Crypto News

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

October 05, 2025

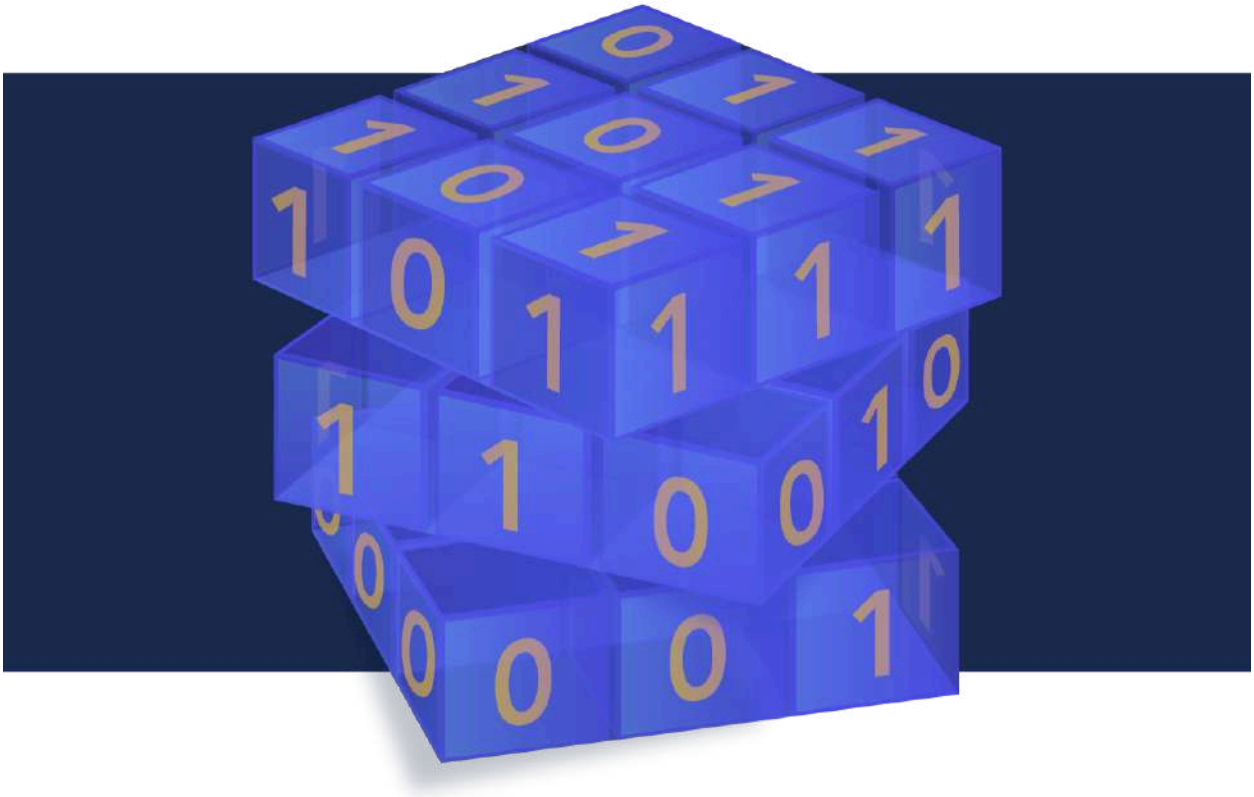

Table of Contents

Editorial

It's officially fall and what a grand time to "fall in" (pun intended) to this exceptional issue of Crypto News. For those who have been to my presentations, you've often heard me say that the controls your organization needs to align with in relation to post-quantum readiness are already there. Especially as they relate to data encryption at rest, in transit, and while processing since those controls refer to the importance of data security. For those who requested a more concrete mapping, you can now find it in a white paper released by NIST in alignment with their National Cybersecurity Center of Excellence (NCCoE) team, which maps quantum-resistant cryptography to NIST CSF 2.0 and SP 800-53. As additional information, this white paper is available here (https://lnkd.in/e6QDtTSY) if you're interested in reviewing it in its entirety. Otherwise, for a more concise update, make your way to article 8.

Another article that piqued my interest is article 21. I've often been asked where I believe we'll see the first evidence of a quantum advantage if an adversary, nation state, or threat actor were to achieve it and chose to use it covertly but on a public stage. My answer is always cryptocurrency. Hitting any aspect of a nation's financial infrastructure is a key method to cause de-stabilization and mass chaos. Everyone likes their money, and no one wants anyone taking it away from them. Article 21 outlines how we are getting ever closer to a quantum computer showing a quantum advantage and making this scenario a reality. If you're interested in learning more about what's at stake and what financial institutions who create and manage these assets can do to prevent this catastrophe, you can refer to article 21 in this newsletter as well as the SEC Post-Quantum Financial Infrastructure Framework (PQFIF) released a few weeks ago and outlined in my post here (https://lnkd.in/eYn9MTd9). We all should be preparing, and we all should be holding all financial institutions, including cryptocurrency exchanges and cryptocurrency guardians, accountable for protecting our money and assets.

There are so many articles of note in this newsletter that you won't want to miss a single one. As always, Happy Reading!

The Crypto News editorial is authored by the co-Chair of the Quantum-Safe SecurityWorking Group (QSS WG) of the Cloud Security Alliance (CSA), Mehak Kalsi, MS, CISSP, CISA, CMMC-CCP 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. Start PQC planning now or suffer

by GlobalData Technology
https://www.verdict.co.uk/pqc-post-quantum-cryptography/?cf-view

Barely heard through the loud, thumping, dubstep that is AI marketing, one of the things that will need attention soon is the move to post quantum cryptography (PQC).

When quantum computers reach a certain level of processing power in the future, it will be possible to use these machines to break today's ubiquitous and effective encryption.

There is no estimate or even a consensus as to when quantum computers will be able to threaten the encryption infrastructure used today. But that doesn't fundamentally matter.

Major government organisations, including the US CISA, the UK's NCSC, and the European Commission have all mandated that organisations move to adopt quantum-resistant encryption by 2035.

This encryption is based on standards created at the US National Institute of Science and Technology (NIST).

Now, 2035 sounds like a long time – but the task of replacing the base encryption used for data in flight and data at rest is a huge task. On top of that, there is worry about a tactic known as store and decrypt, in which bad actors would collect data encrypted with today's standards, then use quantum computing later to decrypt the data.

Game plan PQC

Most governments have laid out a framework for how to approach the problem of PQC and how to proceed. The steps are broad – but show the scope of the work needed, and the necessity of buy-in by everyone – including the CEO and the Board.

There will also be considerable input from teams that evaluate risk for the organisation. It will require a steering committee, and heavy involvement from both information technology departments (IT) and operational technology departments (OT).

At the end of the day, a plan must be formed, based on the criticality of each system, cost, existing replacement plans, and other risk factors, depending on a given organisation's needs. Partnering with the organisation's vendors and service providers to get guidance when they will be supporting PQC will need to be part of the process as well.

Once the discovery, prioritisation and planning stages are done, then implementation can proceed, with the government mandated deadlines kept in mind. With the plan available, then adjustments for unknowns can be made using the criticality and risk evaluations.

The project starts now

Of course, all of this sounds like a nightmare-level project. However, given the distant time horizon, it doesn't have to be, provided the required organisational buy-in, discovery, evaluation, and planning starts now.

Much of the PQC updates can be part of normal upgrade/lifecycle activity. Planning will allow the move to PQC to be strategic, a way to get several things done at once, and avoid rushed decision making and implementation.

It will also allow the organisation to make hard choices with due consideration, such as systems that cannot be upgraded but need to be. But to get to PQC, organisations need to start now – putting it off will cost, money, time, and puts the organisation at risk.

2. Quantum Cybersecurity: The race for unhackable networks in a post-quantum world

by Sukanya Mandal
https://www.techcircle.in/2025/09/29/quantum-cybersecurity-the-race-for-unhackable-networks-in-a-post-quantum-world

As a data and artificial intelligence (AI) strategist, I've focused my career on realising the value of data. But now, my priority has shifted to protecting it. We are facing a quiet but serious crisis that threatens the very foundation of our digital world. It's known as the "Harvest Now, Decrypt Later" (HNDL) attack. This attack turns our most valuable long-term data—intellectual property, state secrets, financial records, and personal health information—into ticking time bombs.

Adversaries are intercepting and stockpiling today's encrypted data. They aren't breaking it now; they're waiting for the day when a powerful quantum computer can breach current encryption standards like RSA and ECC in just hours. For data that needs to stay secure for decades, the threat is not in the distant future; it's happening now. This shifts data protection from just a compliance task to an urgent strategic priority.

The global response to this serious threat has been strong. The U.S. NIST recently finalised its first set of post-quantum cryptography (PQC) standards after a multi-year global competition. New algorithms like ML-KEM (formerly CRYSTALS-Kyber) and ML-DSA (formerly CRYSTALS-Dilithium) are being developed to establish a quantum-resilient digital infrastructure. This is not just a technical upgrade; it's also a geopolitical race for the future of secure communication, as nations around the world push for adoption in critical infrastructure.

Here is where AI intersects with quantum security, creating a complex situation. On one hand, AI acts as a threat multiplier. Research shows AI can analyse energy usage to extract secret keys from PQC algorithms, demonstrating that even quantum-resistant algorithms are vulnerable to intelligent, AI-driven attacks on poorly implemented systems. Generative AI is already fueling highly realistic phishing and social engineering attacks at an unprecedented scale.

On the other hand, AI is also our most crucial defence tool. The first step towards a solution is conducting a thorough cryptographic inventory—a significant data discovery challenge. An organisation can't protect what it doesn't know it exists. AI-powered tools can automate this discovery process, scanning large IT networks to locate every instance of vulnerable cryptography. Beyond just inventory, AI can audit new PQC implementations for weaknesses, enhance performance, and create flexible, adaptive security measures. Imagine an AI-driven network that watches for threats and automatically switches between different PQC algorithms in real time, an idea known as crypto-agility. This represents the future of defense: confronting technological threats with advanced technology.

The journey to a quantum-safe future requires strategic planning, not just a simple fix. It starts with three immediate steps. First, organisations should form a dedicated team to manage the quantum-readiness roadmap. Second, they need to conduct a comprehensive cryptographic inventory, prioritising assets based on the long-term significance of the data they protect. Finally, they should engage with all technology vendors to understand their PQC transition timelines.

The migration will demand a substantial financial investment from governments and businesses worldwide. To illustrate the scale of this expense, the White House has estimated a cost of $7.1 billion for U.S. federal agencies alone. But this is not just an American issue. In Europe, Germany is mandating the transition for critical infrastructure by mid-2026. In Asia, countries like China and India are mobilizing their tech sectors. For a single large global company, the cost is projected to be between $7M and $12M. These figures are daunting, primarily due to the necessity of replacing old systems with secure cryptography. However, this investment is minor compared to the potential cost of a future quantum-enabled breach.

The time for deliberation has passed. The HNDL threat is live, the standards are set, and we have the tools for defense. We are racing not just to build a quantum computer, but to establish a quantum-safe data infrastructure before our adversaries can exploit one against us. By using AI as a key defensive strategy and following a smart, data-driven migration plan, we can succeed in this race.

3. New ML-KEM standard aims to protect data from future quantum attacks

by Devony Hof
https://siliconangle.com/2025/09/29/post-quantum-security-ml-kem-digicert/

Quantum experts are heralding the arrival of a new cryptographic algorithm, Module-Lattice-Based Key-Encapsulation Mechanism, or put more simply: ML-KEM.

Why prepare for post-quantum attacks when quantum computers don’t exist yet? Securing your data now is essential, according to Shane Kelly, principal crypto architect at DigiCert Inc.

“An attacker can take the data that you’re transmitting now,” he said. “They can store it somewhere and when there is a relevant quantum computer, they can start to decrypt it. The higher value your information, the more likely you’re going to be susceptible to this type of attack. Medical information, confidential information, banking information … that’s going to be susceptible.”

Kelly spoke with Lily Chen, mathematician at the National Institute of Standards and Technology, and Panos Kampanakis, principal security engineer of cryptography at Amazon Web Services Inc., for the DigiCert World Quantum Readiness Day event, during an encore broadcast on theCUBE, SiliconANGLE Media's livestreaming studio. They discussed the development of ML-KEM and the future of post-quantum cryptography, or PQC.

ML-KEM: Pure, hybrid or both?

ML-KEM is the recently standardized alternative to ECC or RSA key agreement schemes, with ML-KEM-768 chosen as the primary parameter set to replace widely used algorithms such as X25519. The pressure is on for quantum experts to guarantee that this set of algorithms will protect important data when "Q-day" arrives — the anticipated moment when quantum computers are powerful enough to break today's encryption.

"ML-KEM is considered secure enough to protect government data," Chen said. "The confidence is on the whole research community. This ML-KEM candidate has been in the public domain for five years with rigorous and extensive evaluation and analysis. The community is mature enough to make this decision to select ML-KEM as KEM for the quantum-resistant cryptography key encapsulation algorithm."

In the transition to PQC, cryptography architects have a choice between pure and hybrid algorithms. Pure PQC migration replaces all previous algorithms with quantum-resistant ones, whereas hybrid migration combines traditional public key algorithms with PQC algorithms. ML-KEM can be deployed with either option.

"The industry chose to deploy Kyber [the precursor to ML-KEM] in a hybrid format," Kampanakis said. "Now that we have ML-KEM, we still standardized groups that use ML-KEM in this hybrid scenario, it was basically very simple to switch to ML-KEM from Kyber."

Chen added that developing hybrid mode algorithms in alignment with current standards is necessary to prevent people from using unsafe, ad hoc hybrid algorithms. The goal is to meet companies' needs while staying within the NIST framework.

At AWS, engineers are developing a PQC migration strategy that combines security, flexibility and speed. The company is focused on creating cryptographic libraries that can be deployed consistently across multiple services, ensuring both interoperability and rapid adoption.

"The way we approach these deployments is by using building blocks that allow us to deploy in many services at the same time," Kampanakis said. "When I say building blocks, I mean cryptographic libraries that implement these algorithms. When you have these implementations and you trust them in your libraries, you basically have them deployed in many services that use them across the world."

4. Threat Actors Exploiting SonicWall Firewalls to Deploy Akira Ransomware Using Malicious Logins

by Guru Baran
https://cybersecuritynews.com/sonicwall-firewalls-akira-ransomware/

A new wave of cyberattacks targeting organizations using SonicWall firewalls has been actively deploying Akira ransomware since late July 2025.

Security researchers at Arctic Wolf Labs detected a surge in this activity, which remains ongoing. Threat actors are gaining initial access through malicious SSL VPN logins, successfully bypassing multi-factor authentication (MFA), and then rapidly moving to encrypt data within hours.

The campaign appears to be an opportunistic mass exploitation, affecting victims across various sectors. The initial point of entry is a malicious login to a SonicWall SSL VPN, often originating from Virtual Private Server (VPS) hosting providers instead of typical corporate networks.

Alarmingly, attackers have successfully authenticated against accounts protected with SonicWall's One-Time Password (OTP) MFA feature.

SonicWall has linked these malicious logins to CVE-2024-40766, an improper access control vulnerability disclosed in 2024.

The working theory is that threat actors harvested credentials from devices that were previously vulnerable and are now using them in this campaign, even if the devices have since been patched.

This explains why fully patched devices have been compromised, a fact that initially led to speculation about a potential zero-day exploit.

Once inside a network, the attackers operate with remarkable speed. The time from initial access to ransomware deployment, known as "dwell time," is often measured in hours, with some intrusions taking as little as 55 minutes, Arctic Wolf said. This extremely short window for response makes early detection critical.

Attack Sequence

Attackers use compromised credentials to log into SonicWall SSL VPNs, bypassing OTP MFA. Within minutes of logging in, attackers begin internal network scanning for open ports like SMB (445), RPC (135), and SQL (1433). They use tools like Impacket, SoftPerfect Network Scanner, and Advanced IP Scanner for discovery and lateral movement.

The threat actors create new administrator accounts, escalate privileges for existing accounts, and install remote management tools like AnyDesk, TeamViewer, and RustDesk to maintain access. They also establish persistence using SSH reverse tunnels and Cloudflare Tunnels.

To operate undetected, attackers attempt to disable endpoint security products like Windows Defender and other EDR solutions. They use a "bring-your-own-vulnerable-driver" (BYOVD) technique to tamper with security software at the kernel level and delete Volume Shadow Copies to prevent system restoration.

Before encryption, attackers steal sensitive data. They package files using WinRAR and exfiltrate them with tools like `rclone` and FileZilla. Finally, they deploy the Akira ransomware (using executables named `akira.exe` or `locker.exe`) to encrypt network drives and demand a ransom.

Arctic Wolf recommends that organizations using SonicWall devices take immediate action. The most critical step is to reset all SSL VPN credentials, including related Active Directory accounts, especially if the devices have ever run firmware vulnerable to CVE-2024-40766. Patching alone is insufficient if credentials have already been compromised.

Organizations should also monitor for suspicious VPN logins from hosting providers and look for anomalous SMB activity indicative of Impacket use.

5. Cryptographic Backdoors in Neural Networks Enable Robust Watermarking, Authentication and IP Tracking

by Rohail T.
https://quantumzeitgeist.com/neural-networks-cryptographic-backdoors-enable-robust-watermarking-authentication-tracking/#google_vignette

The increasing reliance on neural networks creates vulnerabilities to malicious interference, and researchers are now demonstrating that these networks can harbour hidden cryptographic backdoors with both destructive and protective potential. Anh Tu Ngo, Anupam Chattopadhyay, and Subhamoy Maitra, from Nanyang Technological University and the Indian Statistical Institute, reveal how a carefully implanted cryptographic backdoor enables powerful, undetectable attacks on neural networks. However, this same technology also underpins robust solutions for watermarking, user authentication, and tracking the unauthorised sharing of valuable intellectual property. The team proves these defensive protocols resist attacks even from adversaries with complete access to the network, representing a significant step towards securing machine learning systems and establishing trust in their operation.

Considering defence applications, scientists present a provably robust neural network watermarking scheme, a protocol for guaranteeing user authentication, and a protocol for tracking unauthorized sharing of neural network intellectual property. This work demonstrates that these practical implementations are provably robust, resisting adversaries with black-box access to the neural network.

Cryptography Secures Deep Learning Against Backdoors

This research investigates backdoor attacks and defenses in deep learning models, focusing on cryptographic techniques for securing models and detecting or preventing attacks. Scientists explore methods for injecting backdoors into models, identifying their presence, and protecting model intellectual property. A key focus is developing cryptographic techniques to create more robust and secure deep learning systems. Backdoor attacks, also known as Trojan attacks, involve injecting hidden triggers into a model during training, causing misclassification when the trigger is present in an input. Researchers are developing detection techniques to identify backdoored models by analyzing model behavior and looking for anomalies.

Robust training strategies aim to make models more resilient to backdoor attacks during training, while input filtering techniques attempt to remove or neutralize potential triggers from input data. A significant

aspect of this work involves cryptographic watermarking, embedding cryptographic signatures into model weights to prove ownership and detect tampering. Secure aggregation uses cryptographic protocols to securely combine model updates during federated learning, preventing malicious participants from injecting backdoors. Homomorphic encryption allows computations on encrypted data, enabling secure inference without revealing the model or input data.

Researchers are also exploring cryptographic transformers, using cryptographic circuits within the model architecture to enhance security. The team utilizes digital signature schemes, such as Dilithium, for model authentication and integrity verification, and hash functions for message authentication and data integrity. Watermarking techniques embed unique patterns into the model to identify its origin and prevent unauthorized copying, while adversarial examples reveal information about the model's internal workings. Sample correlation analysis identifies potential model theft. This research is important because it addresses a critical security challenge in deep learning, protecting models from malicious attacks as they become increasingly prevalent in critical applications like autonomous vehicles and healthcare. The use of cryptography offers a promising approach to enhancing the security and trustworthiness of these models.

Cryptographic Backdoors Secure Neural Networks Effectively

Scientists have demonstrated the effectiveness of cryptographic backdoors within neural networks, achieving both powerful attack capabilities and robust defense mechanisms. This work extends theoretical foundations by linking a cryptographic backdoor directly to adversarial attacks on image classification tasks. The team implemented a digital signature-based backdoor, enabling undetectable manipulation of neural network behavior. Beyond attacks, researchers established three practical applications leveraging these backdoors for enhanced security. They developed a provably robust neural network watermarking scheme, allowing verification of intellectual property ownership.

Furthermore, the team designed a protocol for guaranteeing user authentication and another for tracking unauthorized sharing of neural network intellectual property. These protocols resist adversaries with black-box access to the neural network. Experiments confirm the effectiveness of these protocols, demonstrating their ability to safeguard neural network privacy. Researchers also measured the computational overhead of these applications, verifying their practicality for real-world deployment. The work lays the foundation for quantum-era machine learning applications by utilizing post-quantum cryptographic primitives for implementing the backdoors. This breakthrough delivers a versatile toolkit for securing neural networks, offering both offensive and defensive capabilities with provable robustness.

Backdoors Enable Secure Neural Network Control

This research demonstrates the potential of cryptographic backdoors embedded within neural networks, achieving both powerful attack capabilities and robust defensive mechanisms. Scientists have shown that a carefully constructed backdoor allows for a potent, yet undetectable, attack on a neural network, while simultaneously enabling applications such as secure watermarking, user authentication, and intellectual property tracking. The core achievement lies in proving that these defensive protocols resist adversaries with black-box access to the network, relying on the inaccessibility of the secret key. Experimental results corroborate these theoretical findings, demonstrating effective model ownership verification through watermarking, legitimate user access control via authentication, and source tracing of distributed models through IP tracking.

The team successfully constructed a cryptographic backdoor that operates in parallel with the host neural network, a novel approach with implications for both beneficial and malicious applications. While the research acknowledges limitations, including computational costs, the authors suggest potential optimizations through parallel computing. Future work aims to extend these schemes, building on existing research but adapting it for use with modern machine learning techniques.

6. SuperQ Quantum Releases Post-Quantum Cryptography AI

by Matt Swayne
https://thequantuminsider.com/2025/09/28/superq-quantum-releases-post-quantum-cryptography-pqc-ai/

SuperQ Quantum Computing Inc., a global leader in quantum and supercomputing, is pleased to announce the release of Super™ PQC Analyst, the first in-market component of the Company's forthcoming Super™ PQC Module. Available immediately, Super™ PQC Analyst performs exhaustive, automated diagnostics on Web3 and Web2 infrastructure – from permissionless blockchains and DeFi protocols to conventional websites, APIs and cloud environments – grading their post-quantum readiness and delivering prioritized, standards-aligned mitigation strategies that can be executed through SuperQ's PQC Professional Services team.

Post-quantum cryptography is no longer a distant concern; it is a "today problem". Bad-actor "harvest-now, decrypt-later" campaigns are already siphoning encrypted traffic and wallet data in anticipation of future quantum breakthroughs. At the All-In Summit 2025, Solana co-founder Anatoly Yakovenko warned that there is a "50/50 chance" that quantum computers will be powerful enough within five years to break the cryptographic protections securing Bitcoin wallets. "We should migrate Bitcoin to a quantum-resistant signature scheme," he further added as quoted by Coindesk. Such risk applies equally to every ECDSA- or RSA-based system powering Web2 finance, healthcare, e-commerce and critical infrastructure.

"Enterprises and blockchain networks can no longer wait for a 'Day Zero' quantum event," said Dr. Muhammad Khan, CEO and Board Chair of SuperQ**.** "Super™ PQC Analyst gives CIOs, CISOs and protocol developers a clear, data-driven snapshot of their vulnerability surface and an actionable roadmap to migrate – before quantum computers catch up."

Why the Market Needs Super™ PQC Analyst Now

Independent forecasts by the likes of Grand View Research put global cybersecurity spending at US $272 billion in 2025, rising to over US $500 billion by 2030, with quantum-safe upgrades representing one of the fastest-growing segments. In parallel, the cryptocurrency market cap, which sits at USD $3.9 trillion today according to Coinmarketcap, is projected to hit US $25 trillion by 2030 according to ARK Invest. This is driven by more than 659 million cryptocurrency users [Crypto.com Report] and on-chain stablecoin settlement volumes that surpassed US $5.7 trillion in 2024 [Visa Economic Empowerment Institute Report]. By offering a unified PQC readiness engine for both environments, SuperQ is opening a significant addressable market for its platform and professional services.

Key Features of Super™ PQC Analyst

- **Deep Analysis Engine**: Scans TLS endpoints, smart-contract bytecode, wallet libraries and key-management workflows to detect quantum-vulnerable cryptography, exposed public keys and susceptible transport layers.
- **Readiness Scoring Reporting**: Benchmarks posture against NIST, ETSI and Canadian Centre for Cyber Security migration guidelines, producing board-level dashboards and developer-level task lists.
- **Mitigation Strategy Generator**: Recommends concrete steps such as Kyber/Dilithium key-exchange upgrades, lattice-based signature schemes, quantum-secure randomness sources and hybrid transition patterns.
- **Implementation Pathways**: Handover to SuperQ PQC Professional Services team for consulting on and implementation of the PQC strategy.

Roadmap to the Full Super™ PQC Module

Today's (27 Sep 2025) release is the first milestone in a comprehensive Super™ PQC Module scheduled for commercial availability in Q4 2025. The full suite will bundle:

- **End-to-end software libraries** (SDKs, APIs, smart-contract templates) for quantum-safe encryption, signatures and key management.
- **Hardware accelerators and secure elements** designed in collaboration with semiconductor partners to offload lattice and code-based primitives.
- **Cloud, blockchain and on-prem deployment artifacts** enabling enterprises and decentralized networks to adopt PQC with minimal disruption**.**

SuperQ will continue to expand its network of Super™ Hubs and university collaborations to validate, pilot and scale these solutions worldwide.

7. Securing today for the quantum future: WARP client now supports post-quantum cryptography (PQC)

by Sharon Goldberg, Tochukwu Nkemdilim (Toks), and Koko Uko
https://blog.cloudflare.com/post-quantum-warp/

The Internet is currently transitioning to post-quantum cryptography (PQC) in preparation for Q-Day, when quantum computers break the classical cryptography that underpins all modern computer systems. The US National Institute of Standards and Technology (NIST) recognized the urgency of this transition, announcing that classical cryptography (RSA, Elliptic Curve Cryptography (ECC)) must be deprecated by 2030 and completely disallowed by 2035.

Cloudflare is well ahead of NIST's schedule. Today, over 45% of human-generated Internet traffic sent to Cloudflare's network is already post-quantum encrypted. Because we believe that a secure and private Internet should be free and accessible to all, we're on a mission to include PQC in all our products, without specialized hardware, and at no extra cost to our customers and end users.

That's why we're proud to announce that Cloudflare's WARP client now supports post-quantum key agreement — both in our free consumer WARP client 1.1.1.1, and in our enterprise WARP client, the Cloudflare One Agent.

Post-quantum tunnels using the WARP client

This upgrade of the WARP client to post-quantum key agreement provides end users with immediate protection for their Internet traffic against harvest-now-decrypt-later attacks. The value proposition is clear — by tunneling your Internet traffic over the WARP client's post-quantum MASQUE tunnels, you get immediate post-quantum encryption of your network traffic. And this holds even if the individual connections sent through the tunnel have not yet been upgraded to post-quantum cryptography.

Here's how it works.

When the Cloudflare One Agent (our enterprise WARP client) connects employees to the internal corporate resources as part of the Cloudflare One Zero Trust platform, it now provides end-to-end quantum encryption of network traffic. As shown in the figure below, traffic from the WARP client is wrapped in a post-quantum encrypted MASQUE (Multiplexed Application Substrate over QUIC Encryption) tunnel, sent to Cloudflare's global network network (link (1)). Cloudflare's global network then forwards the traffic another set of post-quantum encrypted tunnels (link (2)), and then finally on to the internal corporate resource using a post-quantum encrypted Cloudflare Tunnel established using the cloudflared agent (which installed near the corporate resource) (link (3)).

When an end user installs the consumer WARP Client (1.1.1.1), the WARP client wraps the end user's network traffic in a post-quantum encrypted MASQUE tunnel. As shown in the figure below, the MASQUE tunnel protects the traffic on its way to Cloudflare's global network (link (1)). Cloudflare's global network then uses post-quantum encrypted tunnels to bring the traffic as close as possible to its final destination (link (2)). Finally, the traffic is forwarded over the public Internet to the origin server (i.e. its final destination). That final connection (link (3)) may or may not be post-quantum (PQ). It will not be PQ if the origin server is not PQ. It will be PQ if the origin server is (a) upgraded to PQC, and (b) the end user is connecting to over a client that supports PQC (like Chrome, Edge or Firefox). In the future, Automatic SSL/TLS will ensure that your entire connection will be PQ as long as the origin server is behind Cloudflare and supports PQ connections (even if your browser doesn't).

The cryptography landscape

Before we get into the details of our upgrade to the WARP client, let's review the different cryptographic primitives involved in the transition to PQC.

Key agreement is a method by which two or more parties can establish a shared secret key over an insecure communication channel. This shared secret can then be used to encrypt and authenticate subsequent communications. Classical key agreement in Transport Layer Security (TLS) typically uses the Elliptic Curve Diffie Hellman (ECDH) cryptographic algorithm, whose security can be broken by a quantum computer using Shor's algorithm.

We need post-quantum key agreement today to stop harvest-now-decrypt-later attacks, where attackers collect encrypted data today, and then decrypt it in future once powerful quantum computers become available. Any institution that deals with data that could still be valuable ten years in the future (governments, financial institutions, healthcare organizations, and more) should deploy PQ key agreement to prevent these attacks.

This is why we upgraded the WARP client to post-quantum key agreement.

Post-quantum key agreement is already quite mature and performant; our experiments have shown that deploying the post-quantumModule-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) algorithm in hybrid mode (in parallel with classical ECDH) over TLS 1.3 is actually more performant than using TLS 1.2 with classical cryptography.

Post-quantum digital signatures and certificates, by contrast, are still in the process of being standardized for use in TLS and the Internet's Public Key Infrastructure (PKI). PQ signatures and certificates are required to prevent an active attacker who uses a quantum computer to forge a digital certificate/signature and then uses it to decrypt or manipulate communications by impersonating a trusted server. As far as we know, we don't have such attackers yet, which is why post-quantum signatures and certificates are not widely deployed across the Internet. We have not yet upgraded the WARP client to PQ signatures and certificates, but we plan to do so soon.

A unique challenge: PQC upgrade in the WARP client

While Cloudflare is on the forefront of the PQC transition, a different kind of challenge emerged when we upgraded our WARP client. Unlike a server that we fully control and can hotfix at any time, our WARP client runs directly on end user devices. In fact, it runs on millions of end user devices that we do not control. This fundamental difference means that every time we update the WARP client, our release must work properly on the first try, with no room for error.

To make things even more challenging, we need to support the WARP client across five different operating systems (Windows, macOS, Linux, iOS, and Android/ChromeOS), while also ensuring consistency and reliability for both our consumer 1.1.1.1 WARP client and our Cloudflare One Agent. In addition, because the WARP client relies on the fairly new MASQUE protocol, which the industry only standardized in August 2022, we need to be extra careful to make sure our upgrade to post-quantum key agreement does not expose latent bugs or instabilities in the MASQUE protocol itself.

All these challenges point to a slow and careful transition to PQC in the WARP client, while still supporting customers that want to immediately activate PQC. To accomplish this, we used three techniques:

1. temporary PQC downgrades,
2. gradual rollout across our WARP client population, and
3. a Mobile Device Management (MDM) override.

Let's take a deep dive into each.

Temporary PQC downgrades

As we roll out PQ key agreement in MASQUE to the WARP client, we want to make sure we don't have WARP clients that struggle to connect due to an error, middlebox, or a latent implementation bug triggered by our PQC migration. One way to accomplish this level of robustness is to have clients downgrade to a classic cryptographic connection if they fail to negotiate a PQ connection.

To really understand this strategy, we need to review the concept of cryptographic downgrades. In cryptography, a downgrade attack is a cyber attack where an attacker forces a system to abandon a secure cryptographic algorithm in favor of an older, less secure, or even unencrypted one that allows the attacker to introspect on the communications. Thus, when newly rolling out a PQ encryption, it is standard practice to ensure that: if the client and server *both* support PQ encryption, it should not be possible for an attacker to downgrade their connection to a classic encryption.

Thus, to prevent downgrade attacks, we should ensure that if the client and server both support PQC, but fail to negotiate a PQC connection, then the connection will just fail. However, while this prevents downgrade attacks, it also creates problems with robustness.

We cannot have both robustness (i.e. the ability for client to downgrade to a classical connection if the PQC fails) and security against downgrades (i.e. the client is forbidden to downgrade to classical cryptography once it supports PQC) at the same time. We have to choose one. For this reason, we opted for a phased approach.

- **Phase 1:** Automated PQC downgrades. We start by choosing robustness at the cost of providing security against downgrade attacks. In this phase, we support automated PQC downgrades – if a client fails to negotiate a PQC connection, it will downgrade to classical cryptography. That way, if there are bugs or other instability introduced by PQC, the client automatically downgrades to classical cryptography and the end user will not experience any issues. (Note: because MASQUE establishes a single very long-lived TLS connection only when the user logs in, an end user is unlikely to notice a downgrade.)

- **Phase 2:** PQC with security against downgrades. Then, once the rollout is stable and we are convinced that there are no issues interfering with PQC, we will choose security against downgrade attacks over robustness. In this phase, if a client fails to negotiate a PQC connection, the connection will just fail, which provides security against downgrade attacks.

To implement this phased approach, we introduced an API flag that the client uses to determine how it should initiate TLS handshakes, which has three states:

- **No PQC:** The client initiates a TLS handshake using classical cryptography only. .
- **PQC downgrades allowed:** The client initiates a TLS handshake using post-quantum key agreement. If the PQC handshake negotiation fails, the client downgrades to classical cryptography. This flag supports Phase 1 of our rollout.
- **PQC only:** The client initiates a TLS handshake using post-quantum key agreement cryptography. If the PQC handshake negotiation fails, the connection fails. This flag supports Phase 2 of our rollout.

The WARP desktop version 2025.5.893.0, iOS version 1.11 and Android version 2.4.2 all support post-quantum key agreement along with this API flag.

With this as our framework, the next question becomes: what timing makes sense for this phased approach?

Gradual rollout across the WARP client population

To limit the risk of errors or latent implementation bugs triggered by our PQC migration, we gradually rolled out PQC across our population of WARP clients.

In Phase 1 of our rollout, we prioritized robustness rather than security against downgrade attacks. Thus, initially the API flag is set to "No PQC" for our entire client population, and we gradually turn on the "PQC downgrades allowed" across groups of clients. As we do this, we monitor whether any clients downgrade from PQC to classical cryptography. At the time of this writing, we have completed the Phase 1 rollout to all of our consumer WARP (1.1.1.1) clients. We expect to complete Phase 1 for our Cloudflare One Agent by the end of 2025.

Downgrades are not expected during Phase 1. In fact, downgrades indicate that there may be a latent issue that we have to fix. If you are using a WARP client and encounter issues that you believe might be related to PQC, you can let us know by using the feedback button in the WARP client interface (by clicking the bug icon in the top-right corner of the WARP client application). Enterprise users can also file a support ticket for the Cloudflare One Agent.

We plan to enter Phase 2 — where the API flag is set to "PQC only" in order to provide security against downgrade attacks — by summer of mid 2026.

MDM override

Finally, we know that some of our customers may not be willing to wait for us to complete this careful upgrade to PQC. So, those customers can activate PQC right now.

We've built a Mobile Device Management (MDM) override for the Cloudflare One Agent. MDM allows organizations to centrally manage, monitor, and secure mobile devices that access corporate resources; it works on multiple types of devices, not just mobile devices. The override for the Cloudflare One Agent allows an administrator (with permissions to manage the device) to turn on PQC. To use the MDM post-quantum override, set the 'enable_post_quantum' MDM flag to true. This flag takes precedence over the signal from the API flag we described earlier, and will activate PQC without downgrades. With this setting, the client will only negotiate a PQC connection. And if the PQC negotiation fails, the connection will fail, which provides security against downgrade attacks.

Ciphersuites, FIPS and Fedramp

The Federal Risk and Authorization Management Program (FedRAMP) is a U.S. government standard for securing federal data in the cloud. Cloudflare has a FedRAMP certification that requires that we use cryptographic ciphersuites that comply with FIPS (Federal Information Processing Standards) for certain products that are inside our FIPS boundary.

Because the WARP client is inside Cloudflare's FIPS boundary for our FedRAMP certification, we had to ensure it uses FIPS-compliant cryptography. For internal links (where Cloudflare controls both sides of the connection) within the FIPS boundary, we currently use a hybrid key agreement consisting of FIPS-compliant EDCH using the P256 Elliptic curve, in parallel with an early version of ML-KEM-768 (which we started using before the ML-KEM standards were finalized) — a key agreement called P256Kyber768Draft00. To observe this ciphersuite in action in your WARP client, you can use the warp-cli tunnel stats utility. Here's an example of what we find when PQC is enabled:

PQC tunnels for everyone

We believe that PQC should be available to everyone, without specialized hardware, at no additional cost. To that end, we're proud to help shoulder the burden of the Internet's upgrade to PQC.

A powerful strategy is to use tunnels protected by post-quantum key agreement to protect Internet traffic, in bulk, from harvest-now-decrypt-later attacks – even if the individual connections sent through the tunnel have not yet been upgraded to PQC. Eventually, we will upgrade these tunnels to also support post-quantum signatures and certificates, to stop active attacks by adversaries armed with quantum computers after Q-Day.

This staged approach keeps up with Internet standards. And the use of tunnels provides customers and end users with built-in *cryptographic agility*, so they can easily adapt to changes in the cryptographic landscape without a major architectural overhaul.

Cloudflare's WARP client is just the latest tunneling technology that we've upgraded to post-quantum key agreement. You can try it out today for free on personal devices using our free consumer WARP client 1.1.1.1, or for your corporate devices using our free zero-trust offering for teams of under 50 users or a paid enterprise zero-trust or SASE subscription. Just download and install the client on your Windows, Linux, macOS, iOS, Android/ChromeOS device, and start protecting your network traffic with PQC.

Cloudflare's connectivity cloud protects entire corporate networks, helps customers build Internet-scale applications efficiently, accelerates any website or Internet application, wards off DDoS attacks, keeps hackers at bay, and can help you on your journey to Zero Trust.

Visit 1.1.1.1 from any device to get started with our free app that makes your Internet faster and safer.

8. NCCoE white paper maps migration to quantum-resistant cryptography against NIST CSF, SP 800-53 controls

by Anna Ribeiro
https://industrialcyber.co/nist/nccoe-white-paper-maps-migration-to-quantum-resistant-cryptography-against-nist-csf-sp-800-53-controls/

The U.S. NIST, through the National Cybersecurity Center of Excellence (NCCoE), released a paper outlining the supported and dependent characteristics of capabilities in NIST's Migration to Post-Quantum

Cryptography project and mapping them to the NIST Cybersecurity Framework 2.0 and Special Publication 800-53 Revision 5. It highlights capabilities in Discovery and Inventory, Interoperability, and Performance. The public comment period for this draft is open through Oct. 20, this year.

In its Cybersecurity White Paper (CSWP) 48, '*Mappings of Migration to PQC Project Capabilities to Risk Framework Documents,*' the NCCoE identified that its Migration to Post-Quantum Cryptography project demonstrates practices to ease the transition from current public-key algorithms to quantum-resistant alternatives. The project's Cryptographic Discovery workstream uses discovery and inventory tools to help organizations understand where and how cryptography protects the confidentiality and integrity of critical data and systems. It also examines how cryptographic inventories can guide risk management and prioritize the adoption of NIST-standardized post-quantum algorithms.

The Interoperability and Performance workstream evaluates how NIST PQC algorithms for key establishment and digital signatures function within communication protocols such as TLS and SSH, as well as with hardware security modules (HSMs). The demonstrated capabilities support security objectives and controls defined in the NIST Cybersecurity Framework 2.0 and SP 800-53, while their responsible implementation depends on adherence to these same frameworks.

The NCCoE Migration to Post-Quantum Cryptography project demonstrates practices to ease migration from current public-key cryptographic algorithms to quantum-resistant alternatives. Project collaborators use cryptographic discovery and inventory tools to help organizations understand where and how cryptography protects the confidentiality and integrity of critical data and systems. They are also exploring the interoperability of NIST PQC algorithms for key establishment and digital signatures in internet communication protocols and HSMs.

The Migration to PQC Project's Quantum-Vulnerable Cryptography Discovery Workstream demonstrates tools for identifying quantum-vulnerable cryptographic algorithms in code development pipelines, software lifecycle components, network services and protocols, and end-user systems and servers. The project provides insights for planning a migration roadmap using a risk-based approach.

Identifying hardware and software assets as part of an inventory is a core function of the Cybersecurity Framework and a prerequisite for effective cybersecurity risk management. This project extends inventory capabilities by discovering cryptographic assets and correlating findings with existing hardware, software, and services inventories. It demonstrates a combination of active and passive cryptographic discovery and inventory technologies.

Interoperability testing of NIST pre-standardized PQ cryptographic algorithms is a core focus to support technology vendors and standards bodies in migrating and developing products that utilize PQC. Benchmarking performance metrics from lab tests helps consortium members and vendors optimize implementations for production-ready use. Understanding these metrics is key to guiding technology providers in offering solutions that support organizational migrations and identifying which PQ algorithms are best suited for specific use cases.

The white paper detailed that the Interoperability and Performance Workstream's consortium members contributed working implementations of selected NIST PQC algorithms across testing scenarios for TLS, QUIC, SSH, and hardware security modules (HSMs). Collaborators implemented these algorithms in a lab environment, gaining practical experience and advancing to the three NIST PQC standards published in

August 2024. Interoperability testing included successful communication between lab server implementations using PQC, and performance measurements documented metrics such as the maximum TLS 1.3 handshake rate.

The Migration to PQC project also highlights outcomes from consortium members engaged in standardizing PQC adoption with organizations such as the Internet Engineering Task Force (IETF).

The white paper also provides mappings between the cybersecurity functions of the logical architecture components demonstrated in the project's lab and the security characteristics outlined in relevant cybersecurity documents. These mappings are intended for organizations implementing PQC migration tools or already using PQC.

Logical architecture components for discovery and inventory tools include cryptographic data collection tools, cryptographic inventory tools, cryptographic analytics tools, and certificate discovery and management tools. Components for post-quantum cryptography implementations in the interoperability and performance workstream include quantum-ready algorithm implementations, quantum-ready cryptographic service implementations, quantum-ready integration tools and application plugins, quantum-ready certificate authority implementations, and quantum-ready hardware security modules (HSMs).

The mappings illustrate how cybersecurity functions from the project's reference design align with NIST-recommended security outcomes and controls, including subcategories from the NIST Cybersecurity Framework 2.0 and controls from NIST SP 800-53. All elements, Logical Architecture Components, component functions, NIST Cybersecurity Framework (CSF) subcategories, and SP 800-53 controls, support ways to reduce cybersecurity risk.

The NCCoE also provided a mapping of tools supporting migration to quantum-resistant algorithms to the CSF. It includes CSF outcomes required for the secure operation of the tools as well as outcomes supported by the platform. The current PQC migration project does not involve the operational use of cryptographic systems; it focuses solely on laboratory demonstrations and measurements in a controlled environment. Consequently, many organizational and operational security objectives do not apply to these mappings.

The white paper also provides a mapping of tools and products that support migration to quantum-resistant algorithms to SP 800-53 controls. It includes controls required for the secure operation of the tools as well as controls supported by the platform. As with the CSF mappings, the current PQC migration project does not involve operational use of cryptographic systems; it focuses solely on laboratory demonstration and measurement in a controlled environment. Consequently, many organizational and operational security controls do not apply.

Since its release in 2014, the NIST CSF has been used by communities with shared interests in cybersecurity risk management. CSF 2.0 refers to 'Community Profiles,' which describe how organizations use CSF Profiles to develop risk management guidance applicable to multiple organizations, distinguishing them from Organizational Profiles that are not publicly shared. A Community Profile can be seen as guidance for a specific community organized around the common taxonomy of the CSF.

The NCCoE provides a guide describing Community Profiles, offering a template, guidance on content, and a Community Profile Lifecycle (Plan, Develop, Use, Maintain). Communities can use this guide to create profiles that support their shared priorities.

"For Migration to Post-Quantum Cryptography, we encourage communities to come together to develop a community profile that will allow the community to use consistent language and build relationships to share practices that ease the community's migration to PQC," the NCCoE white paper mentioned. "One organization has created a cryptographic resilience community profile; your organization could reference that to develop its plan for migration to post-quantum cryptography or quantum readiness efforts to reduce the risk from the threat of a cryptanalytically relevant quantum computer."

In March, the NIST released a status report on the fourth round of its post-quantum cryptography standardization process that aims to establish cryptographic standards that can withstand the potential threats posed by quantum computers, which are expected to have the capability to break many of the cryptographic systems currently in use. The agency also detailed a new algorithm for post-quantum encryption called HQC, which will serve as a backup for ML-KEM, short for Module-Lattice-Based Key-Encapsulation Mechanism, the main algorithm for general encryption.

9. Quantum resilience: Quantum cryptography will protect the future of the global network equipment supply chain

https://www.digitimes.com/news/a20250923PR202.html?chid=9

The modern digital supply chain is no longer a traditional linear sequence but a complex, interconnected ecosystem of suppliers, sellers, logistics providers, and customers.

PQC strengthens supply chain cybersecurity and ensures the security of IoT and operational technology devices.

While digital transformation greatly improves efficiency, it also exponentially expands the overall attack surface. In this model, risks are no longer isolated but systemic and cascading. Supply chain efficiency is built on an implicit digital trust model between partners, which is manifested through application programming interfaces (APIs), shared portals, and integrated software. However, this trust structure, built in pursuit of efficiency, has become a primary attack vector. Cybercriminals are no longer just breaking through firewalls—they are exploiting the fundamental fabric of digital collaboration. As a result, the traditional perimeter defense model is outdated; The new perimeter of defense is the entire supply chain ecosystem, and its security must be built on a zero-trust model enforced with cryptography.

Third-party or fourth-party vulnerabilities

Attackers often use the weakest link in the chain—often smaller, poorly secured vendors—as a springboard to infiltrate the network of their ultimate high-value target. This highlights a stark reality: an organization's security posture is only as strong as its least secure partners. This risk stems from the pursuit of supply chain efficiency, as the smooth operation of business processes requires granting partners a considerable

degree of access. This expansion of access rights, without corresponding strict security controls, constitutes a systemic vulnerability based on excessive trust.

The fundamental role of traditional cryptography and its limitations

Current supply chain security relies heavily on traditional public key cryptography (such as RSA, ECC) to protect data in transit and at rest. Mitigation strategies such as data encryption (using AES), risk assessment, and incident response plans are crucial, but their effectiveness is built on the strength of these underlying cryptographic algorithms. While these methods are still effective against today's threats, the entire security foundation is fragile and faces an existential threat that will be the focus of the next section.

Quantum Horizons: A Paradigm Shift in Cryptographic Threats

Quantum computers use quantum mechanical principles such as superposition and entanglement to solve mathematical problems (e.g., integer factorization, discrete logarithms) that form the security basis of today's public key cryptography (RSA, ECC, Diffie-Hellman). This is not a purely theoretical deduction, but a major engineering challenge that is making rapid progress. Once a quantum computer with sufficient scale and stability comes out, the current encryption system that protects global digital communications will fail in an instant.

"Get First, Decrypt Later" (HNDL): An imminent danger

The Harvest Now, Decrypt Later (HNDL) attack transforms the quantum threat from a futuristic problem to a present reality. The mechanism is that attackers, especially state-state actors, are actively intercepting and storing large amounts of today's encrypted data. These attacks target information with long-term value, such as intellectual property, government secrets, financial records, medical data, and personally identifiable information (PII).

This means that by the time a "Cryptographically Relevant Quantum Computer" (CRQC) appears that can crack current encryption algorithms (known as "Q-Day", which is expected to arrive as early as 2035), these obtained data will be retroactively deciphered. Therefore, the security of any sensitive data transmitted today that requires long-term confidentiality is already at risk.

This attack pattern transforms a company's data retention policy into a huge potential security liability. Regulations such as the Health Insurance Portability and Accountability Act (HIPAA) or the General Data Protection Regulation (GDPR) often require organizations to retain data for an extended period. The HNDL attack vector turns this legal compliance requirement into a potential ticking time bomb. Organizations are legally required to encrypt data stored for years, making it an ideal target for HNDL attacks. This creates a direct conflict between compliance and security: the act of adhering to data retention regulations inadvertently creates vulnerabilities for future quantum decryption threats. Therefore, risk management and legal teams must be immediately involved in the migration strategy of post-quantum cryptography. This is no longer just an IT issue, but a simmering corporate governance and compliance crisis.

.
.
.

Secure the edge: Protect IoT and operational technology equipment in the supply chain

Internet of Things (IoT) and operational technology (OT) devices face the biggest challenges in PQC migration for the following reasons:

- **Long life cycle:** The device may be used in the field for 10-20 years without replacement.
- **Limited resources:** Limited processing power, memory, and energy budgets.
- **Lack of Updability:** Many devices are not designed to be conducive to easy firmware or cryptography updates.

The application of PQC in these areas will be gradual and there will be significant differences between the old and new systems. For "greenfield" systems, such as new IoT product lines, PQC can be integrated from the outset. For "brownfield" systems, such as existing factory OT equipment, the challenge is enormous, often requiring the entire hardware to be replaced. This means that the PQC migration of the supply chain will be a two-speed process. Businesses must prioritize the adoption of PQC in new systems while developing long-term, potentially costly, retirement or retrofit capital plans for existing assets that are not quantum-safe.

Use cases for PQC include:

- **Industrial automation:** Protecting communication between sensors, controllers, and management systems in factories and processing plants.
- **Smart Infrastructure and Logistics:** Protecting smart grid equipment, traffic control systems, and connected logistics sensors.
- **Automotive V2X Communication:** Secure vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications to ensure security and prevent malicious manipulation.
- **Healthcare Supply Chain:** Ensuring the integrity and privacy of data from connected medical devices.

Conclusion and recommendations

Winbond's W77Q Secure Flash Memory is a robust solution to address the PQC threats mentioned above. Key PQC-Safe features of the W77Q Secure Flash include:

- **Platform Resilience:** In accordance with NIST 800-193 recommendations, the system automatically detects unauthorized program changes and can automatically restore to a secure state to avoid potential cyberattacks.
- **Security Software Update and Fallback Protection:** Supports remote security software updates while preventing fallback attacks, ensuring that only legitimate updates can be executed. To maintain the highest level of security and integrity, the W77Q adopts the quantum-secure Leighton-Micali signature (LMS) algorithm recommended by NIST Special Publication 800-208 to ensure the authenticity and integrity of updated software, providing additional security
- **Secure Supply Chain:** Secure Flash ensures the origin and integrity of flash content at every stage of the supply chain. The W77Q implements LMS-OTS-based remote authentication (NIST 800-208). This advanced method effectively prevents content tampering and misconfiguration during assembly, transportation, and configuration, protecting the platform from cyberattacks.

10. Quantum Computing Companies in 2025: Mapping the Global Quantum Landscape

by James Dargan
https://thequantuminsider.com/2025/09/23/top-quantum-computing-companies/

The development of quantum computing companies over the last decade continues to accelerate, driven by the ambition to develop quantum processors and the tools, both hardware and software, that support them.

This article presents a snapshot of the evolving quantum computing ecosystem, as it stands today and heading into 2026.

If you're seeking deeper insights into these quantum companies, regularly updated and enhanced by our analyst team, you may want to explore our Quantum Intelligence Platform.

Quantum Computing's Role Across Industries

Quantum computing is steadily gaining ground in sectors like healthcare, energy, and finance, offering new ways to approach previously intractable computational problems. Unlike other complex technologies such as artificial intelligence (AI) or virtual reality (VR), quantum computing often remains a mystery to the broader public, understood in depth only by experts in the field.

Quantum computing is expected to perform tasks that are currently out of reach for classical systems, powered by purpose-built hardware and software stacks. Companies across the space are working to make this powerful technology more accessible and usable.

As technological breakthroughs continue to unfold, the quantum landscape is expanding rapidly. Here, we explore how the ecosystem of quantum computing companies has taken shape over the last two decades.

Where Does Our Data Come From?

While our list highlights over seventy leading quantum players, it represents only a snapshot of the broader quantum landscape we track through our Quantum Data Intelligence Platform – the world's leading market intelligence source dedicated to quantum technologies.

The platform aggregates and curates comprehensive data from across the global quantum ecosystem, including companies, investors, academic groups, and government initiatives, applying a custom taxonomy and metadata system designed to segment and classify the sector with precision. It combines AI-enhanced big data collection with expert analyst insights, ensuring that funding flows, strategic partnerships, and quantum technology developments are consistently updated, contextualized, and made actionable. By drawing on this foundation, our coverage not only spotlights the innovators shaping the quantum market today but also provides readers with a reliable, data-backed view of how the industry is advancing toward commercial quantum advantage.

Due to space constraints, this list of quantum computing companies is not exhaustive, and some quantum communications or cybersecurity firms are included only where they overlap with key hardware or software developments. Our classification reflects the dual nature of the quantum industry: a race led by incumbents with deep pockets and infrastructure, and a wave of nimble startups carving out novel approaches to quantum engineering, error correction, simulation, and more.

This company list is current as of summer 2025.

Top Quantum Computing Companies in 2025

Leading Big Tech & Public Companies In Quantum (In Alphabetical Order)

Several major U.S. corporations have taken center stage in quantum computing. IBM, with its century-long track record of tech innovation, leads this group. Meanwhile, Google, Microsoft, and AWS, though relatively younger, have each invested significantly in quantum R&D.

Other global players included in this section, which have gone public via SPAC, or Special Purpose Acquisition Company, also featured in our review, recognize the transformative potential of quantum computing across industries. These companies are ramping up their efforts to stay at the forefront as the sector evolves beyond the noisy intermediate-scale quantum (NISQ) era, toward fault-tolerant systems and, ultimately, quantum advantage, the tipping point where quantum machines usefully outperform their classical counterparts.

Amazon Braket, D-Wave Quantum Inc., IBM, IonQ, Google Quantum AI, Microsoft, Quantum Computing Inc., Rigetti Computing, 1QBit, Alice & Bob, Alpine Quantum Technologies (AQT), Anyon Systems, Atlantic Quantum, Atom Computing, BlueQubit, BosonQ Psi (BQP), Classiq Technologies, Crypto Quantique, Delft Circuits, Diraq, EeroQ, eleQtron, evolutionQ, Horizon Quantum Computing, HQS Quantum Simulations

11. Pioneering quantum-safe cryptography with advanced techniques for public blockchains

by Hubert Le Van Gong
https://www.jpmorganchase.com/about/technology/blog/pioneering-advanced-cryptography

Cryptography is the cornerstone of digital security, crucial for protecting information and ensuring communication integrity. In the financial sector, it safeguards sensitive data, authenticates users, and prevents unauthorized access, maintaining trust and reliability. As digital threats continue to evolve rapidly, cryptography is essential for mitigating risks like fraud and cyberattacks, enabling financial institutions to operate securely and efficiently.

At JPMorganChase, we are focused on developing and implementing advanced cryptographic solutions that address real-world challenges. Quantum-safe digital signatures can be used to protect the integrity of digital contracts and agreements, ensuring that they remain secure and trustworthy. These signatures are essential for authenticating transactions, preventing fraud, and ensuring that only authorized parties can access sensitive financial information.

In this post, we summarize our recent innovation in quantum-safe digital signatures, demonstrating a novel technique to secure financial transactions, strategically using post-quantum cryptography in public distributed ledgers.

Recent Innovation: Quantum-Safe Threshold Signatures

- **Threshold Signatures**: Threshold signatures are a crucial technique used in many applications, especially in decentralized finance. It enhances security by requiring multiple parties to collaborate in generating a valid digital signature. Multi-Party Computation (MPC) protocols play a vital role in creating threshold signature schemes by enabling participants to jointly compute a signature without revealing their individual key shares. Instead of relying on a single private key, threshold signatures distribute the signing authority across several participants, each holding a piece of the key. A predefined number of these participants, known as the threshold, must cooperate to produce a valid signature. The resulting signature can be verified using a public key and a standardized verification algorithm, ensuring its authenticity and integrity. This approach not only increases resilience against key compromise but also ensures that no single party can unilaterally sign transactions, making it particularly valuable in safeguarding digital assets.

- **Quantum-Safe Digital Signatures**: Our team recently defined a threshold variant of the newly published NIST standard for quantum-safe signatures, ML-DSA, addressing a significant gap in the cryptographic landscape. Until now, there hasn't been a known quantum-safe multi-party computation ML-DSA scheme, nor a scalable threshold version, posing challenges for its adoption in quantum-safe blockchains. This innovation allows the signing process to benefit from the enhanced security of threshold signatures, ensuring that multiple parties can collaboratively sign without compromising individual key privacy. Remarkably, during verification, the signature still passes as a standard ML-DSA signature, maintaining compatibility with existing systems. This breakthrough not only enhances security but also positions us at the forefront of post-quantum cryptographic solutions, addressing the growing concern over quantum computing's potential to break traditional cryptographic schemes.

- **Publication Details**: the details of this groundbreaking work are documented in a paper titled "Efficient, Scalable Threshold ML-DSA Signatures: An MPC Approach." The paper provides a comprehensive overview of the protocol's design, implementation and potential applications. This publication marks a significant milestone in our ongoing efforts to advance cryptographic research and develop solutions that address the challenges posed by emerging technologies.

12. White House Prepares Executive Actions on Quantum Tech and Post-Quantum Cybersecurity

by Matt Swayne
https://thequantuminsider.com/2025/09/20/reports-white-house-prepares-executive-actions-on-quantum-tech-and-post-quantum-cybersecurity/

The White House is preparing executive actions that would push federal agencies to accelerate adoption of quantum technology and new cybersecurity standards, according to recent media reports.

At least two orders have been in development since summer, NextGov reported, with the focus split between advancing quantum information science and guiding the government's migration to post-quantum cryptography. Post-quantum cryptography refers to new encryption algorithms designed to withstand attacks from future fault-tolerant quantum computers, which could one day break today's digital protections.

The National Institute of Standards and Technology released the first versions of these algorithms in 2023, and the White House plans to use its authority to set migration timelines across agencies. The institute recently released a draft of a white paper to help organizations with that migration.

The scope of the planned actions is still fluid. According to *NextGov*, sources familiar with the drafts suggest there may be as many as three separate orders or as few as one, depending on how broadly the administration decides to cover the topic. Either way, the centerpiece will be federal adoption of post-quantum cryptography, with directives likely to include deadlines for agencies and contractors to begin shifting networks and data systems.

Building on Previous Policy

The move continues a policy line that stretches back to the National Quantum Initiative Act, which was signed into law in 2018 under President Donald Trump. That law provided billions for research and coordination across government, universities, and private industry. The program expired in 2023 and is now awaiting reauthorization in Congress. In the meantime, the White House is signaling that executive powers will be used to keep momentum going.

Earlier this year, the Office of Management and Budget circulated draft guidance that would require agencies to prepare phased migration plans. Contractors were also told to map out how their networks will transition to the new standards. The pending executive actions would give those directives more weight and urgency, *NextGov* reported.

Strategic Stakes

Administration officials have linked the importance of quantum technologies to broader competition in artificial intelligence and other emerging fields. According to *NextGov*, White House science advisers believe progress in quantum hardware and software could open new paths for secure communications, advanced sensing and high-powered computing. At the same time, they warn that without a rapid shift to stronger encryption, adversaries could harvest U.S. data today and decrypt it once powerful quantum machines arrive.

The emphasis on timelines reflects how migration to new cryptography is not a quick swap. Government networks are vast, and many systems are embedded in legacy infrastructure that cannot easily be updated. Industry experts estimate it could take a decade or more to complete the transition, which is why policy pressure is increasing now rather than waiting for commercial quantum computers to be ready.

However, details of the forthcoming executive actions remain scarce.

According to *NextGov*, the orders are expected in the near term, but the exact timing and scope are still under internal review. The number of directives issued will signal how aggressively the administration intends to coordinate quantum policy across agencies.

13. Australia Urges Immediate Action on Post-Quantum Cryptography as CRQC Threat Looms

https://cyble.com/blog/australia-crqc-post-quantum-cryptography-strategy/

The Australian Cyber Security Centre (ACSC), a division of the Australian Signals Directorate (ASD), has issued a comprehensive call to action for organizations to begin preparing their cybersecurity infrastructure for the advent of cryptographically relevant quantum computers (CRQC).

The guidance outlines the urgency of adopting post-quantum cryptography (PQC) and provides a detailed roadmap to complete the transition by the end of 2030.

CRQC: A Future Threat With Present-Day Implications

While fully operational CRQCs do not yet exist, ASD warns that their emergence would render current asymmetric cryptographic algorithms, including RSA, ECDSA, and Diffie-Hellman, ineffective. This could undermine the confidentiality and integrity of encrypted communications, authentication mechanisms, and critical infrastructure.

The threat is particularly acute due to the potential for "harvest now, decrypt later" attacks. Adversaries may already be intercepting and storing encrypted data, intending to decrypt it once CRQC capabilities become available.

"Early action is critical," the ACSC notes, highlighting three key reasons for urgency:

- Transitioning to post-quantum cryptography is complex and time-consuming.
- The development timeline for CRQC is uncertain due to ongoing research in quantum computing.
- Sensitive data encrypted today using classical methods may be compromised in the future.

Transition Timeline: Milestones Through 2030

To address the rising CRQC risk, the ASD's Information Security Manual (ISM) provides a phased approach with concrete milestones:

- **By the end of 2026**: Organizations should have a detailed transition plan that reflects their security priorities, data sensitivity, and system complexity.
- **By the end of 2028:** the Implementation of PQC algorithms should begin with the most critical and sensitive systems.
- **By the end of 2030**: Full transition to post-quantum cryptography should be completed.

- **Post-2030**: Ongoing monitoring, validation, and adaptation of PQC implementations will be necessary to maintain resilience.

The ISM also recommends using ASD-approved post-quantum cryptographic algorithms and advises against using traditional asymmetric encryption methods beyond 2030.

The LATICE Framework for PQC Transition

ASD encourages organizations to adopt the LATICE framework, which outlines five high-level phases for a successful PQC transition:

1. Locate all uses of traditional asymmetric cryptography.
2. Assess the sensitivity and value of affected systems and data.
3. Triage systems are based on criticality and transition difficulty.
4. Implement PQC algorithms using standardized libraries and vendor guidance.
5. Communicate and educate stakeholders to ensure sustained awareness and compliance.

A crucial component of the "Locate" phase involves building a Cryptographic Bill of Materials (CBOM), an inventory of cryptographic dependencies similar in function to a software bill of materials. This allows organizations to track all encryption-related implementations, including protocols, algorithms, and configurations.

Quantum Key Distribution And Hybrid Schemes

Although quantum key distribution (QKD) is often presented as a secure method for quantum-era communication, ASD currently does not endorse QKD due to its reliance on specialised hardware and its practical limitations, particularly around authentication.

In cases where legacy systems require compatibility, ASD allows, but does not recommend, post-quantum/traditional (PQ/T) hybrid schemes. These offer interim interoperability but are ultimately considered vulnerable, as the traditional components will become obsolete once CRQC is achieved.

International Context And Supporting Standards

The ACSC acknowledges that various international bodies are also preparing for the quantum shift. These include:

- **NIST** (U.S.) – Leading the standardization of PQC algorithms.
- **CISA** (U.S.) – Offering critical infrastructure-specific guidance.
- **UK NCSC**, **Canadian CCCS**, and **New Zealand NCSC** – Providing national roadmaps and technical advisories.
- **IETF** – Updating cryptographic standards such as TLS for PQC readiness.
- **ETSI** – Developing frameworks for quantum-safe migration.
- **Post-Quantum Cryptography Coalition** – Supporting industry collaboration and tooling.

While these organizations may provide different timelines or approaches, they share a common emphasis on the urgency of preparing for CRQC.

14. When Passwords Fail: How Quantum Computing Could Shake Digital Security

by The420 Web Desk
https://the420.in/quantum-computing-digital-security-encryption-threat-2025/

In today's digital world, passwords and encryption form the backbone of security. They safeguard banking transactions, government files, and personal information from cybercriminals. Yet, that backbone is on the verge of collapse. The culprit: quantum computing, a technology capable of performing calculations so rapidly that existing security frameworks could crumble in an instant.

The Countdown Begins

Experts warn that in the coming decade, quantum computers will achieve feats that today's supercomputers could not accomplish in centuries. Encryption standards such as RSA and AES, long considered unbreakable, may be rendered obsolete within minutes by quantum machines.

"Encryption is the oxygen of the Internet. Without it, the entire digital ecosystem will suffocate," said Dr. Richard Hudson, a cybersecurity professor at the U.S. Naval Academy.

A Global Investment Race

From Google, IBM, and Microsoft to Chinese government labs, every major technology power is racing to dominate the quantum frontier. Billions of dollars are being poured into developing quantum machines. The U.S. Department of Defense and several European agencies have already incorporated quantum strategy into national security planning.

"This is not just an innovation race—it's a control race. The country that leads in quantum technology will define the rules of digital power for the future," warned John Carlson, former NSA officer.

Banking and Governments in the Crosshairs

Hackers are already hoarding sensitive data. Experts describe the "Harvest Now, Decrypt Later" approach: steal encrypted information today, then decrypt it once quantum computers are viable. The implications are staggering—impacting banking networks, national security infrastructure, and personal digital assets worldwide.

Nikhil Verma, an Indian cybersecurity analyst, emphasized, "If post-quantum cryptography isn't implemented within the next five to seven years, the damage could be irreversible."

A Silver Lining

Quantum computing isn't only a threat—it also promises unprecedented opportunities. Its computational power could revolutionize drug discovery for diseases such as cancer and Alzheimer's, improve climate modeling, and accelerate the development of new materials.

"It's not just a weapon for cracking passwords. It can also open new avenues for science and humanity," said Dr. Mei-Ling Wang, a quantum researcher at the National University of Singapore.

Challenges Remain

Currently, quantum machines are expensive and require near-zero temperatures, sophisticated engineering, and immense energy to operate. Yet history has shown that technologies once deemed impossible quickly integrate into everyday life. Google has already demonstrated "quantum supremacy," while China continues to invest heavily in the field. Experts predict that by 2030, the true impact of quantum computing will become evident.

The Clock Is Ticking

The world has very limited time to prepare. Governments and corporations must adopt post-quantum security frameworks immediately. Investment in education and research is crucial to train quantum scientists and engineers capable of building the next generation of secure systems.

Quantum computing will determine whether the coming decade becomes one of human progress and scientific discovery—or digital insecurity and cyber chaos.

15. NIST Finalizes Guidelines for Implementing 'Handshake' Algorithms Known as Key-Encapsulation Mechanisms

by Chad Boutin
https://content.govdelivery.com/accounts/USNIST/bulletins/3f2be48

To help organizations protect their data against possible future attacks from quantum computers, the NIST has released a publication offering guidelines for implementing a class of post-quantum cryptography (PQC) algorithms known as key-encapsulation mechanisms, or KEMs.

A KEM is a set of algorithms that can be used by two parties to securely establish a shared secret key over a public channel – a sort of first handshake between parties that want to exchange confidential information. Recent examples of KEMs include ML-KEM and HQC.

The new publication, *Recommendations for Key-Encapsulation Mechanisms* (NIST Special Publication 800-227), describes the basic definitions, properties and applications of KEMs and provides recommendations for implementing and using KEMs securely.

The publication also offers guidelines for implementing "hybrid" setups that use both conventional and PQC algorithms together, requiring an attacker to break both. For those organizations that opt to use such hybrid setups during their transition to using PQC, the publication offers a way to implement them safely and securely.

The finalized publication reflects comments received on the initial public draft before the deadline on March 7, 2025, as well as input from NIST's virtual Workshop on Guidance for KEMs held Feb. 25-26, 2025. Comments on the draft are available at the final version's publication details.

16. You don't need quantum hardware for post-quantum security

by Luke Valenta
https://blog.cloudflare.com/you-dont-need-quantum-hardware/

Organizations have finite resources available to combat threats, both by the adversaries of today and those in the not-so-distant future that are armed with quantum computers. In this post, we provide guidance on what to prioritize to best prepare for the future, when quantum computers become powerful enough to break the conventional cryptography that underpins the security of modern computing systems. We describe how post-quantum cryptography (PQC) can be deployed on your existing hardware to protect from threats posed by quantum computing, and explain why quantum key distribution (QKD) and quantum random number generation (QRNG) are neither necessary nor sufficient for security in the quantum age.

Are you quantum ready?

"Quantum" is becoming one of the most heavily used buzzwords in the tech industry. What does it actually mean, and why should you care?

At its core, "quantum" refers to technologies that harness principles of quantum mechanics to perform tasks that are not feasible with classical computers. Quantum computers have exciting potential to unlock advancements in materials science and medicine, but also pose a threat to computer security systems. The term *Q-day* refers to the day that adversaries possess quantum computers that are large and stable enough to break the conventional public-key cryptography that secures much of today's data and communications. Recent advances in quantum computing have made it clear that it is no longer a question of *if* Q-day will arrive, but *when*.

What does it mean, then, for your organization to be quantum ready? At Cloudflare, our definition is simple: *your systems and communications should be secure even after Q-day*.

However, this definition often gets muddied by vendors insisting that products *built using quantum technology* are required in order to *secure* an organization *against quantum adversaries*. In this blog post we explain why quantum technologies are neither necessary nor sufficient to protect against attacks by a quantum adversary.

The good news is that there is already a solution: post-quantum cryptography (PQC). PQC protects against attacks by quantum adversaries, but PQC is not a quantum technology — it runs on conventional computers

without specialized hardware. You can use PQC today on the computers you already have, without buying expensive new hardware.

Post-quantum cryptography

We've written quite a few blog posts on post-quantum cryptography already, so we will keep this section brief.

The public-key cryptography that we've used for decades to secure our data and communications is based on math problems (like factoring large numbers) that are believed to be computationally hard to solve on conventional computers. If you can efficiently solve the underlying math problem, you can efficiently break the cryptography and the systems that depend on it. As it turns out, the math problems underlying much of today's public-key cryptography can be efficiently solved by specialized algorithms, like Shor's algorithm, on large-scale quantum computers.

The solution? Pick new hard math problems (like finding "short" vectors in algebraic lattices) that are no easier to solve with a quantum computer than with a conventional computer. Then, build new cryptographic systems around them. The US National Institute of Standards and Technologies (NIST) launched an international competition in 2016 to identify and standardize such cryptographic systems, which resulted in several new standards for post-quantum cryptography being published in 2024, and several more under consideration for future standardization.

Post-quantum cryptography (PQC) runs on your existing phones, laptops, and servers. PQC runs at Internet scale and can even be more performant than classical cryptography. Except in rare cases, like when you need additional hardware acceleration in cheap smartcards or to replace legacy systems that lack cryptographic agility, there is no need to purchase new hardware to migrate to PQC.

If you want to know how to protect your organization from security threats posed by quantum computers, you can stop reading now. Post-quantum cryptography is the solution.

Alternatively, you can read below for our perspective on hardware-based quantum security technologies that are sometimes marketed as security solutions.

Quantum security technologies

Quantum technologies capture the imagination. Quantum computers (possibly linked together in a quantum Internet) promise to deliver breakthroughs in drug discovery and materials science via advanced molecular simulation. Measurement of physical quantum processes can be used to generate entropy with mathematically provable properties.

This is exciting technology and fundamental scientific research. But this technology is not required to secure data and communications against quantum attackers.

In this section, we'll explain why quantum security technologies do not need to be part of your quantum readiness strategy, and any decision to invest in quantum technology should not be based on a desire to defend data and communications systems against the threat of quantum adversaries. Instead, investments should be based on a desire to improve quantum technologies in their own right, for example to help with applications like chemistry, machine learning, and financial modeling.

Our position here is largely in agreement with the strategies towards quantum security technologies of the US National Security Agency (NSA), UK National Cyber Security Centre (NCSC), NL National Cyber Security Centrum (NCSC), and DE Federal Office for Information Security (BSI). We'll focus on two quantum technologies widely marketed as security products: quantum key distribution (QKD) and quantum random number generation (QRNG).

Quantum key distribution

Quantum key distribution (QKD) is a hardware-based solution to secure communications across point-to-point links. Rather than relying on hard mathematical problems, QKD relies on principles of quantum physics to establish a shared symmetric secret between two parties, while ensuring that eavesdropping can be detected. QKD provides security guarantees that are based on physical properties of the communication channel. Once a shared secret is established, parties can switch to traditional symmetric-key cryptography for secure communication. QKD is the first step towards a futuristic "quantum Internet." However, there are some fundamental reasons why QKD cannot be a general replacement for classical cryptography running on conventional hardware.

Most importantly, *QKD does not operate at Internet scale*. QKD is used to establish an unauthenticated secret between pairs of parties with a direct physical link between them. The parties can then use an authentication mechanism based on conventional cryptography to bootstrap a secure communication channel over that link. While building dedicated physical links may be feasible for cross-datacenter communication or across major Internet backbones, it is not possible for most pairs of parties on the Internet. In particular, deploying QKD for the "last-mile" connection to end-user devices would require that each device has a direct physical connection to every server or device it needs to securely communicate with.

Connectivity aside, there's a good reason why the Internet doesn't rely on secure point-to-point links: they do not scale (or rather, they scale exponentially). Bringing a new device online would require a change to *every other device* it needs to communicate with, a massive operational burden on everyone. Fortunately, there's a better way. The OSI model for networking provides an abstraction such that two parties can communicate even if they don't share a direct physical link, so long as some chain of physical links exists between them. Public-key cryptography, invented in the seminal "New Directions in Cryptography" paper in 1976, allows two parties participating in the same public-key infrastructure to establish a secure end-to-end encrypted communication channel, without requiring any prior setup between them. The massive scaling enabled by these technologies is why the secure Internet exists as we know it. Secure point-to-point links are not part of the solution.

Lack of scalability is enough for us to disqualify QKD outright: if a technology can't bring security to the whole Internet, we're not going to spend much time on it.

The challenges with QKD don't stop there though.

QKD touts theoretical security guarantees, but achieving security in practice is not so simple. QKD systems have been plagued by implementation attacks, both classical sidechannel attacks and new ones specific to the technology. Further, QKD works best over a special medium: either fiber or a vacuum. QKD has been demonstrated over the air, but performance and the implementation security mentioned before suffers. We still have not seen QKD work on a mobile phone or over Wi-Fi networks.

Further, neither QKD nor any other quantum technologies provide authentication to prove that the party on the other end of the key exchange is who you think they are. This opens the door for a classic monster in the middle (MITM) attack, where an adversary intercepts your connection, establishes a separate secure QKD link to you and your intended destination, and then sits in the middle reading and relaying all traffic. To prevent this, you must authenticate the identity of the party you are connecting to, using either pre-shared keys or conventional public-key cryptography. The bottom line is, whether or not you invest in QKD, you still need a solution for authentication to protect against active attackers armed with quantum computers. Practically speaking, that means you need PQC, but PQC is already a standalone solution that provides both authentication and key agreement, which leads to questions of why use QKD in the first place.

Some proponents argue that QKD should be integrated into existing systems as an extra security layer. The value proposition of QKD relates to the "harvest now, decrypt later" threat. In public-key cryptography, the key exchange messages used to set up encryption keys to secure a communication channel are exchanged in full view of a potential adversary. If an adversary records the key exchange messages, they might hope to use improved techniques in the future to solve the hard math problems upon which the security of the key exchange relies, allowing them to recover the encryption keys and decrypt the communication. If encryption keys are exchanged directly via QKD instead, the eavesdropper protections provided by QKD stop an adversary from recording messages that could later allow them to recover the encryption key (e.g. by using a quantum computer or other advances in cryptanalysis). The problem is, however, that this "extra security layer" is brittle, and limited to a single physical link. As soon as the data is transmitted elsewhere – for instance at an Internet exchange point or to travel to an end-user – the QKD security ends. For the rest of its journey, the data is protected by standard protocols like TLS, making the value of the initial QKD link questionable.

While we hope the technology progresses, QKD is neither necessary nor sufficient for security against a quantum adversary. PQC is sufficient for security against a quantum adversary, already runs on your existing hardware, and works everywhere.

Quantum random number generators

Quantum random number generators (QRNGs) are a type of "true" random number generator (TRNG) that work by harnessing inherent unpredictability of quantum mechanics, for example by measuring atomic decay or shooting photons at a beam splitter. Other types of classical (non-quantum) TRNGs use physical phenomena that exhibit random properties, such as thermal noise from electrical components, the motion of hot wax in lava lamps, double pendulums, hanging mobiles, or water wave machines.

In cryptography and computer security, the essential property required from a random number generator is that the outputs are unpredictable and unbiased. This can be achieved by taking a small seed (say, 256 bits) of true randomness and feeding it to a cryptographically-secure pseudorandom number generator (CSPRNG) to produce an essentially limitless stream of pseudorandom output indistinguishable from true randomness. The randomness used to seed the CSPRNG can be based on either classical or quantum physical processes, as long as it is not known to the adversary. Whether or not you use a QRNG to generate the seed, a CSPRNG is essential for cryptographic applications.

We are the first to get excited about fun new sources of randomness. However, we'd like to emphasize that randomness derived from quantum effects is not necessary to combat threats from quantum computers. Quantum computers do not enable any practical new attacks against classical TRNGs in widespread use today.

Your decision to invest in QRNGs should be based on a perceived improvement in the quality of randomness they produce and not on a perceived threat to classical TRNGs from quantum computing.

Post-quantum cryptography at Cloudflare

Cloudflare has been at the forefront of developing and deploying PQC, and we are committed to making PQC available for free and by default for all of our products. And we run it at scale – already over 40% of the human-generated traffic to our network uses PQC.

So what's in that 40%? PQC is supported for all website and API traffic served through Cloudflare, most of Cloudflare's internal network traffic, and traffic running over our Zero-Trust platform. All these connections use post-quantum key agreement to protect against the "harvest now, decrypt later" threat, where an adversary intercepts and stores encrypted data today with the hope of decrypting with a quantum computer or other cryptanalytic advances in the future. Key agreement is an important first step, but there's still more work to be done. We're actively working with stakeholders in the industry to prepare for the upcoming migration to post-quantum signatures to prevent active impersonation attacks from quantum adversaries (after Q-day).

Quantum readiness strategy

If purchasing quantum hardware is not necessary, how *should* organizations prepare for a quantum future? The most effective strategy will depend on your organization's individual needs, but some general strategies will pay off for most organizations:

Investing in basic security practices is a good start. Hire the right expertise if you don't already have it. Find vendors that support post-quantum encryption in their offerings today, and whose products are cryptographically agile so you can enjoy a seamless transition to post-quantum signatures and certificates when the industry migrates before Q-day. Follow a tunneling strategy: routing application traffic over the Internet via secure quantum safe tunnels allows you to reduce your attack surface area with minimal changes to existing systems. If you're already a Cloudflare customer (or want to be), our Content Distribution Network and Zero Trust platform makes this easy.

17. NIST explains how post-quantum cryptography push overlaps with existing security guidance

by Eric Geller
https://www.cybersecuritydive.com/news/nist-post-quantum-cryptography-guidance-mapping/760638/

The National Institute of Standards and Technology on Thursday published guidance describing how implementation of post-quantum cryptography (PQC) both supports and relies on the safeguards in the agency's major cybersecurity publications.

The draft NIST document, derived from the output of the agency's PQC migration project, is designed to illustrate the connections between the tools required for adopting quantum-resistant encryption and the security practices that NIST recommends in its Cybersecurity Framework and other guidance.

"The capabilities demonstrated in the project support several security objectives and controls identified" in other NIST guidance documents, the agency said in its new publication. "At the same time, responsible implementation of the demonstrated capabilities is dependent on adherence to several security objectives and controls identified in these risk framework documents."

Collecting information about which technologies use cryptography supports the Cybersecurity Framework practices of creating hardware and software inventories, the document notes. Similarly, analyzing cryptographic weaknesses supports the CSF practice of identifying vulnerabilities in technology assets.

On the flip side, the CSF practice of establishing clear processes for managing technology configurations is a prerequisite to the PQC migration step of implementing new quantum-resistant algorithms, the document says. And the CSF practice of identifying threats to an organization "can inform requirements for" quantum-ready hardware security modules.

In addition to mapping PQC activities onto the CSF, the document also maps them onto NIST's security and privacy controls catalog, known as Special Publication 800-53. Analyzing cryptographic weaknesses supports the principles in 800-53's risk assessment category, according to the document, while implementing PQC algorithms will often require adherence to that publication's section on public key infrastructure certificates.

In the document, NIST also encourages organizations focused on PQC migration to collaborate on a CSF profile, a document explaining how their community is using the CSF to accomplish their goals. Similar CSF profiles exist for ransomware mitigation, GPS data integrity and semiconductor manufacturing. NIST said a CSF profile for PQC activities would "ease the community's migration to PQC."

18. Self-Replicating Worm Hits 180+ Software Packages

by Brian Krebs
https://krebsonsecurity.com/2025/09/self-replicating-worm-hits-180-software-packages/

At least 187 code packages made available through the JavaScript repository **NPM** have been infected with a self-replicating worm that steals credentials from developers and publishes those secrets on **GitHub**, experts warn. The malware, which briefly infected multiple code packages from the security vendor **CrowdStrike**, steals and publishes even more credentials every time an infected package is installed.

The novel malware strain is being dubbed **Shai-Hulud** – after the name for the giant sandworms in Frank Herbert's *Dune* novel series – because it publishes any stolen credentials in a new public GitHub repository that includes the name "Shai-Hulud."

"When a developer installs a compromised package, the malware will look for a npm token in the environment," said **Charlie Eriksen**, a researcher for the Belgian security firm Aikido. "If it finds it, it will modify the 20 most popular packages that the npm token has access to, copying itself into the package, and publishing a new version."

At the center of this developing maelstrom are code libraries available on NPM (short for "Node Package Manager"), which acts as a central hub for JavaScript development and provides the latest updates to widely-used JavaScript components.

The Shai-Hulud worm emerged just days after unknown attackers launched a broad phishing campaign that spoofed NPM and asked developers to "update" their multi-factor authentication login options. That attack led to malware being inserted into at least two-dozen NPM code packages, but the outbreak was quickly contained and was narrowly focused on siphoning cryptocurrency payments.

In late August, another compromise of an NPM developer resulted in malware being added to "**nx**," an open-source code development toolkit with as many as six million weekly downloads. In the nx compromise, the attackers introduced code that scoured the user's device for authentication tokens from programmer destinations like GitHub and NPM, as well as SSH and API keys. But instead of sending those stolen credentials to a central server controlled by the attackers, the malicious nx code created a new public repository in the victim's GitHub account, and published the stolen data there for all the world to see and download.

Last month's attack on nx did not self-propagate like a worm, but this Shai-Hulud malware does and bundles reconnaissance tools to assist in its spread. Namely, it uses the open-source tool TruffleHog to search for exposed credentials and access tokens on the developer's machine. It then attempts to create new GitHub actions and publish any stolen secrets.

"Once the first person got compromised, there was no stopping it," Aikido's Eriksen told KrebsOnSecurity. He said the first NPM package compromised by this worm appears to have been altered on Sept. 14, around 17:58 UTC.

The security-focused code development platform **socket.dev** reports the Shai-Halud attack briefly compromised at least 25 NPM code packages managed by CrowdStrike. Socket.dev said the affected packages were quickly removed by the NPM registry.

In a written statement shared with KrebsOnSecurity, CrowdStrike said that after detecting several malicious packages in the public NPM registry, the company swiftly removed them and rotated its keys in public registries.

"These packages are not used in the Falcon sensor, the platform is not impacted and customers remain protected," the statement reads, referring to the company's widely-used endpoint threat detection service. "We are working with NPM and conducting a thorough investigation."

A writeup on the attack from **StepSecurity** found that for cloud-specific operations, the malware enumerates AWS, Azure and Google Cloud Platform secrets. It also found the entire attack design assumes the victim is working in a Linux or macOS environment, and that it deliberately skips Windows systems.

StepSecurity said Shai-Hulud spreads by using stolen NPM authentication tokens, adding its code to the top 20 packages in the victim's account.

"This creates a cascading effect where an infected package leads to compromised maintainer credentials, which in turn infects all other packages maintained by that user," StepSecurity's **Ashish Kurmi** wrote.

Eriksen said Shai-Hulud is still propagating, although its spread seems to have waned in recent hours.

"I still see package versions popping up once in a while, but no new packages have been compromised in the last ~6 hours," Eriksen said. "But that could change now as the east coast starts working. I would think of this attack as a 'living' thing almost, like a virus. Because it can lay dormant for a while, and if just one person is suddenly infected by accident, they could restart the spread. Especially if there's a super-spreader attack."

For now, it appears that the web address the attackers were using to exfiltrate collected data was disabled due to rate limits, Eriksen said.

Nicholas Weaver is a researcher with the **International Computer Science Institute**, a nonprofit in Berkeley, Calif. Weaver called the Shai-Hulud worm "a supply chain attack that conducts a supply chain attack." Weaver said NPM (and all other similar package repositories) need to immediately switch to a publication model that requires explicit human consent for every publication request using a phish-proof 2FA method.

"Anything less means attacks like this are going to continue and become far more common, but switching to a 2FA method would effectively throttle these attacks before they can spread," Weaver said. "Allowing purely automated processes to update the published packages is now a proven recipe for disaster."

19. `Cryptography remains the weapon of the weak against the strong'

by ForkLog
https://forklog.com/en/cryptography-remains-the-weapon-of-the-weak-against-the-strong/

As dystopian plots inch into reality, some still strive to protect their personal data and defend privacy online. ForkLog spoke with cypherpunk Anton Nesterov about the main threats to confidentiality and how to counter them. The interview was first published in our monthly digest, FLMonthly.

"The state has never been the only enemy"

ForkLog: What is today the core of cypherpunk ideology: privacy for an open society, or distrust of authority?

Anton Nesterov: The core of cypherpunk is the idea of broad deployment of cryptography, aimed at anyone who decides to encroach on confidentiality. Cypherpunks trust neither the state nor corporations nor words – they trust only the mathematics embedded in cryptographic protocols.

ForkLog: In his early writings, Julian Assange said that cryptography is the weapon of the weak against the strong. How effective is that weapon today, when the "strong" (states, corporations) possess unprecedented surveillance and hacking capabilities?

Anton: The threat that advances in computing would lead to unprecedented surveillance was understood from the outset. In 1968, packet-network pioneer Paul Baran wrote about the moral responsibility of engineers to protect privacy, calling those who agree to work on its destruction "the whores among us," while describing this as inevitable and saying such people would always be found.

In 1983, New York Times journalist David Burnham published The Rise of the Computer State, an Orwellian account of the then-nascent practices of mass computerised data collection. We now live in a world where everything in that book is part of daily life.

Cypherpunks emerged against that backdrop and saw protection in cryptography. Surveillance capabilities have grown, but so too has the unprecedented range of cryptographic ways to protect oneself. Cryptography remains the weapon of the weak against the even stronger.

ForkLog: The state used to be seen as privacy's chief foe. Today we voluntarily hand our data to corporations. Has the main opponent changed?

Anton: The state has never been the sole enemy; opponents are all who wish to violate confidentiality. Corporations can be compelled by the state to hand over information, so the boundary between them is porous. The opponent can also be an individual — and cryptography protects against that, too.

ForkLog: Some claim the battle for privacy is already lost. Mass surveillance, big data — we live in a world of total monitoring. Is there still any point in fighting?

Anton: Totalitarian states exist, but that does not mean the struggle for democracy is lost. This struggle will last forever.

ForkLog: People "accept surveillance" for the convenience of services. How can this be reversed? How do you convince an ordinary person that their privacy matters more than comfort?

Anton: The usual answer is a tirade about a free society and the importance of confidentiality in protecting against authoritarianism and safeguarding free speech. These are correct and important arguments, but many do not care; some even roll their eyes. They avoid politics, try to live simply, keep their heads down, do not work in fields that require heightened confidentiality, and think these issues do not concern them. They do.

They need closer-to-home examples. Right now, hundreds of terabytes of Russian citizens' data from convenient services lie openly accessible, leaked by Ukrainian hacktivists. This shows what services actually store and how valuable that information is. It is now clear that with a bit of social engineering you can make a person do almost anything — and it works on ordinary people who "have nothing to hide." Data enables blackmail, identity theft, stalking and many other unpleasant things.

People will have to understand that anyone will use their data against them in any way possible, including ways they do not suspect — and they will not like it. Confidentiality is necessary to guard against this. Cryptography is necessary to ensure confidentiality.

ForkLog: How does the cypherpunk movement respond to challenges that did not exist in the 1990s: facial recognition, predictive analytics, AI censorship, centralised digital currencies (CBDC)?

Anton: You cannot roll back facial recognition; the technology is here — cheap and accessible. In the hands of the state it becomes especially dangerous. The danger lies not only in surveillance itself, but in the fact that facial recognition cannot be perfect. Combined with police power and the heightened trust law enforcement can place in ``AI" evidence, this has already led to ugly cases.

Consider the case of Aleksandr Tsvetkov, whom a facial-recognition system at Domodedovo airport mistook for a composite sketch of a serial killer. He was held in pre-trial detention for 10 months and interrogated until he signed a confession.

Such things regularly happen in the United States, too. This is not uniquely Russian, but a consequence of mixing a "magic box" with policing. We cannot stop facial recognition, but we can stop its use by the state through legislative bans, as in some US cities.

Predictive analytics and scoring more broadly have many problems. These are utterly opaque systems. No one can say what exactly the black box does or why it produces a given result. Statistical models can find correlations that exist but lack significance. Rare events are a separate problem.

Data collection itself can contain errors. Yet decisions are then made automatically on that basis — decisions no one can explain — and those decisions affect people's lives. That is how credit scoring works; it is used to set insurance prices; it determines which ads you see online; it informs governmental and other decisions.

Cypherpunks advocate protecting data with strong cryptography, which solves these problems at the root.

AI censorship differs little from any other big-tech censorship. States force companies to impose restrictions; no one wants to fall under the regulator's knife. Fortunately, many open large models have appeared, so this problem is partly addressed and AI's future is not so murky.

CBDCs were discussed by cypherpunks back in 1994, albeit under a different name. Their approach to the technology is no different from their approach to traditional banking; the solution is cryptocurrencies.

ForkLog: If you had to assemble a "modern survival kit" for a cypherpunk, which tools would it include?

Anton: The main tool is your head and an understanding of the subject. Practical confidentiality begins with threat modelling, so it is hard to single out anything universal.

Still, I would name a few underrated basics: free software with the latest updates from a reliable source; full-disk encryption; authentication via a WebAuthn hardware token (and a hardware wallet for cryptocurrencies); never reusing passwords; and striving always to leave as little data as possible.

A truly private blockchain

ForkLog: Bitcoin, with its pseudo-anonymous and public blockchain, is often criticised for lacking privacy. Are anonymity-focused coins (Monero, Zcash) worthy substitutes? Or does the very concept of decentralised money already fit the movement's spirit?

Anton: In their current form, Monero and Zcash are hard to call final solutions; they have many usability constraints. They were created when cryptography was just emerging and many problems were unresolved.

For true mass adoption of cryptocurrencies, a private blockchain is simply essential. Companies' transactions are commercial secrets; even the modern banking system can preserve that in most cases. One can imagine how this would hit ordinary people, too: a payment at a hotel across the country would signal that no one is at home. Combined with balances, you can imagine automated lists of the most attractive targets for burglars.

These are not the properties we want in new money. The state can request data from a bank, but it is not available to just anyone in real time. Banking has no such public-by-default case and there is legal liability for breaching bank secrecy — yet for some reason this is still considered normal in cryptocurrencies.

Unfortunately, efforts to solve this face immense pressure, especially after the crackdown on Tornado Cash with sanctions and criminal cases. It became clear that a public business model for such projects is off-limits due to risk. zkSNACKs stopped hosting a CoinJoin coordinator, Trezor ended its support, and the developers of Samourai Wallet were arrested.

The entire industry is feeling a huge chilling effect from how others have been treated, yet some research continues nonetheless.

We can have private transactions on Bitcoin. CoinJoin is not perfect, but it exists. Confidential Transactions and Bulletproofs were attempts. ZeroSync is now actively researching the potential of zero-knowledge proofs on Bitcoin.

I think we will follow the same path as with cryptography in general. It was once banned; people claimed it would let terrorists, paedophiles, Soviet spies and other bogeymen communicate undetected — but now we live in a world where TLS is on practically every site, because its absence helped other scary people steal money.

Today the idea of a private blockchain meets resistance from states, citing the same reasons: terrorism financing, money laundering. But we cannot sacrifice banking secrecy because that makes us vulnerable to people who want to harm us.

The limits of paranoia

ForkLog: Encryption tools used to be the domain of geeks. Today Signal, Tor Browser and VPNs are far more accessible. Has this helped popularise the cypherpunk movement?

Anton: Cypherpunks popularised cryptography to the point that it is everywhere; a world without it is unimaginable. Perhaps not to the absolute we would like, but the ideas have permeated. The development

of crypto-protocols and the emergence of more user-friendly software have expanded the user base. The cypherpunk goal is for everyone to use cryptography without noticing it.

Aleksei Yurchak, in "Everything Was Forever, Until It Was No More", noted an internal contradiction the Soviet state faced. On the one hand, the USSR mass-produced shortwave receivers, set up amateur radio clubs, and the magazine Radio published DIY receiver instructions. On the other, huge resources were spent jamming "enemy voices", even though the very basis for receiving them — shortwave receivers and radio skills — had been created by the state itself.

The spread of censorship-circumvention and privacy tools looks similar. The state spends trillions on ТСПУ to limit access to information, but this forces people to use circumvention tools that also render traffic inaccessible to analysis via СОРМ.

Each move by the state turns more people into cypherpunks. They start thinking about traffic analysis when YouTube loads poorly; about confidentiality when they see absurd prison terms for some decade-old VKontakte images. That is probably the main driver of cypherpunk growth in Russia today.

ForkLog: Where does cypherpunk end and paranoia begin?

Anton: There is a medical boundary. Paranoia is something unrelated to reality. If you think the FSB installs traffic-interception boxes at every network node, you are not imagining it — it does; that is a fact, and you will have to live with it. If you think the FSB is trying to control you by sending signals through your microwave, see a doctor.

ForkLog: AI can be used both for total surveillance and censorship, and to build stronger tools for cryptography and anonymity. Do you see AI as a threat, a tool, or all of the above?

Anton: The main threat with AI is social. People place too much trust in a large statistical model that merely predicts the next token in a message. Marketers bear some blame for selling it as an infallible supercomputer with all human knowledge, which strongly appeals to those far from technology.

This has many consequences across domains, from AI slop swamping search results to wrong decisions at many levels due to overestimating a neural network's quality. The effect will diminish once the technology becomes more familiar and society learns to live with it.

I do not think AI will greatly affect cryptography or that there is deep potential for synergy. Perhaps AI will help generate a logo for papers on a new cryptographic protocol. They are, after all, different technologies.

ForkLog: Is it worth an ordinary person starting to fight for privacy if they have already left a digital footprint?

Anton: It will keep them from leaving more.

ForkLog: If you had to update the cypherpunk manifesto, what new theses would you add?

Anton: The cypherpunk manifesto is a finished text; it already says what needed to be said. The task is to follow it.

20. Number Theoretic Transform Accelerates Lattice-based Encryption Via Quasilinear Polynomial Multiplication

by Quantum News
https://quantumzeitgeist.com/encryption-number-theoretic-transform-accelerates-lattice-based-quasilinear-polynomial/#google_vignette

The discrete Fourier Transform decomposes signals into their constituent frequencies, and a related mathematical tool, the Number Theoretic Transform, offers powerful advantages for modern cryptography. Banhirup Sengupta from the Tata Institute of Fundamental Research, Peenal Gupta from PinakashieldTech OÜ, and Souvik Sengupta from IONOS SE, demonstrate how this transform operates on groups and finite fields, using polynomials in place of traditional sine waves. Their work introduces fast versions of cyclic and negacyclic convolutions based on the Number Theoretic Transform, significantly reducing the complexity of polynomial multiplication, and paving the way for more efficient lattice-based encryption schemes and potentially, homomorphic encryption. This advance addresses a critical need for faster and more secure cryptographic methods in an increasingly data-driven world.

Fast NTT significantly reduces the complexity of polynomial multiplication, improving efficiency from quadratic to quasilinear time. This advancement is crucial for lattice-based cryptography, a promising approach to post-quantum cryptographic schemes offering resilience against attacks from both classical and quantum computers.

This field depends on the mathematical properties of lattices, regular arrangements of points in space, to build cryptographic tools. The speed of polynomial multiplication directly impacts the efficiency of many lattice-based schemes, making NTT a vital component. Traditional polynomial multiplication has a time complexity of $O(n^2)$, becoming inefficient for large polynomials. NTT offers a solution by transforming polynomials from a coefficient representation to a frequency representation over a finite field, leveraging the properties of finite fields to perform multiplication in the frequency domain as a much faster operation. An inverse NTT then transforms the result back to the coefficient domain, reducing the time complexity to $O(n \log n)$ through a divide-and-conquer approach.

NTT relies on carefully chosen finite fields to ensure efficient transforms and inverse transforms, utilizing primitive roots of unity within the finite field. Algorithms like Cooley-Tukey and Gentleman-Sande are optimized for different orderings, utilizing the divide-and-conquer strategy and employing 'butterflies' to combine partial results. NTT is crucial for the efficiency of lattice-based cryptographic schemes, such as Kyber, Falcon, and Dilithium, which rely heavily on polynomial arithmetic and the Module Learning With Errors (Module-LWE) problem. The NTT, analogous to the Discrete Fourier Transform but operating on polynomials over finite fields, enables efficient polynomial multiplication by reducing its complexity from quadratic to quasilinear time. Researchers introduced concepts of cyclic and negacyclic convolutions, developing both NTT and its inverse, alongside fast algorithms to accelerate these processes. Calculations with NTT require specific properties of the modulus, 'q', the number used for the remainder after division.

For NTT to function, an n-th root of unity must exist within the integer ring modulo q. Furthermore, for negacyclic convolution, essential for certain cryptographic applications, both an n-th and a 2n-th root of unity must exist within the same ring. Theorems were established defining the conditions for the existence of these roots of unity, ensuring successful NTT implementation. Utilizing the periodicity and symmetry properties of the 2n-th root of unity, scientists developed algorithms like the Cooley-Tukey and Gentleman-Sande methods, which decompose the NTT calculation into smaller, manageable steps, significantly speeding up the process. By leveraging techniques similar to the Discrete Fourier Transform but adapted for finite fields, NTT achieves a significant reduction in computational complexity, moving from quadratic time to quasilinear time complexity through a divide-and-conquer approach. The practical implications of this work are considerable, particularly within the field of lattice-based cryptography. NTTs are already widely implemented in prominent post-quantum cryptography (PQC) algorithms like Kyber and Falcon, and the research highlights further potential for optimization. For example, the authors demonstrate how direct sampling in the NTT representation can substantially reduce the number of required transforms in signature schemes, such as Dilithium. While the specific gains achieved depend on the parameters of the cryptographic scheme being used, future research could explore further optimizations tailored to specific applications and investigate the potential for NTTs in other areas beyond cryptography where efficient polynomial multiplication is crucial.

21. Quantum Computing Cracks Toy Crypto Key—What It Means for Bitcoin Security

by Beincrypto
https://www.mitrade.com/insights/news/live-news/article-3-1095654-20250904

Quantum computing has taken a symbolic step closer to testing crypto's defenses. Researchers have shown that IBM's 133-qubit machine can break a six-bit elliptic curve cryptographic (ECC) key.

The experiment has sparked debate over whether attacks on Bitcoin and Ethereum are a distant possibility or an inevitable threat.

Breaking a 6-Bit Key: Demonstration, Not Disaster

Researcher Steve Tippeconnic used IBM's ibm_torino system to crack a toy-sized six-bit ECC key, applying a Shor-style quantum attack.

The machine derived the private key from the public key equation $Q = kP$ by running a staggering 340,000-layer quantum circuit.

While impressive, the breakthrough does not threaten real crypto assets. Bitcoin and Ethereum rely on ECC-256 (256-bit elliptic curve cryptography), which is astronomically more complex.

As analysts note, breaking ECC-256 with current hardware is still beyond reach.

Yet, the test matters. It demonstrates that quantum hardware is now powerful enough to solve simplified versions of crypto's underlying math.

As quantum scientist Pierre-Luc observed, the next milestones will be error correction and modular arithmetic—both crucial steps toward scaling these toy experiments to real-world key sizes.

The Crypto Stakes: $1 Trillion Locked in ECC-256

Ethereum co-founder Vitalik Buterin recently estimated a 20% chance that quantum computers could break modern cryptography by 2030. This risk is amplified by the trillions of dollars now secured by ECC-based wallets and blockchains.

For crypto users, the immediate danger is not cracking today's keys. Rather, it is the "harvest now, decrypt later" scenario, where attackers archive encrypted data, planning to unlock it once quantum power matures.

That risk has already reshaped the sovereign Bitcoin strategy. In August, El Salvador split its 6,284 BTC treasury, worth $681 million, across 14 addresses. No wallet holds more than 500 BTC.

Officials framed the move as a hedge against quantum threats, reducing exposure by minimizing the risk of reusing addresses where public keys are permanently visible.

"Limiting funds in each address reduces exposure to quantum threats," the government explained, adding that the redesign aligns with global best practices in sovereign custody.

Not Everyone Buys the Quantum Threat

Skeptics argue that quantum fears are overblown. Graham Cooke, a Google veteran, dismissed claims that Bitcoin is at risk, calling its math "unbreakable."

"Imagine 8 billion people. Each with a billion supercomputers. Each is trying a billion combinations per second. The time needed? Over 10^40 years. The universe is only 14 billion years old," Cooke illustrated.

He added that even advances from Microsoft, Google, and IBM won't change this reality, noting that Bitcoin's math remains an unbreakable barrier.

Wall Street and Quantum-Safe Blockchain

Meanwhile, traditional finance (TradFi) is hedging early. Between 2020 and 2024, global banks made 345 blockchain investments, backing infrastructure in tokenization, custody, and payments.

As BeInCrypto reported, some are already testing quantum-secure digital assets. HSBC, for example, piloted tokenized gold using post-quantum cryptography in 2024.

This signaled that those institutions see quantum defense not as hype but as a future requirement for financial markets.

What Comes Next for Crypto Security

The six-bit crack does not threaten Bitcoin or Ethereum today. However, it suggests that quantum progress is no longer theoretical. It is practical, visible, and accelerating.

For now, ECC-256 stands firm. But as Buterin warned, the crypto industry cannot afford complacency.

"By the time quantum computers reach the level needed to break current encryption, it may already be too late," he stated.

From sovereign treasuries like El Salvador to Wall Street tokenization pilots, preparations for a post-quantum financial era are underway.

The conversation goes beyond whether crypto will adapt, now centering on how and how soon.

22. Quantum Is Closer Than You Think—So Why Are You Still Encrypting Like It's 2015?

by Bob Burns
https://securityboulevard.com/2025/09/quantum-is-closer-than-you-think-so-why-are-you-still-encrypting-like-its-2015/

Not long ago, the idea that quantum computers could one day break today's strongest encryption felt like science fiction. Today, it's no longer about if—but when. While real-world demonstrations of quantum algorithms like Shor's remain largely theoretical or experimental in nature, the pace of quantum hardware advancements and sustained government investment have shifted the narrative. Regulators around the world are now treating quantum risk as a near-term reality, not a distant possibility.

With mandates from bodies like NIST, NSA, and the EU calling for post-quantum cryptography (PQC) migration plans, quantum readiness has become a boardroom topic. The real question is: if quantum threats are now shaping regulation, roadmaps, and risk registers—why are so many organizations still encrypting like it's 2015?

According to the 2025 Thales Data Threat Report, only 48% of organizations are actively assessing their encryption strategies, and just 33% trust their cloud or telco providers to manage post-quantum security. That's alarmingly low, considering we're entering the final decade before NIST formally recommends deprecating RSA and ECC, algorithms that underpin most of the digital trust infrastructure we rely on today.

The Coming Quantum Reckoning

The promise of Quantum Computing is that it can potentially solve problems that classical computing considers impossible. For example, it could break encryption algorithms like RSA and ECC that depend upon the complexity of solving challenges such as the factoring problem or the discrete logarithm problem. Quantum algorithms like Shor's upend this entire equation, potentially reducing the solution time to hours or minutes.

This isn't just an academic concern. The increase in the volume of highly sensitive datasets accessed and processed by organizations—from medical records to national infrastructure—means a significantly expanded exposure surface for data with long-term value and long-lived consequences.

A quantum adversary doesn't need to break your encryption today to pose a threat. They can intercept and store encrypted data now—potentially by exploiting known vulnerabilities in large language models or business logic—and decrypt it years later when quantum computing capabilities mature. This strategy, known as "harvest now, decrypt later," is especially dangerous for autonomous systems that rely on historical data: the delayed exposure of that data could compromise not only privacy but also the integrity of future decisions and actions.

In fact, 58% of organizations in the Thales report cited the future decryption of today's data as a top concern, with 63% worried about future encryption compromise and 61% about key distribution in a quantum context.

The Lag in Crypto Agility

It's not only that many organizations haven't transitioned to post-quantum cryptography (PQC), but that agility was not a major consideration when building their infrastructures. Too often, encryption technologies are added onto systems years after they were architected.

Today, PQC readiness means more than swapping out an algorithm. It often requires protocol redesign, library updates, reconfiguring HSMs and TPMs, and modernizing brittle networks that can't handle longer keys or more complex TLS handshakes. And while NIST has released cryptographic algorithm standards, the PQC compatible PKI and certificate standards are only starting to materialize.

It shows. According to the report, only 45% are working to improve their cryptographic agility, and only 40% have resilience or contingency plans. Incredibly, 2% of respondents still have no formal plans to address quantum threats at all.

NIST Has Spoken, The Clock Is Ticking

If your organization is waiting for formal guidance to act, the time has come. The U.S. National Institute of Standards and Technology (NIST) has made its position clear:

- In 2022, NIST released the first set of finalist PQC algorithms.
- In 2023, NIST released the first set of draft PQC cryptographic algorithm standards.
- In 2024, it published the final algorithm standards along with a PQC transition guide.
- The guide advises deprecating RSA and ECC by 2030, with complete discontinuation by 2035.

Ten years may sound like a comfortable horizon, but cryptographic transitions are anything but quick. The migration from SHA-1 to SHA-2 took nearly a decade. PQC is more complex, more invasive, and requires broader ecosystem alignment. Waiting until 2030 to start planning would be like beginning to build your flood defenses after the first floor is already underwater.

Trusting Providers Isn't Enough

While major cloud providers and telecoms have begun integrating PQC into their services, 67% of organizations are not relying on them. This lack of trust might stem from performance concerns, unclear shared responsibility models, or limited visibility into provider-level cryptographic control. Either way, the takeaway is the same: crypto agility must be owned, not outsourced.

Providers cannot be expected to patch every protocol, upgrade every endpoint, and safeguard every byte of archived data, primarily when internal systems may not yet support PQC algorithms.

What Now? The Road to Readiness

Encouragingly, many organizations are beginning to take action:

- 57% are evaluating or prototyping PQC algorithms.
- 48% are assessing their encryption strategies.
- 27% are implementing quantum random number generation (QRNG), an essential component of PQC.
- And 22% are exploring quantum key distribution (QKD) as a longer-term secure communications method.

However, this still leaves nearly half the industry behind. In a world where AI, quantum computing, and autonomous systems converge, cryptographic inertia is a risk no enterprise can afford.

Here's how to shift gears:

- **Conduct a quantum risk assessment:** Identify what data must remain confidential long-term, including archives and intellectual property.
- **Map your cryptographic landscape:** Inventory where and how encryption is used: protocols, libraries, certificates, keys.
- **Prioritize cryptographic agility:** Design systems supporting rapid cryptographic updates, including hybrid modes (classical + PQC). Survey the suppliers of your cryptographic technology to understand their roadmap and plan accordingly.
- **Plan for interoperability:** Don't break backward compatibility prematurely—leverage hybrid-algorithm strategies where needed.
- **Start now:** Waiting until standards are mandated means playing catch-up. Begin evaluating PQC tools and NIST-approved algorithms immediately.

No Time For Complacency

The breakthroughs of 2024 and the pace of development suggest that Q-day could be closer than we think, and the encryption we rely on today won't hold forever.

This isn't a time for complacency or conservative roadmaps. This is a problem now, not a next-decade project. It's time to stop encrypting like it's 2015 because when quantum computers arrive, they won't wait for your next budget cycle.

23. Researchers Reveal How Standard Post-processing Conceals Attacks on Random Number Generators, Compromising NIST Tests

by Quantum News
https://quantumzeitgeist.com/reveal-how-standard-post-processing-conceals-attacks-random/

Random number generators underpin much of modern digital security, yet a critical vulnerability exists in how these devices are currently validated, according to new research. Yifan Chen, Dong Wang, Yibo Zhao, and colleagues from the Institute of Software, Chinese Academy of Sciences, and other institutions, demonstrate that standard post-processing techniques, designed to improve randomness, can effectively conceal physical attacks on the generator itself. The team shows that even severely compromised raw data, failing fundamental randomness tests, can be transformed into a certified random sequence after undergoing a common extraction process, creating a false sense of security. This discovery reveals a profound flaw in current validation methods, which focus solely on the final output and overlook the potential for attacks on the underlying entropy source, demanding a shift towards more comprehensive security assessments.

Statistical Detectability of Attacks After Extraction

Current designs of Quantum Random Number Generators (QRNGs) typically use randomness extraction to lessen the impact of imperfections in the quantum source. This work investigates the statistical detectability of physical attacks on QRNGs following randomness extraction, challenging the idea that extraction guarantees statistical invisibility. The motivation stems from the increasing use of QRNGs in critical applications, where the integrity of random numbers is paramount. While randomness extraction is a widely adopted security measure, a comprehensive understanding of its limitations is crucial.

This study addresses whether an attacker, with partial knowledge of the QRNG's internal state, can still detect the attack through statistical analysis of the extracted random numbers. The potential for subtle biases to accumulate and become detectable, even after extraction, poses a significant threat to the security of QRNG-based systems. The primary objective is to determine the minimum detectable bias, or the threshold beyond which an attacker can reliably identify the attack. This involves developing a statistical framework for quantifying the detectability of biases and applying it to analyze the performance of different extraction algorithms. Ultimately, this work aims to provide a more nuanced understanding of the security implications of randomness extraction in QRNGs and to inform the design of more robust and secure random number generation systems.

Extraction Conceals Quantum Source Imperfections

Designs of Quantum Random Number Generators (QRNGs) typically employ post-processing techniques to refine raw random data, followed by statistical verification. This paper demonstrates a critical flaw in this widely adopted practice: the powerful extraction process can create a false sense of security by perfectly concealing physical-layer biases. Researchers investigated the impact of these extraction techniques on the ability to detect subtle imperfections in the underlying quantum source. The methodology involves a detailed analysis of the statistical properties of both the raw and extracted random number sequences, using theoretical modelling and numerical simulations.

Specifically, the team examined how different extraction algorithms affect the ability to identify correlations and non-random behaviour in the generated numbers. The study reveals that even if a QRNG exhibits significant physical-layer biases, the extraction process can effectively mask these imperfections, leading to

the false conclusion that the generated numbers are truly random. This poses a serious security risk, as an attacker could exploit these hidden biases to predict or manipulate the generated random numbers.

Physical Manipulation Compromises Quantum Randomness

This research paper details a significant security vulnerability in Quantum Random Number Generators (QRNGs), specifically highlighting a physical-layer attack that can compromise their randomness. The core problem is that QRNGs are not inherently secure; the implementation of these generators is susceptible to manipulation. Physical components used to detect quantum events can be subtly influenced, leading to predictable outputs. The researchers successfully demonstrated an attack that manipulates the detection process within a QRNG, biasing the measurement of the quantum process and creating a correlation between the generated numbers and the attacker's control.

This vulnerability is particularly dangerous because it's difficult to detect through standard statistical randomness tests; the generated numbers appear random while being subtly controlled. The attack focuses on the photodetector used to register single photons, a common component in many QRNGs. The researchers subtly manipulate the bias voltage of the photodetector, shifting the detection threshold and altering the probability of detecting a photon, introducing a correlation between the generated bits and the applied bias. This manipulation is designed to be small enough to avoid triggering obvious anomalies, allowing the attack to remain undetected by standard randomness tests.

The implications of this attack are significant, compromising the security of applications relying on QRNGs for cryptographic keys, simulations, or other sensitive tasks. Enhanced security measures are needed, including real-time monitoring of the physical entropy source, physical security measures to protect the QRNG hardware, advanced detection techniques to identify subtle biases, and a broader recognition of the importance of considering physical-layer attacks on all security-critical systems. Key takeaways include that QRNGs are not a silver bullet for randomness, implementation details matter, statistical tests alone are insufficient to guarantee QRNG security, physical-layer security is crucial, and continuous monitoring of the physical entropy source is essential. This research serves as a wake-up call for the QRNG community, emphasizing the need for a holistic approach to security that considers both the quantum process and the physical implementation.

Post-processing Conceals QRNG Physical Attacks

This research demonstrates a critical flaw in the standard security validation of quantum random number generators (QRNGs). The study reveals that powerful post-processing techniques can inadvertently conceal physical-layer attacks on the entropy source, potentially leading to false certification of a compromised device. The team experimentally demonstrated this vulnerability by compromising an amplified spontaneous emission (ASE)-based QRNG with a power supply ripple attack. While the initial raw data failed standard security tests, the application of a common randomness extraction algorithm allowed it to pass all statistical validations. This outcome highlights that a QRNG can meet certification criteria even when its underlying quantum process is under external control, posing a significant risk to applications like cryptography.