuroHPC Joint Undertaking, Europe is already deploying early quantum computing prototypes in countries including France, Germany, and Finland. These systems will evolve into hybrid high-performance computing (HPC)–quantum platforms, designed to accelerate industrial use cases and support Europe's AI strategy.

In communications, the EuroQCI initiative aims to build a secure quantum network spanning all EU countries and overseas territories, using both terrestrial fiber and satellite links. The first space-based quantum key distribution satellite, Eagle 1, is scheduled for launch in 2026. By 2030, the EU plans to connect its terrestrial and space segments to form a unified secure communication network.

The strategy also highlights quantum sensing as a priority, with applications ranging from gravimetry for subsurface mapping to next-generation medical diagnostics. A European quantum MRI pilot network will be launched in 2025, aiming to develop and clinically validate quantum-enhanced imaging systems. Quantum gravimeters – sensors capable of detecting underground water, magma, and infrastructure – will also be deployed across Europe, with airborne and spaceborne platforms under study.

Defense, Space, and Strategic Autonomy

Quantum technologies are classified as dual-use, with strategic implications for both civilian and military operations. The Commission plans to align quantum development with European defense goals, including through contributions to the European Armament Technological Roadmap and cooperation with the European Space Agency. Specific efforts include developing GNSS-free navigation systems using quantum sensors, secure battlefield communications, and space-based gravimetry.

The Commission will also initiate a *Quantum Sensing Space and Defence Roadmap* in 2026 and fund spin-in initiatives to integrate civil quantum innovations into military systems. These efforts align with recent

actions under the European Defence Fund and NATO's growing interest in becoming a "quantum-ready alliance."

Funding, Investment and Supply Chain Resilience

To address chronic underfunding, particularly in the growth stages, the Commission is encouraging public-private co-investment through vehicles like the European Innovation Council (EIC). The new Scaleup Europe Fund, launched in May 2025, will invest directly in strategic sectors including quantum. National governments are urged to reallocate cohesion funds toward deep tech startups aligned with European goals.

On the supply chain front, the EU will map risks and dependencies across the quantum stack – from rare materials to control electronics. Results from a comprehensive *Quantum Technology Risk Assessment* are expected by 2026, according to the paper. These findings will inform mitigation strategies, including diversification, onshoring of production, and export control reform.

Workforce: a Strategic Bottleneck

Europe produces over 110,000 STEM graduates annually, but the quantum sector faces acute labor shortages, especially in applied areas like software engineering, systems integration, and cybersecurity. To address this, the Commission will launch a *European Quantum Skills Academy* in 2026, offering training modules, fellowship schemes, and virtual teaching resources. The plan also includes apprenticeships, researcher-in-residence programs, and quantum-focused digital skills competitions.

Efforts to promote diversity and close the gender gap are included in the academy's mandate. The long-term goal is to establish geographically distributed quantum training centers, integrated with national Quantum Competence Clusters and semiconductor skills hubs.

The Global Competition

The strategy mentions the increased investments from countries and regions around the world that are aimed at attaining a global leadership position in quantum technology. For example:

- **China**: With an estimated $15 billion in public funding, China leads in quantum communications, operating a 12,000-kilometer network, including two quantum satellites. Its state-driven approach prioritizes strategic applications, but private sector investment remains limited. It's important to note that China's actual budget is not transparent, so experts often dispute the $15 billion figure.

- **United States**: The US excels in private sector funding, with more than $1 billion invested in quantum startup in the first quarter of 2025 alone, according to The Quantum Insider. Its collaborative ecosystem, involving government labs, universities, and industry, gives it an edge in innovation, though public funding lags behind China.

- **Europe**: The EU has invested around $10 billion, primarily driven by Germany, and hosts nearly a quarter of global quantum companies. However, a 2025 Quantum Industry Consortium (QuIC) report warns that Europe risks losing its edge without closing funding gaps and building a full-stack ecosystem.

Outlook: Challenges and Opportunities

Europe's strategy leverages its strengths – research output and a robust startup scene – while addressing weaknesses like fragmentation and insufficient private investment. International cooperation, such as with the US, Japan, and South Korea, is also emphasized to set global standards and share resources.

The strategy identifies **several challenges**:

- **Fragmentation**: Coordinating 27 Member States is complex, risking duplication and inefficient resource use.
- **Funding Gaps**: While public investment is substantial, private funding lags behind the US, and sustainable financial support is needed for startups.
- **Talent Competition**: Attracting and retaining quantum talent is critical, especially as global demand grows.

Despite these challenges, the strategy lists **significant opportunities** exclusive to Europe:

- **Research Excellence**: Europe leads in academic output and trains more quantum specialists than any other region.
- **Startup Ecosystem**: With a strong presence of quantum companies, Europe can drive innovation if supported effectively.
- **Strategic Initiatives**: Programs like EuroHPC and EuroQCI position Europe to lead in quantum computing and secure communications.

From Strategy to Execution

Obviously, plans and strategies do not work without action. The strategy addresses this.

Quantum Europe Strategy is backed by detailed action points, much will depend on sustained funding, legislative support, and private sector engagement. The proposed *Quantum Act*, roadmap publications, pilot deployments, and industrial partnerships represent a concrete step toward scaling Europe's scientific strengths into globally competitive quantum platforms.

If successful, the strategy could mark a pivotal shift in Europe's technological trajectory, turning a fragmented innovation landscape into a unified economic force in what many see as the next great computing revolution.

51. No, Chinese Did Not Crack RSA with Quantum (Yet)

by Marin Ivezic
https://www.hstoday.us/subject-matter-areas/cybersecurity/no-chinese-did-not-crack-rsa-with-quantum-yet/

For the last two days my inbox (and LinkedIn messages) has been flooded with questions about headlines claiming that "Chinese researchers broke RSA encryption with a quantum computer, threatening global data security." Let's address this clearly: No, no such cryptographic apocalypse has occurred, and there's no indication that such a feat is imminent**.** In fact, the report making the rounds doesn't bring the quantum threat any closer to reality, let alone break any of today's encryption.

This buzz stems from a year-old Chinese research paper that – while scientifically interesting – only managed to factor a very small 22-bit RSA number using a D-Wave quantum annealer. That is a far cry from breaking the 2048-bit RSA keys that protect real-world communications (for context, the largest RSA key ever cracked by classical methods is only 829 bits, RSA-250, factored in 2020). The Chinese paper (published in the *Chinese Journal of Computers* in May 2024) was discussed in a recent news article with the alarmist title *"China breaks RSA encryption with a quantum computer, threatening global data security."* That article – in my view a very irresponsible piece – got picked up by other outlets and spread on social media, fueling confusion.

So, let's set the record straight.

What Did the Chinese Researchers Actually Achieve?

A team led by Professor Wang Chao at Shanghai University published a paper describing how they factored a 22-bit RSA integer using a D-Wave quantum annealing processor. In plain terms, they broke down a number on the order of 2.3 million (specifically 2,269,753) into its prime factors. They did this by reframing the factoring task as a combinatorial optimization problem that the D-Wave quantum annealer could attempt to solve. Essentially, they demonstrated an academically interesting approach with no practical security value, since it worked only on a trivially small RSA number.

Notably, the team also reported using a hybrid quantum–classical method to factor a larger 50-bit RSA number (around 15 decimal digits) – marking the first time a 50-bit RSA integer was factored on quantum annealing hardware. More recently, in 2025, the same group announced factoring a 90-bit RSA number using an improved hybrid approach. That 90-bit demo is the largest quantum-assisted factorization to date – still far smaller than any RSA keys used in practice, but an impressive academic milestone.

To make matters more confusing, the same researchers also published a paper in late 2024 with the clickbaity title *"A First Successful Factorization of RSA-2048 Integer by D-Wave Quantum Computer."* Despite its title, that paper did **not** actually crack a 2048-bit RSA key in any general sense. It used a bit of mathematical trickery – focusing on a special class of 2048-bit integers that are much easier to factor than a real RSA modulus – to claim a result. In other words, they didn't factor a standard 2048-bit RSA modulus (the kind used in real encryption); they tackled some specially structured numbers to theoretically demonstrate a method.

Bottom line: None of these papers come anywhere close to compromising the cryptography currently in use. They haven't demonstrated any path by which these toy demonstrations could scale up to crack contemporary RSA encryption. These results certainly do not bring the so-called "Q-Day" (the day a quantum computer breaks public-key crypto) any closer, nor do they threaten "global data security." Given the overly grandiose titles of some of their papers, I suspect the research team is well aware that their claims can bait Western media outlets eager to jump on alarmist "China broke encryption" stories.

Is This a Cryptographic Breakthrough? Not Really.

So, is the Chinese 22-bit factoring experiment a meaningful cryptographic breakthrough? Not really. Here's why this result does not mean RSA is "cracked":

Trivial Key Size: A 22-bit RSA key is astronomically smaller than the 2048-bit keys used in real encryption. A 22-bit RSA modulus (≈2 million) is so small that a classical laptop can factor it in milliseconds. Even the "breakthrough" 50-bit or 90-bit examples are tiny. (For comparison, the largest RSA key ever factored classically was a 829-bit number, RSA-250, in 2020.) In short, 22, 50, or 90 bits is nowhere close to 2048 bits – these demonstrations were on cryptographically irrelevant sizes.

No Quantum Speedup: The experiment did not demonstrate any scalable quantum speedup over classical algorithms. There's no evidence that their method is faster than classical factoring on any larger input – quite the opposite. In January 2023, when another Chinese team claimed a hybrid 372-qubit approach to RSA-2048, experts like Peter Shor quickly pointed out that their algorithm had *not* been shown to run faster at scale and "could still take millions of years" to factor a real RSA-2048 key. The same principle applies here: there is no proven quantum advantage.

Heavy Classical Assistance: The researchers leaned heavily on classical computation before and after the quantum annealing step. Significant classical pre-processing was used to reduce the problem size and to embed the problem onto the quantum hardware. The D-Wave annealer wasn't doing all the work – it needed a lot of help from classical algorithms to factor even these tiny numbers.

Exponential Scaling Remains: The approach the team used still suffers from exponential scaling as the numbers grow larger. Even the authors acknowledge that only a 22-bit number "fell this time" and that their strategy "pays a price in exponential scaling," which is why they couldn't go beyond such a small modulus. There's no evidence that their method can leap from toy 50–90 bit examples to, say, a 1024-bit or 2048-bit RSA key without an exponential explosion in required time and qubits. In other words, no feasible path to breaking modern RSA has been demonstrated – certainly not by this experiment.

In short, the paper showcases an interesting research result: it shows that quantum annealers like D-Wave can contribute to factoring very small integers, pushing the state-of-the-art by a few bits. It's a nice incremental step for quantum optimization research. But it's nowhere near a practical attack on real encryption, and it doesn't point to any clear route for scaling up to break RSA-2048.

"The Sky is Falling" – Media Hype and Fear-Mongering

If the Chinese result itself was modest, the media coverage around it was anything but. Some outlets and social media posts spun this into a sensational story, tapping into a narrative of an impending "quantum threat" from China. For example, one news article ran the ridiculous headline quoted above and opened breathlessly with the claim that *"the math behind RSA encryption is starting to bend to the will of the quantum realm"*. It even went on to call the 22-bit demo *"the first time that a real quantum computer has posed a substantial threat to… algorithms in use today"* – a gross exaggeration, to put it mildly.

Unfortunately, this kind of hyperbole isn't isolated. Every few months, we see a similar hype cycle when a Chinese research team announces some incremental progress in quantum computing or cryptography. It's become a predictable pattern. A few recent examples:

January 2023: A group of Chinese researchers (Yan et al.) claimed that with a 372-qubit quantum computer and a hybrid algorithm, they *could* factor RSA-2048. This was based on actually factoring only a 48-bit number using a 10-qubit test device. The claim made headlines worldwide and provoked panic about an imminent crypto-breaking quantum machine. Within days, experts debunked it – Peter Shor himself pointed out that the team completely failed to address how fast their algorithm would run and that, given the approach described, it would "still take millions of years" to factor a real RSA-2048 key . In short, the claim was vastly overstated. It generated a huge media buzz about "Chinese quantum supremacy" before cryptographers and quantum scientists swiftly explained why it wasn't a meaningful threat.

December 2024: The same Wang Chao team in Shanghai published *"A First Successful Factorization of RSA-2048..."* with that misleading title. As mentioned, it did not actually factor a 2048-bit RSA modulus in the sense people care about, but some media nevertheless ran with it as if "China cracked RSA-2048." I analyzed that claim at the time in a blog post (see above), showing why it was *not even close* to breaking a real RSA-2048 key.

April 2025: Wang Chao's group announced factoring a 90-bit RSA number on a D-Wave quantum computer – the largest quantum-assisted factorization to date. While this is a notable research achievement in the quantum realm, it's still nowhere near breaking real encryption. Yet, some news articles framed it as a "quantum code breakthrough" inching us toward the dreaded Q-Day when all encryption falls. The *South China Morning Post*, for instance, touted it as setting a "*new benchmark... an achievement that not long ago was thought to be impossible*". True in a narrow technical sense, perhaps, but the tone of such pieces fed the notion that our data might soon be unsafe. In reality, 90 bits vs. 2048 bits is a night-and-day difference.

June 2025: The recent piece we're discussing took things to another level by explicitly claiming the 22-bit experiment is *"threatening global data security."* It even roped in quotes about newly minted post-quantum cryptography standards and advice for businesses to urgently migrate their encryption, implying that this little demo is a sign of imminent crisis. In reality, while organizations should be transitioning to post-quantum encryption (more on that later), this specific experiment doesn't change any timelines – it was not a sign that RSA is about to collapse tomorrow.

The net effect of these recurring hype cycles is counterproductive. They grab headlines and induce panic, but they also breed confusion and fatigue. If every minor research paper is trumpeted as "the sky is falling," the public and policymakers either overreact repeatedly or eventually become numb to real warnings. It's akin to crying wolf – after too many false alarms, when a truly significant quantum breakthrough does occur, people might shrug it off because they've heard so many exaggerated claims before.

No Proven Path (Yet) to Cracking RSA-2048

It's important to understand that the approach used by the Chinese researchers is not new, and it has not been proven to scale anywhere close to RSA-2048. The idea of reducing integer factorization to an optimization problem that something like a quantum annealer could try to solve has been around for decades. (Microsoft researchers, for example, published a paper on "Factoring as Optimization" back in 2002 .) Since then, numerous teams have explored these optimization-based factoring methods, but none have found a scalable way to factor large RSA keys. In practice, these methods keep hitting the same wall of exponential complexity.

The takeaway from all this: RSA-2048 remains unbroken, and none of these results thus far have illuminated a clear path to breaking it without a massive leap in quantum computing capabilities (likely requiring a full-fledged, fault-tolerant quantum computer running Shor's algorithm someday). The quantum annealing route is a fascinating research direction and will likely continue to improve bit by bit, but it has not demonstrated any change in the fundamental scaling law of the problem. Each time the record is extended by a few bits, the effort required (in qubits, runtime, and classical post-processing) grows dramatically. There's no sign of a sudden jump from these toy examples to factoring a 1024-bit or 2048-bit RSA key.

It's also worth emphasizing: the Chinese research team themselves are not claiming they've broken RSA-2048, nor that they can decrypt your bank traffic or HTTPS communications. They're exploring an alternative quantum computing paradigm (adiabatic/annealing computing) for cryptanalysis, which is a valid scientific pursuit. Even Professor Wang Chao has described their progress as "*an incremental but essential nudge,*" noting that mainstream 2048-bit RSA keys remain far beyond their reach. The real problem is how these results get portrayed outside the lab. The researchers published their findings in academic forums – it's the media and commentators who often misrepresent them as earth-shattering breakthroughs. (Arguably, the researchers could choose less sensational titles to avoid misinterpretation, but that's a separate issue.)

Stay Informed, Not Alarmist

None of this is to say that the quantum threat to encryption isn't real in the long run. It certainly is – in the future. Virtually all experts agree that a sufficiently advanced quantum computer (capable of running Shor's algorithm at scale) will one day break RSA and ECC. That's why there is a global effort underway to transition to post-quantum cryptography (PQC) in the coming years. Governments and enterprises should indeed be preparing for Q-Day in a rational way: by inventorying their cryptographic systems, adopting the new PQC standards (such as those being standardized by NIST), and ensuring crypto-agility (the ability to swap out cryptographic algorithms easily) in their infrastructure. These are sensible, proactive measures to guard against future quantum threats.

What we don't need, however, is panic every time a minor academic result is published – especially when such results are hyped out of proportion. Overreactions and sensationalism can be just as harmful as complacency. It's crucial to stay informed with facts and context, rather than giving in to alarmism or flashy headlines.

In conclusion, to answer the original question that spurred this discussion: No, Chinese researchers have not cracked RSA-2048. Not even close**.** What they have done is advance the field of quantum computing research by incrementally factoring larger (but still very small) integers with the help of quantum annealing. It's a cool result for the quantum optimization community and deserves recognition as such – but it's not a cause for panic, nor a sign of an impending crypto-apocalypse.

I would also suggest that the researchers themselves be careful in how they present their work to the public. As leading computer scientist Scott Aaronson quipped about one of these recent papers, *"one has to anticipate and head off the way that claims are going to be misinterpreted."* In other words, it's not enough to technically avoid false statements; you should also try to prevent people from reading false things into your statements. That's advice we could all stand to heed in the midst of a hype-prone environment.

52. Crypto-Procrastination: Preparing for a Quantum Secure Economy, Today

by Jaime Gómez García
https://www.infosecurity-magazine.com/opinions/crypto-procastination-quantum/

As the era of quantum computing approaches, the foundations of digital security are under threat. Modern cryptographic systems that maintain the confidentiality, authenticity and integrity of data and digital signatures will no longer be secure once a cryptographically relevant quantum computer exists.

For sectors like finance and banking, where the security of records underpins global trust and stability, this presents a critical challenge. Quantum-enabled attackers could decrypt sensitive communications, forge digital signatures and compromise important legal documents.

Fortunately, organizations do not have to respond to abstract risk scenarios or uncertain timelines given that they now have concrete milestones to guide them in their journey to the era of cryptographic assurance.

With the US NIST's post-quantum cryptographic standards now in place, the phase out of quantum-vulnerable algorithms is possible and is anticipated to occur in the next 10 years. Such standards provide the compliance and technical foundation for proactive planning today.

Crypto-Procrastination: Why Action is the Best Policy

"Crypto-procrastination" refers to widespread hesitancy to start actions towards the transition to quantum-safe cryptography and improving cryptographic management in organizations.

The term describes how organizations are delaying action on quantum-safe cryptography, due to three main reasons: underestimating the impact of the risk and the associated compliance requirements, misunderstanding the challenges of the transition and treating quantum threats as too distant to merit action.

Part of the challenge lies in the fact that quantum security remains poorly understood across many organizations, making it difficult to elevate as a strategic priority. To act decisively on quantum safety demands a certain depth of knowledge.

Further, with CISOs pressed by immediate threats such as ransomware or nation-state cyber activity, longer-term quantum milestones can seem too distant. This disconnection contributes to inertia at the exact moment when forward planning is most essential.

The longer organizations delay, the greater the risk of compressed implementation timelines which can strain resources, inflate costs and reduce the quality and security of outcomes.

By starting now, institutions can spread investments, integrate changes into regular update cycles, and engage in coordinated sector-wide planning. The advantage is not just risk reduction—it's long-term resilience, smoother compliance and more informed, cost-effective decision-making.

Navigating the Quantum Security Timelines

Encouragingly, the evolving conversation around quantum timelines, once characterized by speculation, is now giving way to clarity and strategic foresight. While academic debate continues, it has helped raise awareness and sparked productive dialogue within industries.

Many organizations are beginning to recognize that preparing for post-quantum security is not about reacting to an imminent threat, but about building long-term resilience in a measured, standards-aligned way. This shift in mindset is already paving the way for collaborative planning and innovation.

And we do have a certain milestone: Post-quantum cryptography standards are already available and in widespread use (for instance, in web browsing to major search engines), and the end of life of the quantum-vulnerable cryptography has been set between 2030 and 2035.

The need to transition has become a compliance requirement supported not only by standards, but also by sector-specific regulations like the EU's Digital Operational Resilience Act (DORA) and PCI-DSS, capturing growing attention from financial supervisors like the Monetary Authority of Singapore and the Bank of Israel.

Impact on the Financial Sector

Financial institutions are vulnerable to quantum threats as they depend on cryptography to secure their operations. Customers rely on cryptographic tools to securely authenticate, communicate, and sign documents—all essential to daily financial operations.

The same mechanisms protect the operations among financial institutions in markets, wholesale operations, etc.

A successful quantum attack could compromise transaction integrity, allowing hackers to disclose financial information, manipulate payments, forge digital signatures and bypass authentication mechanisms.

Without post-quantum cryptography, the financial ecosystem—from online banking to secure payments—faces serious cybersecurity risks. As quantum computing advances, financial institutions must accelerate efforts to implement quantum-resistant cryptography, ensuring their systems remain secure and resilient for the post-quantum era.

The consequences of these types of breaches extend far beyond individual institutions, posing a systemic risk to global financial stability. As noted in the World Economic Forum's quantum security white paper, proactively addressing quantum risk is essential to maintaining financial stability and public trust as digital infrastructure evolves.

Quantum Readiness: the Role of Standards Bodies and Regulation

The transition to quantum-safe cryptography cannot happen in silos. Cross-sector roadmap alignment is essential. Through collaborative platforms that bring together academia and industry experts, these

organizations, including ETSI, are shaping the technical foundations and policy frameworks needed to support a quantum secure future.

The financial sector, supervisors and regulators are putting the spotlight on mature cryptography management practices. Existing regulations, such as DORA or PCI-DSS, require organizations to prevent future challenges to cryptography.

Financial sector organizations, like the Europol Quantum Safe Financial Forum or FS-ISAC, are driving collaboration initiatives to share best practices and coordinate efforts. The global, interconnected and interoperable nature of the financial ecosystem sets the need for a strong global alignment in the sector at large on the priorities and timeline to implement the transition.

Given the financial sector's high level of interconnectivity, a synchronized migration strategy would streamline the transition by addressing key bottlenecks, including:

- **Fragmentation:** Misaligned strategies due to organizations adopting different approaches
- **Prolonged reliance on outdated cryptography:** The need to maintain legacy cryptography to accommodate slower adopters
- **Duplicated effort:** Wasted resources as companies independently solve the same challenges without knowledge sharing

A global action plan is essential to prevent crypto-procrastination and ensure an orderly transition. The global financial system must build a cohesive, strategic roadmap toward a quantum-secure economy today.

Leadership in a Standards-Led Era

The good news is that the roadmap to a quantum-secure economy is clear and anchored in emerging standards that make implementation achievable today. By adopting quantum-safe cryptographic solutions, financial institutions can adapt to evolving standards, protect sensitive assets, mitigate security risks and reinforce customer trust before quantum-enabled attacks become a reality.

Proactive action ensures long-term resilience, regulatory compliance and the continued integrity of global operations. Financial organizations will be able to take control of their futures, ensure resilience and uphold trust as they navigate tomorrow's quantum threats.

53. How a post-quantum approach to cryptography can help protect mainframe data

by Anne Dames
https://www.ibm.com/think/insights/post-quantum-cryptography-protect-mainframe

As the industry gets closer to achieving a cryptographically relevant quantum computer, the security of data—operational, personal and financial—will be more critical than ever. Protecting that data from this newest risk vector will become a top priority for many enterprises.

Unfortunately, the public key cryptographic algorithms defined in current standards, which were developed and published in the 1970s, rely on mathematical problems that challenge *classical* computers. These industry standards are still used in some of today's data protection schemes. Someday soon, a cryptographically relevant quantum computer might break those cryptography standards, thereby compromising sensitive data.

Although such a machine does not yet exist, cyberattackers can steal encrypted data today, store it and then wait for quantum computing decryption technologies to evolve. Known as "harvest now, decrypt later," this strategy underscores the need for post-quantum, also known as *quantum-safe* or *quantum-resistant*, cryptography. Although no practical quantum attacks currently exist, some data stored today might remain sensitive for decades. As quantum computing advances, the risks to traditional encryption methods increase.

Cyberattackers put a bullseye on the mainframe

The mainframe isn't immune to this threat. It's an attractive target for cybercriminals because it stores and processes vast amounts of sensitive data in companies across all industries. In addition, many applications use cryptographic methods that aren't quantum resistant, leaving them and the data they rely on and store vulnerable to quantum attacks. Understanding your use of cryptography is critical to using the mainframe's robust security capabilities to help protect your sensitive data and assets.

The security of transactional data is especially critical to enterprises in banking, healthcare and defense. To protect this mission-critical data, these enterprises are clamoring for post-quantum cryptography (PQC) that uses a type of encryption believed to withstand attacks from quantum computers. Adopting PQC is intended to help ensure that mission-critical data residing on the mainframe remains protected now and in the future.

Crackerjack cryptographers try cracking the code

PQC is built on mathematical problems and algorithms designed to resist quantum attacks and protect information assets. In 2016, the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) held a global competition among cryptography experts to develop cryptographic algorithms resistant to being broken by quantum computing methods. This was followed by 8 years of rigorous testing by encryption and cryptography experts and enthusiasts worldwide.

Scores of algorithms yield 3 new standards

In 2022, NIST selected 4 unbroken algorithms for standardization from the 82 cryptographic algorithms submitted by individuals and teams across academia and industry. IBM Research®, with industry and academic partners, developed 3 of them. The 4th selected algorithm was co-developed by a researcher who has since joined IBM.

In August 2024, NIST published the first 3 post-quantum cryptographic algorithms, including 2 that were developed by IBM Research and its partners. A draft of the 4th algorithm is expected to be published soon. According to Jay Gambetta, Vice President of Quantum and an IBM Fellow with IBM Research, "NIST's publication of their first three post-quantum cryptography standards marks a significant step in efforts to build a quantum-safe future alongside quantum computing."

Transitioning to PQC can be challenging. The first step toward creating a quantum-safe mainframe environment is to identify and fix potential vulnerabilities. This process entails classifying cryptographic algorithms as *quantum resistant* or *quantum vulnerable* and then remediating those deemed *quantum vulnerable*.

IBM Z: The mainframe platform that's up to the challenge

According to Gambetta, "IBM's mission in quantum computing is twofold: to bring useful quantum computing to the world and to make the world quantum-safe." Demonstrating this commitment, the IBM Z® system became an early adopter of the 2 primary algorithms selected for PQC standardization by NIST with the launch of the IBM z16® system in April 2022. Security is engineered into the z16® system with 2 of the 4 NIST-standardized cryptographic algorithms built into the platform tier. The system uses cryptographic methods designed to help protect against attacks from both classical and quantum computers.

Queuing up quantum safety for today and the future

The importance of PQC for enterprise mainframe data—today and into the future—is difficult to overstate. PQC is a vital component of mainframe security in today's complex and vulnerable enterprise computing environment. By adopting a suitable set of NIST-standardized post-quantum cryptographic algorithms, you'll be better able to employ defenses against certain attacks from classical and quantum computers, helping to ensure the continued security and integrity of your mission-critical mainframe data and enterprise systems.