Crypto News

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

May 01, 2025

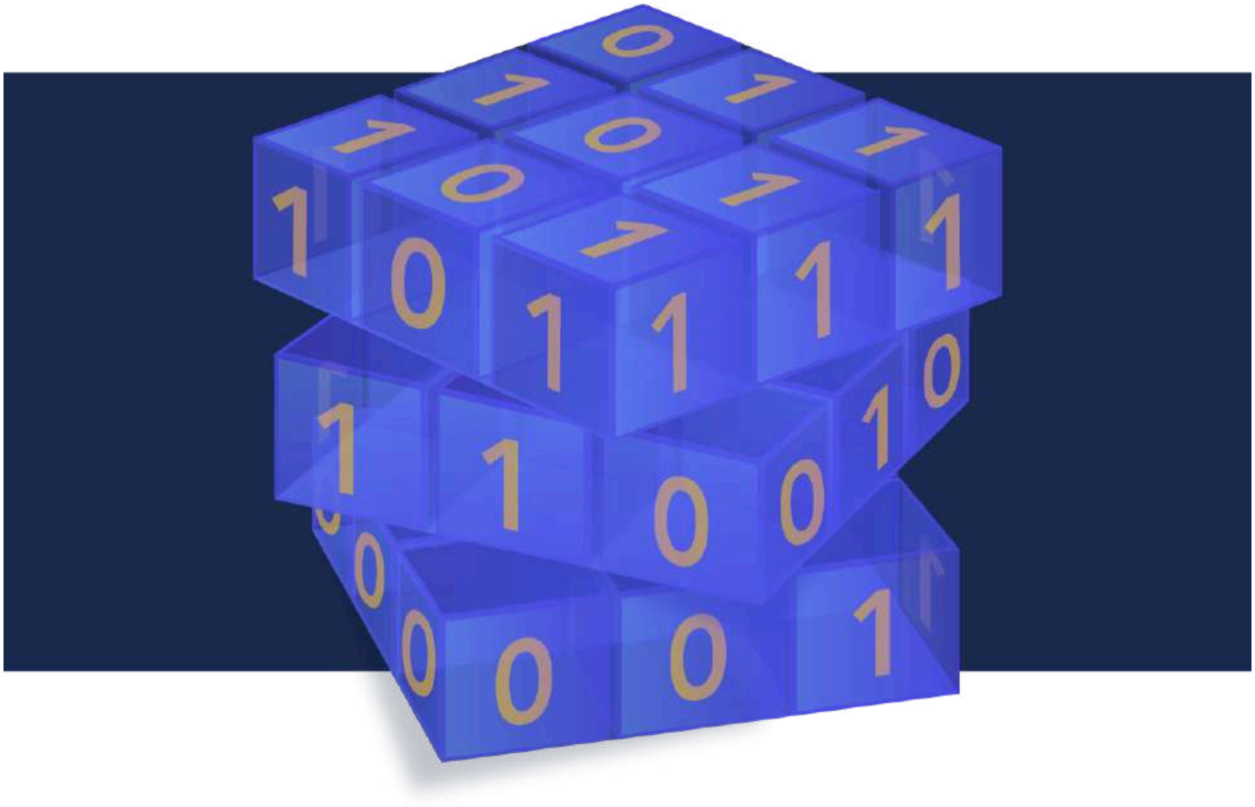


Table of Contents

Editorial

Happy Summer Readers! As the International Year of Quantum Science and Technology progresses, we have yet another great issue for you to peruse. Let's dive right in and start with an opportunity to make some cash for your upcoming vacation. Project Eleven will award 1 Bitcoin to anyone who can use a quantum computer to break elliptic curve cryptography (ECC) with Shor's algorithm. Though there are a couple of criteria you'll need to meet, the goal is to "highlight the real-world cryptographic risks of advancing quantum hardware." You will note that they're being kind and stating that the keys need only be 25 bits, far shorter than the 256-bit ECC key a quantum computer will need to factor, but it's a start. Make your way to article 18 for more information and perhaps you too can register to win. If you'd like a refresher on the threat that Project Eleven is referring to, make your way to article 20 to learn more about the quantum threat and why migrating to post-quantum cryptography is the solution your organization needs to embrace to be quantum resilient.

While DARPA in the United States has selected 18 companies, 15 publicly named with 3 remaining un-named, for their Quantum Benchmarking Initiative (QBI) in article 29 to identify approaches for building fault-tolerant quantum computers that can achieve utility-scale operations by 2033; Paris is aiming to do the same in order to make Europe the world leader in quantum technology development. The Paris Quantum Network is comprised of 11 nodes across Paris and its suburbs to address the inherent limitations of Quantum Key Distribution (QKD) - distance and scalability. It seems that Paris will not only be a tourist destination for visitors to marvel at the architecture of the Eiffel Tower and priceless art of the Louvre, but it may also become a hub for quantum technologies. Read more details in article 33.

With the International Year of Quantum in full swing, there's plenty of news to stay on top of. You'll want to make sure you don't miss the other articles in this newsletter or you may just find yourself ... behind the curve (why yes, that is an ECC pun). 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. Oracle releases FIPS-validated crypto module for Java

by Paul Krill
https://www.infoworld.com/article/3975363/oracle-releases-fips-validated-crypto-module-for-java.html

Oracle has announced Oracle Jipher, which makes cryptographic services available for Java developers using the standard Java Cryptography Architecture (JCA) framework.

Announced April 29, Jipher is a Java cryptographic service provider that packages a Federal Information Processing Standards (FIPS) 140-2 validated OpenSSL cryptographic module. Jipher is packaged as a JAR file and is downloadable from Java Tools and Resources and from My Oracle Support for Java SE users.

Oracle noted that the JDK includes cryptographic service providers such as Sun, SunRsaSign, and SunJC, which provide concrete implementations of algorithms as defined by the JCA framework. These providers let Java applications access security algorithm implementations by specifying a particular provider or by letting the framework locate the requested algorithm by searching through the registered providers in the specified preference order. However, these cryptographic service providers are not FIPS-140 validated. FIPS-140 standards, which are published by the National Institute of Standards and Technology (NIST), define security requirements for cryptographic modules.

Jipher enables deployments of Java applications in FIPS 140-regulated environments. It achieves this by leveraging the OpenSSL 3.x FIPS module, Oracle said. Jipher requires an up-to-date release of Oracle JDK 17 or JDK 21, or GraalVM for JDK 17 or JDK 21, and is made available under the Java SE OTN license. It is supported for Java SE subscribers and users running Java workloads in Oracle Cloud Infrastructure.

Jipher represents a significant advancement in Oracle’s commitment to delivering standards-compliant security solutions, Oracle said. With JDK 24, released in March, Oracle delivered two post-quantum algorithm implementations standardized by FIPS 203 and FIPS 204 to help protect Java users against emerging threats of quantum computing.

2. Quantum-Safe Cryptography: The Time to Start Is Now

by Cloudflare
https://www.govtech.com/voices/quantum-safe-cryptography-the-time-to-start-is-now

How would you react if you knew that all your constituents' information is now readable and available to the highest bidder? Since the proliferation of the Internet and digitization of government services, agencies and governments have feared this scenario. To mitigate that possibility, many cybersecurity tools have been put in place — and encryption is a critical security control that maintains the confidentiality and integrity of sensitive data. Put simply, encryption obfuscates data into an unreadable format that can only be decrypted with the proper key.

Encryption is used for both data in motion (i.e., data that's being transmitted) and data at rest (i.e., data that's being stored). Symmetric key algorithms use a shared secret key to encrypt and decrypt and are highly efficient for bulk data encryption. Data at rest is typically encrypted with symmetric key algorithms, and data in motion is encrypted with symmetric keys as well — but only after a shared secret key can be securely established between two parties.

Asymmetric algorithms use different keys — one public, one private — to validate two parties' identities and then to securely establish the shared secret (symmetric) key between them. Once the shared secret key is established, a symmetric key algorithm takes over to bulk-encrypt the communication. Public key infrastructure (PKI) describes the set of systems and standards that support today's asymmetric cryptography, including components like digital certificates that contain public keys, digital signatures that validate identities and certificate authorities that establish trust in digital certificates, among many others.

Encryption deployment and methodologies have evolved as the Internet and applications have changed, but the algorithms have been fairly stable for the last 10 years. As the advent of quantum computing draws closer, there's a significant risk that quantum computers will have the power to crack today's entire PKI ecosystem.

Quantum computing has been a commonly held goal for many years. It holds great promise for solving many chemical, material and other difficult computing concerns that modern computers cannot address. As of mid-2024, the belief was that a practical quantum computer would be available in 10 to 15 years. However, in the last three months, Microsoft, Google and Meta have introduced new quantum chips, and many now believe a practical quantum computer could be available in five to 10 years. This is a win for researchers and many industries that will benefit from these systems, but it greatly accelerates the risk to all digital communication around the world.

If we are still five to 10 years away from a quantum computer, why are we worried about this today? There are two main reasons why this is a concern today: (1) the ability of cyber criminals to harvest now and decrypt later and (2) the need to migrate cryptographic components.

Harvest Now, Decrypt Later. The most critical concern and area to address today is with data in transit. This can be constituents responding to government sites with personal information or government systems posting data to the cloud. Today, adversaries can intercept and store encrypted data transmissions, even if they are currently secure. Once quantum computing becomes viable, these archived transmissions could be decrypted, exposing sensitive information that was previously protected.

Deploying New Cryptographic Algorithms. As seen in the past, replacing encryption algorithms across large systems can take more than a decade. Transitioning to quantum-resistant cryptography will require extensive coordination, time and resources.

These challenges are especially critical for industries, such as health care and government, where data holds long-term value. Given the potential risks, there is an urgent need to accelerate the adoption of post-quantum cryptographic solutions to ensure data remains secure in the quantum era. Fortunately, industry, with guidance and leadership from the NIST, has been working on developing quantum-secure cryptography over the last decade.

In November 2024, NIST finalized several post-quantum cryptography algorithms for standardization, creating the foundation for widespread adoption. CRYSTALS-Kyber has emerged as the primary key establishment mechanism, while CRYSTALS-Dilithium, FALCON and SPHINCS+ provide options for digital signatures with different performance characteristics and security assumptions.

To support both security and compatibility, hybrid approaches combining classical and quantum-safe algorithms dominate current implementations. These approaches typically layer quantum-safe algorithms alongside traditional cryptography, ensuring protection against both conventional and quantum threats while minimizing disruption.

There is also an increased focus on crypto-agility to enable smooth transitions between algorithms as standards evolve and vulnerabilities are discovered. This emphasizes flexible cryptographic architectures that can rapidly swap algorithms without requiring extensive system redesigns.

6 STEPS TO PREPARE FOR QUANTUM-SAFE ENCRYPTION

By taking a proactive, structured approach now, government agencies can avoid being caught off guard when quantum computing reaches a point where it can threaten today's encryption. The cost of preparation is far less than the cost of a future data breach enabled by quantum decryption. Below is a simple playbook to get you started.

1. **Conduct a Cryptographic Inventory:** Identify where and how cryptographic algorithms are used across your systems (e.g., TLS/SSL, VPNs, secure emails, encrypted databases). Include third-party systems and cloud services in your review.

2. **Assess Data Sensitivity and Longevity:** Classify data based on its sensitivity and how long it needs to remain confidential. Prioritize data that must be protected for more than 10 years (e.g., health records, financial info, government contracts).

3. **Monitor Developments in Post-Quantum Cryptography (PQC):** Stay updated on standards from NIST's Post-Quantum Cryptography project. Begin evaluating these algorithms for integration into your systems.

4. **Develop a Post-Quantum Transition Plan:** Create a migration strategy for transitioning current cryptographic protocols to quantum-resistant alternatives. Include a dual cryptography or "hybrid" model during the transition period, using both classical and post-quantum algorithms to hedge risk.

5. **Train and Educate Key Staff:** Provide training for security, engineering and compliance teams on the implications of quantum computing. Ensure leadership understands both the technical and business risks involved.

6. **Test and Simulate:** Use labs or test environments to simulate PQC implementation and identify performance, compatibility or integration issues early. Evaluate hybrid models and run cost/impact analyses.

At Cloudflare, we've been researching, developing and standardizing post-quantum cryptography since 2017. We firmly believe that quantum-safe cryptography should be accessible to all and simple to deploy.

Our approach provides immediate protection while eliminating the need for complex cryptographic implementations, certificate management or compatibility testing. Simply tunnel your traffic through Cloudflare’s quantum-safe connections to immediately protect against harvest-now-decrypt-later attacks, without the burden of upgrading every cryptographic library yourself.

3. Cryptography Pioneer Adi Shamir: World 'Would Be Better' Without Cryptocurrencies

by Vince Dioquino
https://decrypt.co/317115/cryptography-pioneer-adi-shamir-world-would-be-better-without-cryptocurrencies

Cryptocurrencies have failed to deliver on their promises, cryptography pioneer Adi Shamir suggested at the RSA Conference in San Francisco, California, on Tuesday.

"My personal opinion is that the world would have been better without cryptocurrencies," he told attendees of an expert panel at the conference, per an initial report by *The Register*.

Shamir, co-inventor of the RSA encryption algorithm, was unequivocal about his position. While praising Satoshi Nakamoto's seminal whitepaper on Bitcoin as pushing a "very lofty" ideal, he believes cryptocurrencies are far from achieving decentralization.

"Everything is highly centralized in a small number of very large exchanges," the cryptographic legend said, adding that, "No one is using it in order to make payments; people are using it once in order to speculate."

Shamir went on to criticize how cryptocurrencies have "enabled all the malware," adding that it "would have been very difficult to extract so much money from companies" without it.

Ed Felten, Professor Emeritus of computer science at Princeton University, also sat on the panel.

Replying to Shamir, Felten posed a more level-headed view, saying it'd be "foolish" to "defend every cryptocurrency in the world or everybody who's in that space."

Felten, who is also co-founder and chief scientist at Offchain Labs, the company behind Ethereum layer-2 network Arbitrum, pointed out how crypto can still be of value.

"It reminds me of the early internet," Felten said. "There are a lot of people doing silly things, some people doing dangerous and criminal things, but there's a lot of people building interesting things."

To this, Shamir replied he believes blockchain technology, crypto's underlying framework, "might still have great applications."

A cryptography pioneer

In 1977, Shamir, alongside his co-inventors Ron Rivest and Leonard Adleman, developed the RSA encryption algorithm.

It was a groundbreaking public-key cryptosystem that enabled secure digital communication without requiring any two parties to share a secret key in advance.

In 2002, the trio won the Turing Award, widely regarded as the highest distinction in computer science.

Shamir's early contributions paved the way for many tools in common use today: secure web browsing, digital signatures, encrypted email, VPNs, and even software licenses.

His cryptographic innovations have also become essential to cryptocurrency security. Shamir's Secret Sharing (SSS), a technique he developed in 1979, found its way decades later to crypto wallets such as Trezor, Ledger, and Vault12.

Despite his monumental work, Shamir isn’t infallible.

In 2013, he wrote a paper about the purported links between Bitcoin creator Satoshi Nakamoto and Dread Pirate Roberts, an alias previously used by Ross Ulbricht, the founder of the Silk Road dark web marketplace. The paper's claims were later debunked.

4. Post-quantum cryptography, the next evolution of digital security

by **Amit Roy Choudhury**
https://govinsider.asia/intl-en/article/post-quantum-cryptography-the-next-evolution-of-digital-security

If you were to find yourself on the lovely streets of Amsterdam, a tourist looking for the trendiest shop to buy stroopwafel or the way to The Dam, the best person to run into might just be Anita Wehmann.

That's because she is friendly, approachable, and most importantly, totally unassuming.

But in place of being a tourist, this writer meets Wehmann in Singapore, and so, instead of directions, we speak about how post-quantum cryptography represents a critical evolution in digital security.

In the same friendly and unassuming manner, she explains, in simple terms, why this is essential in the coming age of quantum computers.

Wehmann is the programme manager for Digital Resilience, Central Dutch Government, which is part of the Netherland’s Ministry of the Interior and Kingdom Relations.

Speaking to *GovInsider*, on the sidelines of the recent Festival of Innovation, she shares that quantum secure cryptography is a vital part of the Dutch government’s digital resilience programme, which is the main priority of the country’s overall information strategy.

Wehmann, who took part in FOI, was in Singapore as part of a delegation from the Netherlands and she met, among others, officials from the Cyber Security Agency of Singapore (CSA).

What was once a literary sub-genre in science fiction, post-quantum cryptography now represents a critical evolution in digital security and is designed to protect sensitive information from potential future threats from powerful quantum computers.

“Unlike current cryptographic systems that rely on mathematical problems [which are] difficult for classical computers to solve, post-quantum cryptography uses encryption methods also resistant to quantum computational capabilities,” Wehmann notes.

European Commission also onboard

In Europe, not only for instance the German, French and Dutch governments, but also the European Commission has recognised the strategic importance of post-quantum cryptography, Wehmann explains.

The Commission has launched a recommendation to develop a coordinated EU implementation roadmap for the transition to post-quantum cryptography (PQC).

The goal of the roadmap is to ensure that digital communications and data remain protected, even as quantum computing technology advances, thereby maintaining the integrity and confidentiality of sensitive information in an increasingly complex technological landscape, she adds.

To develop the EU roadmap on PQC, France, Germany, and the Netherlands co-chair the established EU workstream and work together with 21 other EU member states, the EU Commission and the EU agency **ENISA**.

As part of this co-chair team, Wehmann helps to establish the roadmap. “No country or organisation can do this in isolation. We need to work together and help each other. This includes exploring opportunities for further collaboration between the Singaporean and the Dutch government on this common challenge”, she notes.

The workstream is currently working on a first paper with recommendations focused on the EU member states. These recommendations involve creating cryptographic inventories, conducting risk assessments, developing a timeline and implementation plan, but also creating awareness among all stakeholders, she explains.

By following the recommendations in the paper, countries are not only preparing for potential quantum threats but are simultaneously improving their overall cybersecurity maturity and organisational security practices, she adds.

Singapore has also been working to develop digital resilience in the era of quantum computers.

In 2023, Singapore launched its National Quantum-Safe Network Plus (NQSN+). NQSN+ is part of Singapore’s Digital Connectivity Blueprint, which outlines the next bound of Singapore’s digital connectivity to 2030.

Netherlands digitalisation strategy

Talking about the Netherlands' One Nation Digitalisation Strategy, Wehmann emphasises that without digitalisation the Dutch government cannot function and "a lot of investments are needed for this".

There are four independent layers of government in the Netherlands: the national government, provinces, municipalities and the water board.

Noting that these four layers cannot be independently digitalised, a country-wide digitalisation strategy has been formulated.

The priorities for the strategy include a uniform application of cloud technology and the responsible use and sharing of data across all levels of government.

On top of that, the government will utilise artificial intelligence (AI) while putting citizens and entrepreneurs first.

"We will also strengthen the government's digital resilience and digital autonomy so that data is secured, and we can provide the continuity of essential services both in normal and extreme conditions," she adds.

To make all this work, the government has digitally equipped all civil servants with the necessary digital skills, Wehmann says.

Difference between a crisis and an incident

Making a subtle distinction between crisis management and incident management, during her presentation at the Festival of Innovation, Wehmann shares that these two represent distinct approaches to handling disruptions.

Incident management operates within the framework of standard operational procedures, addressing issues through established protocols and routine problem-solving techniques, she notes.

"These are typically predictable scenarios that can be resolved using existing organisational structures, with minimal deviation from normal business operations."

Crisis management, by contrast, says Wehmann, emerges when an event transcends routine handling and threatens the fundamental functioning of an organisation.

"Such situations are characterised by high uncertainty, significant potential impact on continuity, reputation, and assets, and require an extraordinary response," she adds.

The key difference lies in scale and complexity.

While incident management focuses on immediate resolution using standard processes, crisis management demands a holistic approach that encompasses not just solving the immediate problem but also managing broader implications, Wehmann notes.

"In the digital age, particularly with cybersecurity challenges, the line between an incident and a crisis can be increasingly blurred, making sophisticated crisis management frameworks crucial for organisational resilience," she says.

Wehmann notes that having, what she calls, "a lukewarm phase" bridges the gap between crisis management and routine incident handling.

"During this phase, a dedicated team maintains a 24/7 vigilance, conducting regular team meetings and systematically gathering information about a developing situation, particularly in digital and cybersecurity contexts where threats can evolve rapidly," she adds.

The lukewarm phase allows teams to track media reactions, assess infrastructure implications, and make timely, adequate responses before a situation potentially transforms into a full-blown crisis, ultimately enhancing overall organisational resilience and response capabilities, she says.

5. BrainChip-Chelpis-Mirle team up on robotic cryptographic security

by Jean-Pierre Joosting
https://www.eenewseurope.com/en/brainchip-chelpis-mirle-team-up-on-robotic-cryptographic-security/

Chelpis, a chip company leading the Quantum-Safe Migration ecosystem in Taiwan, is developing an M.2 card using the AKD1000 to be inserted into targeted products to support their cryptographic security. The M.2 card is based on a design from BrainChip and an agreement to purchase a significant number of AKD1000 chips for qualification and deployment. Upon completing this phase, Chelpis plans to increase its commitment with additional orders for the AKD1000.

Furthermore, this agreement is the first step in a collaboration exploring the development of an AI-based post-quantum cryptographic security robotic chip designed to fulfil next-generation security and AI computing requirements. This project is a joint development effort with Chelpis partner company Mirle, and it has been formally submitted for consideration under Taiwan's chip innovation program. The funding aims to promote a new system-on-chip (SoC) that integrates RISC-V, PQC, and NPU technologies. This SoC will specifically support manufacturing markets that emphasise a Made-in-USA strategy. Miller plans to build autonomous quadruped robotics that mimic the movements of four-legged animals for industrial and factory environments. Chelpis is exploring BrainChip's advanced Akida™ IP to incorporate advanced visual GenAI capabilities into the proposed SoC design to achieve this.

"The ability to add Edge AI security capabilities to our industrial robotics project that provides the low power data processing required is paramount to successfully achieving market validation in the robotics sector," said Ming Chih, CEO of Chelpis. "We believe that BrainChip's Akida is just the solution we need to bring our SoC to fruition. Their event-based processing and advanced models are a strong foundation for developing a platform for manufacturing customers looking to leverage advanced robotics in their facilities."

"Akida's ability to efficiently provide cyber-security acceleration with energy efficiency can help secure autonomous robotic devices," said Sean Hehir, CEO of BrainChip. "Akida's innovative approach to supporting LLMs and GenAI algorithms could serve as a key contributor to Chelpis as they pursue government funding to develop their SoC and advance their industrial robotic initiatives."

6. NetApp security updates target future quantum threats

by Tim McCarthy
https://www.techtarget.com/searchstorage/news/366623312/NetApp-security-updates-target-future-quantum-threats

NetApp wants to secure enterprise storage against tomorrow's threats today by adding post-quantum encryption algorithms to its storage software.

These new algorithms, available Tuesday for all NetApp customers' block and file workloads, are joined by new ransomware protection updates for NetApp BlueXP, the vendor's hybrid cloud control console.

It never hurts to be ahead of the curve, even if a future of ubiquitous quantum computers won't arrive anytime soon, said Mitch Lewis, an analyst at The Futurum Group.

"[Quantum] is starting to work its way into those checkboxes for security folks," Lewis said. "[It's] still speculation, but it will be [real] at some point."

NetApp's specific post-quantum encryption follows standards released by the U.S. Department of Commerce's National Institute of Standards and Technology last August. These three algorithms are designed to harden general public network encryption and digital signature encryption against quantum computers.

A handful of other storage vendors have started to offer some level of quantum protection, such as IBM for tape backups, Lewis said, but quantum security in storage is still a relatively nascent space.

Network and security teams have begun bracing for quantum computing attacks or challenges, so it makes sense for storage and data teams to brace for similar attacks, said Simon Robinson, an analyst at Enterprise Strategy Group, a division of Omdia.

"Security is a team sport, and it encompasses all aspects of infrastructure," Robinson said. "NetApp is focused on getting ahead of it."

BlueXP updates

New capabilities coming to BlueXP are focused on preventing more immediate ransomware threats, according to NetApp.

These capabilities include role-based access controls based on specific ransomware definitions, so specific security team members or others in the organization can respond to threats that may affect their business. Customers recovering from an attack using BlueXP will benefit from a redesigned UI and data protection workflow creation, the company said.

NetApp's OnTap storage OS will continue to harden itself against ransomware attacks in the months to come, said Gagan Gulati, vice president of product for data services at NetApp. The OS's Autonomous Ransomware Protection capability, which enables real-time detection of ransomware signatures within the storage layer, now supports [Amazon FSx for NetApp OnTap](), an AWS file storage service.

This capability will expand to block workloads this year, which includes a new set of challenges to overcome before wider release to avoid false positives on attacks, Gulati said. Block data provides significantly less information than files, meaning logging changes that indicate malicious changes over daily workload changes need to avoid false positives.

"If you're able to detect early, you can act early," he said. "The false positive rate [needs] to be close to zero."

NetApp's security focus will appeal to enterprise customers who need reliable and secure storage systems over the high-end capabilities and speed that are touted by vendors looking to court generative AI workloads, Lewis said.

NetApp is no stranger to [marketing its platform for AI](), but traditional block and file workloads still dominate much of the enterprise storage market, he said

"It's not like [AI is] the only big customer," Lewis said. "There are still plenty of enterprises that need file storage."

7. Over half of firms prepare for post-quantum cryptography shift

by Catherine Knowles
https://securitybrief.co.uk/story/over-half-of-firms-prepare-for-post-quantum-cryptography-shift

Over half of organisations in the United States, United Kingdom and Germany are making progress towards readiness for post-quantum cryptography (PQC) migration, according to a new survey from Utimaco.

The survey, conducted with more than 200 organisations across three countries, examines the current status and timelines for PQC migration, as well as preferred migration strategies and common barriers.

With quantum computers expected to break common public key encryption schemes by 2030, the urgency to address PQC has become more pressing for IT security professionals. The so-called "Q-Day" – when malicious actors could exploit these new quantum capabilities – would require a shift in the existing cryptographic landscape.

According to the survey's findings, 20% of organisations reported they have already begun migrating to PQC. A further 34% plan to start the process in the next one to three years. Another 21% expect to embark on PQC migration within three to five years, aligning their efforts with the anticipated timeline for quantum threats.

The data also indicates that a quarter of respondents have no current plans to migrate to PQC, highlighting that some sectors may still be assessing the requirements and impact of such a transition.

Migrating to PQC is described by respondents as a significant transformation requiring substantial changes to cryptographic infrastructure across various use cases. Adoption of new cryptographic algorithms poses challenges for legacy systems, especially due to larger key sizes and differences in technical implementation compared to current systems.

The survey reveals that most organisations that have begun planning for PQC are gravitating towards a hybrid cryptographic approach, with 63% favouring a mix of classical and post-quantum cryptographic technologies. This approach aims to combine familiar systems with newer methods for enhanced security during the migration phase.

A range of other strategies are evident among participants. Twenty-six percent view larger symmetric key sizes as a viable defensive measure, while 17% plan to implement full PQC solutions. Twelve percent intend to use Quantum Key Distribution (QKD) as an additional security measure. Another 20% selected none of these or other unspecified methods, which could include utilising larger asymmetric key sizes or adhering to guidelines from national cyber security agencies.

Cindy Provin, Chief Strategy Officer at Utimaco, commented on the findings, stating: "The reality is that quantum threats aren't far away. At Utimaco, we're working closely with customers and partners like NIST to provide solutions that ease the path to post-quantum readiness, and our survey showcases progress towards that goal. While there is still a portion of organizations out there that lack a plan for the road to PQC readiness, we are hard at work to ensure access to easy-to-implement solutions with the latest algorithms to help them - and our customers - on this journey."

The survey results reflect a varied landscape of preparedness among organisations as the anticipated arrival of quantum computing capabilities draws closer. Many are taking a proactive approach to ensuring future-proof security, but other groups remain in the evaluation phase or undecided about their next steps.

8. Quantum Computing Threatens Cyber Defences Globally

by Sophie Rice
https://cybermagazine.com/cyber-security/quantum-computing-creates-cyber-risks-as-firms-lag-behind

Quantum computing is advancing at speed, but most organisations lack strategies to address the cyber risks it brings, according to ISACA research.

Organisations are lagging as technology giants push the boundaries of quantum computing, exposing cyber risks that demand urgent attention.

ISACA, the global professional association for cybersecurity credentials, has found only 4% of organisations have developed strategies to address quantum computing’s impact, despite major hardware advancements from Microsoft, Google and AWS.

European IT leaders voice concerns over cybersecurity threats linked to quantum computing, according to ISACA's latest research.

The report arrives at a time when Microsoft has launched its Majorana 1 chip, Google has introduced its "state of the art" Willow chip and AWS has unveiled its Ocelot chip.

These breakthroughs, emerging in late 2024 and early 2025, indicate that quantum computing could reach everyday business operations sooner than many organisations expect.

ISACA's findings reveal that 67% of European IT professionals fear quantum computing will increase or shift cyber risks over the next decade.

Microsoft's Majorana 1 chip is intended to make quantum computers more viable, while Google's Willow chip and AWS's Ocelot chip represent major leaps forward in quantum processing.

These rapid developments create clear opportunities for innovation, but cyber risks loom large.

Chris Dimitriadis, Chief Global Strategy Officer at ISACA, explains: "Given recent quantum advancements and breakthroughs, we can expect quantum computing to be present in our day-to-day platforms and processes within the next few years.

"Whilst this will present great opportunities for innovation in several industries, significant cybersecurity risks emerge both in terms of quantum in a silo as well as through the rise of quantum AI."

Chris stresses that quantum technology threatens existing internet security: "Cryptography is present in all businesses, industries and sectors, and quantum computing has the potential to break the cryptographic protocols that we use, rendering simple services useless.

"At the same time, quantum will substantially transform AI by boosting its capabilities, together with the risks associated with it."

As hardware progresses, so do the threats.

ISACA's data shows that 67% of IT professionals worry about quantum computing breaking current encryption methods before post-quantum cryptography standards are widely implemented.

Organisations unprepared for quantum computing cyber risks

Despite the National Institute of Standards and Technology (NIST) developing post-quantum cryptography standards for over a decade, understanding remains low among IT professionals.

Only 5% report strong knowledge of these standards, exposing a major risk gap.

The same lack of readiness appears in wider business strategies.

ISACA's research reveals that 52% of organisations have not integrated quantum computing into any formal strategies or roadmaps, nor do they plan to. Meanwhile, 40% of cyber and IT professionals say their organisations have not considered post-quantum cryptography solutions.

Quantum literacy is alarmingly low. Just 2% of respondents strongly agree they understand quantum computing capabilities.

Without adequate understanding of quantum technology, organisations remain vulnerable to emerging cyber risks.

Moreover, most cyber and IT professionals underestimate the pace of change.

Only 35% believe quantum computing will become mainstream within years, despite hardware leaps by Microsoft, Google and AWS suggesting a faster timeline.

These gaps between recognised cyber risks and actual preparation pose serious threats.

Though 56% of respondents see business opportunities in quantum computing, and 44% expect it to enable major innovations, few organisations have developed robust quantum strategies.

Quantum workforce development lags behind technology

The UK Government has committed more than £60m (US$80.4m) to quantum skills programmes running until 2034, recognising the pressing need for expertise.

However, ISACA warns that organisations must match this effort internally to address cyber risks from quantum technology.

ISACA's findings suggest workforce development and strategic planning need urgent improvement. Without investment in training and preparedness, businesses could face cyber threats capable of undermining entire digital infrastructures.

"As a society that relies so heavily on digital systems, it's imperative that we take this seriously," says Chris.

"Organisations must make sure that they are already planning about how their operations might look in a post-quantum world, while they keep developing a holistically trained workforce on AI. They simply cannot afford to defer this critical preparation, risking the stability of the global economy itself.

"We need to build a holistically trained workforce on Quantum (and continue doing this for AI) and then create a plan for transition to the post-quantum era, enabling the safe adoption of these emerging technologies, so we can enjoy the benefits of innovation in a safe manner."

Quantum computing's evolution is no longer theoretical.

It is happening now and cyber risks are growing alongside it.

To protect their operations and take advantage of future technology, organisations must urgently address quantum readiness across strategy, cyber defences and workforce capabilities.

9. Strategy: quantum technology is Finland's new driver of growth and builder of a sustainable future

by Ministry of Economic Affairs and Employment
https://tem.fi/en/-/strategy-quantum-technology-is-finland-s-new-driver-of-growth-and-builder-of-a-sustainable-future

Quantum technology promises an unprecedented leap in computing power, telecommunication security and sensor ability to measure physical quantities. According to Finland's quantum technology strategy published on 24th April 2025, resources are necessary for the research and development of these technologies and their application and the time to invest in them is now.

Finland's key competitive advantage is a well-functioning national ecosystem where the strong competence is based on decades of research on science and technology that support the development of quantum computing. Finland is one of the few countries capable of producing entire quantum computers.

National quantum funding has been limited in Finland compared to the reference countries of Sweden and the Netherlands. As a small country, Finland cannot compete with state aid. Resources should be focused on activities that promote the achievement of quantum benefits as quickly as possible and the utilisation of commercial opportunities after this pre-development phase.

“Finland has the world's leading quantum ecosystem. The new quantum strategy provides the tools and guidelines needed for this ecosystem to develop and further strengthen its position in international competition. Continuing contributions to skills, cooperation and investments are necessary to safeguard this position in the future too,” says CEO of VTT Technical Research Centre of Finland Antti Vasara, who chaired the working group.

“Investing in quantum expertise is a strategic choice for Finland. Our expertise in this area is world-class and it is important to ensure that this continues in future too. Quantum technology is at the focus of international technology competition and we want Finland to remain among the key players in this field,” says Minister of Economic Affairs Wille Rydman.

Eight proposals for measures

The working group proposes eight measures to ensure that the quantum technology sector will play an important role in Finnish business and industry in 2035. These are:

1. **creating a network-like quantum competence centre** that enables the efficient organisation of education and training that supports the development of the quantum technology sector in cooperation between different actors

2. **ensuring access of companies, researchers and students** to world-class quantum computers based on different technologies in environments that also combine artificial intelligence and high-performance computing

3. **establishing a competitive Finnish research and development environment** to support the RDI activities, testing and piloting of quantum devices and components

4. **introducing quantum-secure encryption methods** in infrastructure essential for the critical functions in society

5. **preparing a long-term quantum RDI programme** to create networks of technology developers, researchers and end-users to encourage them to cooperate nationally and internationally

6. **leveraging private funding** to enable global growth of deep-tech companies in the quantum sector

7. **influencing EU-level and international regulation related to quantum technology**, standardisation and the operating conditions of the sector in a way that supports the growth and development of the Finnish quantum ecosystem

8. **organising the national coordination of cooperation** between quantum sector actors and providing resources for this, monitoring of the development of the quantum community, and interest representation.

10. Gmail’s New Encrypted Messages Feature Opens a Door for Scams

by Lily Hay Newman
https://www.wired.com/story/gmail-end-to-end-encryption-scams/

Google announced at the beginning of April that it is launching a streamlined tool that will allow business users to easily send “end-to-end encrypted” emails — an effort to address the longstanding challenge of adding additional security protections to email messages. The feature is currently in beta for enterprise users to try out within their own organization. It will then expand to allow Google Workspace users to send end-to-end encrypted emails to any Gmail user. By the end of the year, the feature will allow Workspace users to send the more secure emails to any inbox. Email spam and digital fraud researchers warn, though, that while the feature will provide a new option for email privacy and security, it will also inevitably spawn new phishing attacks.

End-to-end encryption is a protection that keeps data scrambled at all times except on the sender and recipient's devices, and it is difficult to add to the historic email protocol. Mechanisms to do it are typically very complicated and costly to implement and only make sense for large organizations trying to meet specific compliance requirements. In contrast, Google's end-to-end encrypted email tool is simple to use and doesn't require significant IT overhead. The scenario that digital fraud researchers are most concerned about, though, relates to the case where a Workspace user sends an end-to-end encrypted email to a non-Gmail user.

“When the recipient is not a Gmail user, Gmail sends them an invitation to view the E2EE email in a restricted version of Gmail,” Google wrote in a blog post. “The recipient can then use a guest Google Workspace account to securely view and reply to the email.”

The fear is that scammers will take advantage of this new and more secure communication mechanism by creating fake copies of these invitations that contain malicious links, and prompt targets to enter their login credentials for their email, single sign-on services, or other accounts.

“Looking at Google's implementation, we can see it introduces a new workflow for non-Gmail users—receiving a link to view an email,” says Jérôme Segura, senior director of threat intelligence at Malwarebytes. “Users might not yet be familiar with exactly what a legitimate invitation looks like, making them more susceptible to clicking on a fake one.”

Given email's technical limitations, Google created a way for an organization's Workspace to automatically manage keys — used to descramble encrypted messages. Key management is what makes end-to-end encrypting email so difficult, so offering a solution that is easy for customers is a departure from what's currently available. The fact that the organization's Workspace controls the keys rather than storing them locally on a sender and recipient's devices does mean that the feature doesn't quite qualify as end-to-end encryption in the strictest sense of the term. But researchers say that for use cases like business compliance, the tool could still be extremely useful. And individuals who want end-to-end encrypted communications should just use a purpose-built app like Signal.

When Gmail users receive one of the new encrypted emails from a Google Workspace user, Google's extensive array of dynamic spam filters and fraud detection mechanisms will be in play to protect against spam, phishing, and rogue imposters broadly. But email users outside the Google ecosystem will also be able to receive encrypted email invitations, which makes the service available to anyone, but also will leave non-Google users to their own devices.

Scammers will prey on anything topical to generate new scams, and this threat certainly isn't unique to Google's new encrypted email feature. The invitations to view end-to-end encrypted emails will come with a warning that says, “Be careful when signing in to view this encrypted message. This message is from an external sender and is encrypted. Make sure you trust the sender and their identity provider before entering your username and password.”

“While it’s absolutely true that scammers are always looking for new ways to abuse any product, we built this particular technology with this risk in mind,” Google spokesperson Ross Richendrfer said in a statement. “The notifications users will receive in this case are very similar to Drive file sharing notifications that go out whenever someone shares a doc or file. All the protections we employ to keep scammers from capitalizing on these messages will help us protect this new class of notifications as well.”

Generations of Google Drive and Google Docs scams show, though, that it is particularly difficult to combat imposter invitations outside of Google's ecosystem. But when it comes to the new end-to-end encrypted email feature, “it was either adding a warning or not allowing this feature for non-Gmail users,” Malwarebytes's Segura says.

In fact, the new tool may offer particularly good fodder for scammers, given that Google is such a trusted organization, and targets may have heard about how end-to-end encryption is a special, gold-standard security feature.

“It's almost as if someone at Google knew this was a bad idea and asked for a warning to be added,” Malwarebytes’ Segura says. “It's quite likely fraudsters will jump on the opportunity to craft phishing emails using this exact same template, even including the original warning that will be overlooked.”

11. PQShield launches UltraPQ-Suite for deeply specialized implementations of post-quantum cryptography

by Dr Axel Y. Poschmann
https://pqshield.com/pqshield-launches-ultrapq-suite-for-deeply-specialized-implementations-of-post-quantum-cryptography/?_gl=1*sa0u9p*_up*MQ..*_ga*NzA2ODk3MzM0LjE3NDU2MDA2MjY.*_ga_ZPKYGFFDSF*MTc0NTYwMDYyNi4xLjAuMTc0NTYwMDYyNi4wLjAuMA..

We are proud to announce the launch of a newly updated product suite, beginning with the introduction of PQPlatform-TrustSys – a new quantum-safe Root of Trust solution that will enable ASIC and FPGA hardware to achieve compliance with new PQC standards set out in regulations like the NSA’s CNSA 2.0.

PQPlatform-TrustSys falls under the ultra secure pillar of PQShield’s UltraPQ-Suite, which offers a range of ultra fast, ultra small and ultra secure highly optimized implementations of PQC for critical use cases as the global supply chain delivers the transition to new cryptographic standards.

Deeply-specialised implementations of PQC for a post-standards world

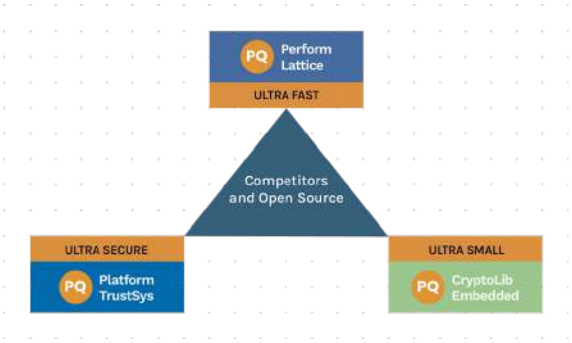
Our varied product suite allows organisations to choose implementations of PQC that best match their priorities – something that is increasingly important for manufacturers that require either fast-performance, high-security, or low-footprint solutions.

Its three pillars – **ultra fast, ultra secure and ultra small** – means we are able to deliver high quality PQC products to address customers’ optimization problems head-on.

- **Ultra fast** delivers high-performance PQC at the core of the network to accelerate new and existing applications in FPGA or ASIC. Our core product in this category, PQPerform-Lattice, optimises key encapsulations per second to maintain strong latency performance and optimise power consumption. This is particularly critical in the networking sector, for example with applications like firewalls, routers and HSMs.

- Our **ultra secure** implementations are optimised for use in products that are the target of highly sophisticated attackers, for instance in critical infrastructure devices with a long lifecycle that require the highest levels of integrity. Side channel attack (SCA) and fault injection attack (FIA) resistance are also key to this category. This is particularly important for device attestation, where confirming that your device has not been tampered with, compromised, or running unauthorized firmware/software enabling remote trust establishment is critical. PQPlatform-TrustSys is our leading product in this pillar but there are also a range of modular IPs that can future proof existing security implementations.

- **Ultra small** targets implementations in memory-constrained devices, embedded systems, microcontrollers and devices that are already in the field, like energy smart meters and industrial controls. Our leading ultra small product, PQCryptoLib-Embedded, is the smallest implementation of PQC on the market. This is particularly useful for OEMs and device manufacturers, where efficient implementations of PQC are needed to secure end-to-end-encrypted (E2EE) comms channels, as well as ensuring data confidentiality and integrity.

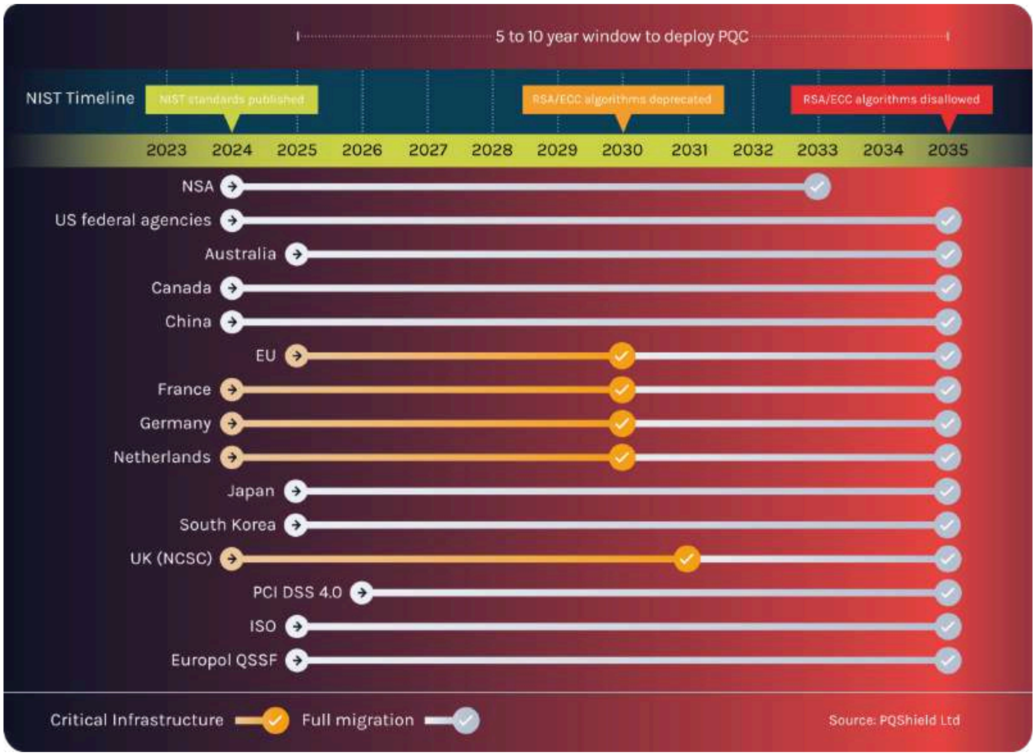


Our deep knowledge of global PQC standards (as co-authors of all PQC standards to date), cryptographic algorithms, patented technologies, protocols and security techniques sets us apart from both competitors and open-source alternatives. Our solutions are rigorously tested to meet Cloud, Edge, or Government grade standards, aligning across certifications like NIST, Common Criteria, SESIP, and PSA.

Introducing PQPlatform-TrustSys – PQC-first Root of Trust

In 2024, the PKfail vulnerability highlighted multiple security issues within Secure Boot and Secure Update mechanisms, which now need to be updated to PQC to protect organisations and maintain platform security, as Secure Boot and Secure Update play a fundamental role in protecting against malware.

Product developers will need to ensure they meet both existing and new regulatory requirements with clear timelines set out by NIST, both for the adoption of PQC and more crucial for Secure Boot, the complete phase-out of RSA by 2035.



Source: PQShield Ltd

The newest product in our range, PQPlatform-TrustSys, is designed to respond to these challenges, helping manufacturers achieve compliance with cybersecurity regulations with minimal integration time and effort. Built as a PQC-first design, this allows for strong, efficient, and quantum-resistant security implementations, free from the limitations of older architectures.

PQPlatform-TrustSys offers comprehensive key management by tracking the key's origin and permission including key revocation, which is an essential and often overlooked part of securing any large-scale cryptographic deployment. It allows the Root of Trust to enforce restrictions on critical operations and maintain security even if the host system is compromised. Additionally, both key origin and permission attributes are extended to cryptographic accelerators that are connected to a Private Peripheral Bus.

When a device is physically exposed to potential attackers – which includes most implementations of ASIC and FPGA hardware in consumer devices, automotive use, and communications networks – so-called "side-channel attacks" that exploit timing, power, and fault vulnerabilities need to be considered as well.

Ali El Kaafarani, founder and CEO of PQShield, said: *"With new standards announced, last year was pivotal in the progress towards quantum security. 2025 is where we run into the real challenge – implementation. Given the wide range of implementation use cases, we need to offer manufacturers enough flexibility and crypto-agility to roll out PQC in a way that meets their priorities.*

"I am proud to be launching PQShield's UltraPQ-Suite to help the supply chain on this journey. Our ultra secure, ultra fast and ultra small products address the major challenges manufacturers face when choosing an implementation of PQC, enabling them to more easily protect the next generation of devices and digital infrastructure that reaches the market."

Dr Axel Poschmann, VP of Product at PQShield, said: *"I am excited to introduce PQPlatform-TrustSys to support ASIC and FPGA manufacturers in bringing quantum-safe products to market. This hardware holds a critical role in the global technology supply chain, and by assisting its adoption of post-quantum cryptography, we can help accelerate the overall global transition to quantum security."*

The launch follows our achievement of FIPS 140-3 certification through the Cryptographic Module Verification Program (CMVP), which is designed to evaluate cryptographic modules and provide agencies and organizations with a metric for security products, as well as building our own silicon test chip to prove this can all be delivered 'first time right'.

12. Post-Quantum Cryptography: Defending Against Tomorrow's Threats Today

by Benjamin Mourad
https://securityboulevard.com/2025/04/post-quantum-cryptography-defending-against-tomorrows-threats-today/#google_vignette

Recent advancements in quantum computing are pushing the boundaries of what is possible for technologists and hackers alike.

Quantum computers leverage the principles of quantum mechanics to solve problems exponentially faster than classical computers, rendering current encryption methods useless.

McKinsey forecasts that by 2030, up to 5,000 quantum computers will be operational worldwide, so while they are not yet a mainstream reality, they still pose an immediate threat. Cybercriminals who "hack now, crack later" can steal encrypted data and decrypt it in the future when quantum computers are readily available.

The federal government is recognizing the importance of safeguarding sensitive data in the quantum era, releasing guidelines like the NIST's post-quantum encryption standards.

But to defend sensitive information, now and in the future, organizations must turn to post-quantum cryptography, or PQC, now. By performing a cryptographic key assessment (CKA), developing a PQC encryption strategy and prioritizing crypto-agility, organizations can prepare for quantum computing cyberthreats.

Immediate Steps to Implement PQC

PQC works by using mathematical equations with quantum properties to create unsolvable encryption equations. To begin transitioning to PQC, organizations must take a methodical and strategic approach.

The first step in any encryption transition is conducting a Cryptographic Key Assessment (CKA), which involves reviewing an organization's existing encryption methods, identifying risks and ensuring compliance with security policies. A CKA also includes examining things like unencrypted traffic, expired certificates, self-signed certificates and weak encryption algorithms.

By performing a CKA, organizations can identify vulnerabilities in their cryptographic hygiene and take steps to improve their security posture. A CKA is a foundational step to validate the current key encryption posture and prepare for quantum readiness.

Once the current encryption landscape is understood, the next step is to develop a PQC encryption strategy. This involves identifying critical assets and data that may be vulnerable to quantum attacks and ensuring they are secured with PQC. The strategy should include selecting appropriate PQC algorithms, such as NIST-approved algorithms like CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+ and Falcon.

It's also essential to ensure that the PQC solution integrates with existing infrastructure and operations without causing disruptions. One effective strategy is to use separate key management systems, which allow for the encryption keys to be changed as needed without affecting data transmission. Additionally, organizations can adopt PQC-as-a-service (PQCaaS) solutions, which enable them to integrate quantum-safe encryption into their current infrastructure without needing to replace hardware or overhaul systems.

Long-Term Recommendations for PQC

PQC is an evolving field, and ongoing support is essential to ensure systems remain secure. Continuous PQC Encryption Support (CPES) helps organizations to ensure their encryption systems are compatible with the latest quantum-safe standards and protected against downgrade attacks. The ongoing support provided by CPES is vital for organizations looking to stay ahead of the curve as quantum computing evolves.

While implementing PQC across an entire organization's network may not be feasible in the short term, organizations should prioritize securing their most valuable data and critical applications – or their "crown jewels." A phased approach allows organizations to pilot PQC within a manageable scope while testing and validating the technology.

Additionally, crypto-agility, or the ability to easily adapt encryption methods as threats evolve, is essential given quantum computing's fluid nature. Organizations should look for PQC solutions that support both symmetric and asymmetric encryption and are flexible enough to adapt as the quantum landscape changes.

Quantum computing represents a revolutionary leap forward in technology, but it also poses a fundamental threat to cybersecurity. PQC offers a viable solution, and organizations should begin implementing it now to ensure their data remains secure in the future.

By assessing their current encryption practices and migrating to PQC, organizations can mitigate the risks posed by quantum computing and ensure they are prepared for the challenges of tomorrow.

13. China breaks quantum code barrier—sparking new concerns over data security

by Akash Pandey
https://www.newsbytesapp.com/news/science/chinese-researchers-break-90-bit-rsa-encryption-barrier-using-quantum-computer/story

A major breakthrough in the field of quantum cryptology, Shanghai University Professor Wang Chao has factored a 90-bit RSA integer.

The achievement was possible using the D-Wave Advantage quantum computer, something that was previously thought impossible.

Quantum cryptology is the practice of writing or solving codes by taking advantage of principles of quantum mechanics in the subatomic world.

Quantum computing: A potential threat to data security

With the rapid advancements in quantum cryptology, it is important to note that experts have been warning us about the risks associated with this technology.

They say we are moving closer to Q-Day - a hypothetical point when quantum computers could break even the most secure encryptions.

This would pose a major threat to personal privacy, data security, prompting scientists globally to develop countermeasures like post-quantum cryptography.

Wang's team surpasses previous quantum cryptology benchmarks

Notably, Wang's team has already broken the previous quantum cryptology benchmarks established by researchers at Fujitsu, Lockheed Martin, and Purdue University.

They did this by creatively combining quantum annealing algorithms with classical cryptographic techniques.

To note, quantum annealing is a technique that employs quantum mechanics to find the minimum energy state of a system, which corresponds to the optimal solution of an optimization problem.

Challenges in quantum computing and cryptography

A Beijing-based quantum computing expert emphasized two major challenges in the field: the absence of self-correction capabilities in existing quantum computers, rendering calculations error-prone, and a hardware-software mismatch.

Wang's team employed the D-Wave Advantage system with 5,760 qubits to convert the RSA factorization problem into a Closest Vector Problem (CVP).

They then employed multiple classical algorithms and the quantum tunneling effect of the annealing process to optimize the CVP solution for increased search efficiency.

Breakthrough may hasten the arrival of quantum threat

While the breakthrough made by Wang's team could hasten the quantum threat, experts have already been urging industries such as banking, blockchain, and government services to proactively adopt post-quantum cryptography.

A practice called "quantum migration" is already in place where advanced encryption techniques are being used to shield sensitive data from being decrypted decades later by future quantum machines.

Wang admitted this achievement isn't the end of RSA encryption.

14. Aegiq, BT, and Others Successfully Demonstrate Performance of their Quantum Link Assurance System (QLAS)

by Joe Spencer
https://quantumcomputingreport.com/aegiq-bt-and-others-successfully-demonstrate-performance-of-their-quantum-link-assurance-system-qlas/

Aegiq and BT, along with other partners successfully demonstrated performance of their Quantum Link Assurance System (QLAS) at Adastral park in Suffolk, England. Funded through UK Research and Innovation (UKRI), the Quantum Link Assurance System solves an important operational obstacle for the commercial adoption of fibre-based QKD, by offering independent link validation. The solution is designed to seamlessly fit into standard optical fibre communications networks.

GQI attended the demo at Adastral Park to view the system and get a better understanding of the wider impact of this project.

What Is It?

First, it’s important to highlight that QLAS is *not* strictly a quantum technology, based on the definition of quantum 2.0. Nor is it a quantum communications system. QLAS utilises mathematical foundations of quantum communications, specifically the statistical covariance matrix, a formulation in CV-QKD to analyse a transmitted wave form injected to a fibre, and on the return, they measure the transmission of correlated light, as well as the uncorrelated light and state of polarisation. This allows QLAS to detect changes in the state of polarisation, or amplitude of light compared to the original wave form and determine if there has been any tampering, eaves-dropping or damage to fibres in optical communications systems. Not only that, it can also detect external interference and act as a passive sensor, so it has applications not only in the telecommunications domain but also in the security sector.

Why Does This Matter?

To BT, this demonstration shows the power of sensing and optics in telecommunications systems. For BT, this is now being implemented alongside BT’s Hydra team to collect data on system health, tampering but mainly in support of front-line engineers and services. This system can detect if a fibre has been bent, damaged, moved and allows BT to have a more resilient service through predictive maintenance. But there's also revenue generation opportunities for BT, as this system is a passive sensor, it could also detect things of interest nearby cables, for example water leaks allowing BT to monetise this data in other service sectors.

The exciting thing about this technology is that it is ready to be integrated into classical systems as well as future quantum systems. Aegiq and BT see this as a stepping stone to getting end-users and customers comfortable and interested in the inevitable coming of quantum technology solutions.

For Aegiq, this demonstration shows near-term commercially viable technology utilising the knowledge and capability of the photonics industry building quantum devices, and allows Aegiq to be present at the end-user community getting clients comfortable with the idea of quantum.

15. Quantum Randomness Could Create a Spoof-Proof Internet

by Gayoung Lee & Lee Billings
https://www.scientificamerican.com/article/quantum-computer-makes-random-number-breakthrough/

The allure of quantum computers is, at its heart, quite simple: by leveraging counterintuitive quantum effects, they could perform computational feats utterly impossible for any classical computer. But reality is more complex: to date, most claims of quantum "advantage" — an achievement by a quantum computer that a regular machine can't match — have struggled to show they truly exceed classical capabilities. And many of these claims involve contrived tasks of minimal practical use, fueling criticisms that quantum computing is at best overhyped and at worst on a road to nowhere.

> Now, however, a team of researchers from JPMorganChase, quantum computing firm Quantinuum, Argonne National Laboratory, Oak Ridge National Laboratory and the University of Texas at Austin seems to have shown a genuine advantage that's relevant to real-life issues of online security. The group's results, published recently in *Nature*, build upon a previous certification protocol — a way to check that random numbers were generated fairly — developed by U.T. Austin computer scientist Scott Aaronson and his former postdoctoral researcher Shih-Han Hung.
>
> Using a Quantinuum-developed quantum computer in tandem with classical, or traditional, supercomputers at Argonne and Oak Ridge, the team demonstrated a technique that achieves what is called certified randomness. This method generates random numbers from a quantum computer that are then verified using classical supercomputers, allowing the now-certified random numbers to be safely used as passkeys for encrypted communications. The technique, the team notes, outputs more randomness than it takes in — a task unachievable by classical computation.

"Theoretically, I think it's interesting because you need to put together a lot of technical tools in order to make the theoretical analysis fly," says Hung, now an assistant professor of electrical engineering at National Taiwan University. "Random-number generation is a central task for modern cryptography and algorithms. You want the encryption to be secure and for the [passkey] to be truly random."

When it comes to Internet security, randomness is a weapon — a mathematically impenetrable shield against malicious adversaries who seek to spy on secret communications and manipulate or steal sensitive data.

The two-factor authentication routinely used to protect personal online accounts is a good example: A user logs in to a system with a password but then also uses a secure device to receive a string of randomly generated numbers from an external source. By inputting that string, which can't be predicted by adversaries because of its randomness, the user verifies their identity and is granted access.

"Random numbers are used everywhere in our digital lives," says Henry Yuen, a computer scientist at Columbia University, who was uninvolved with the study. "We use them to secure our digital communications, run randomized controlled trials for medical testing, power computer simulations of cars and airplanes—it's important to ensure that the numbers used for these are indeed randomly generated."

In more cryptographic applications, on the other hand, it's not enough to just generate random numbers. We need to generate random results that we know for certain are the outcome of an unbiased process. "It's important to be able to prove the randomness to a skeptic who does not trust the device producing the randomness," says Bill Fefferman, a computer scientist at the University of Chicago, who was not involved in the new work. Implementing such protocols to check each and every outcome would be "impossible classically," Fefferman says, but possible with the superior computational potential of quantum devices.

"Quantum computers and quantum technologies offer the only way to reliably generate and test randomness," Yuen says. Unlike classical computers, which depend on binary "bits" to process information, quantum computers operate on qubits, which can have an infinite number of possible orientations when existing in a superposition state. These qubits allow quantum computers to process exponentially larger loads of data at much faster rates.

The quantum computer involved in the latest demonstration uses 56 such qubits to run the protocol developed by Aaronson and Hung. The gist of the procedure is relatively straightforward. First, the quantum computer is given a complex problem that requires it to generate random outputs, in a process called random circuit sampling. For a small enough quantum computer, usually under 75 qubits, these outputs can be traced on classical computers to ascertain that the results couldn't have been generated classically, explains Christopher Monroe, a quantum computing expert at Duke University, who was not involved in the study.

Verifying this is the next step in the protocol, but it includes an added caveat: time. The quantum computer must generate its outputs faster than they could be mimicked (or "spoofed") by any known classical computing method. In the team's demonstration, the Quantinuum system took a couple of seconds to produce each output. Two national laboratory supercomputers subsequently verified these outputs, ultimately devoting a total of 18 hours of computing time to generate more than 70,000 certified random bits.

These bits were certified using a test that gives the outcomes something called a cross-entropy benchmarking (XEB) score, which checks how "ideal" the randomness of the distributions is. A high XEB score coupled with a short response time would mean that a certain outcome is very unlikely to have been influenced by any interference from untrusted sources. The task of classically simulating all that effort to spoof the system would, according to Aaronson, require the continuous work of at least four comparable supercomputers.

"The outcome of the [certified randomness test] is governed by quantum-mechanical randomness—it's not uniformly random," Aaronson says. For example, in the case of Quantinuum's 56-qubit computer, 53 out of

56 bits could have a lot of entropy, or randomness, and that would be just fine. "And, in fact, that it's not uniform is very important; it's the deviations from uniformity that allow us to test that in the first place that yes, these samples are good. They really did come from this quantum circuit."

But the fact that these measurements must be additionally verified with classical computers puts "important limits on the scalability and utility of this protocol," Fefferman notes. Somewhat ironically, in order to prove that a quantum computer has performed some task correctly, classical supercomputers need to be brought in to pick apart its work. This is an inherent issue for most of the current generation of experiments seeking to prove quantum advantage, he says.

Aaronson is also aware of this limitation. "For exactly the same reason why we believe that these experiments are very hard to spoof using a classical computer, you're playing this very delicate game where you need to be, like, *just* at the limit of what a classical computer can do," Aaronson says.

That said, this is still an impressive first step, Fefferman says, and the protocol will be useful for instances such as public lotteries or jury selection, where unbiased fairness is key. "If you want random numbers, that's trivial—just take a Geiger counter and put it next to some radioactive material," Aaronson says. "Using classical chaos can be fine if you trust the setup, but doesn't provide certification against a dishonest server who just ignores the chaotic system and feeds you the output of a pseudorandom generator instead," Aaronson adds in a reply to a comment on his blog post about the protocol.

Whether the protocol will truly have practical value will depend on subsequent research—which is generally the case for many "quantum advantage" experiments. "The hype in the field is just insane right now," Monroe says. "But there's something behind it, I'm convinced. Maybe not today, but I think in the long run, we're going to see these things."

If anything, the new work is still a formidable advance in terms of quantum hardware, Yuen says. "A few years ago we were thrilled to have a handful of high-quality qubits in a lab. Now Quantinuum has made a quantum processor with 56 qubits."

"Quantum advantage is not like landing on the moon—it's a negative statement," Aaronson says. "It's a statement [claiming that] no one can do this using a classical computer. Then classical computing gets to fight back.... The classical hardware keeps improving, and people keep discovering new classical algorithms."

In that sense, quantum computing may be akin to "a moving target" of sorts, Aaronson says. "We expect that, ultimately, for some problems, this war will be won by the quantum side. But if you want to win the war, you have to do problems where the quantum advantage is a little bit iffier, where it's a little bit more vulnerable."

16. Bruce Schneier tackles AI hype, NSA surveillance, and cyber 'rage fatigue'

by Tom Spring
https://www.scworld.com/news/bruce-schneier-ai-hype-nsa-surveillance-and-cybersecuritys-real-challenges

Security technologist Bruce Schneier tackled some of cybersecurity's toughest questions in a candid AMA-style session Thursday (17 Apr 2025). In it, he covered AI, NSA surveillance, cryptography and broader societal threats beyond typical cyber concerns.

Responding to "rage fatigue" tied to a drumbeat of recent bad news headlines in cybersecurity from the gutting of CISA, recent CVE-MITRE scares and the DOJ's targeting of Chris Krebs, Schneier said:

"We're at the receiving end of a strategy that is deliberately designed to be overwhelming and exhausting. All we can do is help where we can, and stay confident that others are doing the pieces we can't do."

The threat of tariffs on computer components, semiconductors and the potential restrictions of software exports is also taking a cyber toll, Schneier said. "The world's economies are deeply, inexorably international, and the current trade war is going to disrupt things in ways we are not anticipating. And it's not going to be good."

The AMA was moderated by Cecilia Marinier, Vice President of Innovation and Scholars at the RSA Conference and part of an RSAC Community Event. Schneier will speak later this month at the RSAC 2025 cybersecurity conference at a keynote titled *AI, Security, and Trust*.

At times philosophical, other times blisteringly direct, Schneier's shed light on a cybersecurity landscape fraught not only with technical vulnerabilities but also with deep moral fissures as he sees it.

Cybersecurity: A 'rounding error' amid existential threats

When asked directly about the most pressing digital threats, be it AI misuse or quantum computing, Schneier quipped. "I generally hate ranking threats, but if I had to pick candidates for 'biggest,' it would be one of these: income inequality, late-stage capitalism, or climate change," he wrote. "Compared to those, cybersecurity is a rounding error."

Cryptography's moral imperative

Schneier downplayed fears around quantum computing. "The engineering challenges are nowhere near solved. And two, the math is way ahead of the physics — we are slowly getting quantum-resistant cryptography algorithms," he explained.

Asked whether cryptography should formalize ethics as rigorously as it does security he citing Phil Rogaway's seminal paper, *The Moral Character of Cryptographic Work* stating cryptographers can no longer afford to be apolitical technicians. Ethics, he implied, must be engineered.

"I'm intrigued by the idea that multiagent systems (networks of autonomous software agents that interact and make decisions) could be designed to embed certain values," Schneier said. "It's not something I've thought about much, but it makes sense. And it ties into a broader frustration I have with how people talk about bias in AI... We like some biases. Maybe a bias towards fairness, or justice, or kindness. When we like biases, we call them values. And, yes, we are going to want that."

AI Snake Oil and the marketing mirage

Discussing artificial intelligence, Schneier anticipated SOC analysts and incident responders using AI as a vital support tool.

"What I expect to happen is for both SOC analysts and incident responders to have a bevy of AI tools at their disposal, and that those tools will make the humans faster and more effective," Schneier wrote.

At the same time, he also cautioned of widespread "AI snake oil," noting bluntly that many vendors push AI solutions that are mostly "marketing bulls#!t."

"I think that AI-assisted incident response is more likely to be on the real side," he said.

Security Theater and the psychology of safety

He also reaffirmed the persistent relevance of his well-known critique, "security theater," highlighting ongoing airport screening practices by the Transportation Security Administration as emblematic of giving the public a false sense of security. Schneier wrote, "The difference between the feeling of security and the reality of (cybersecurity) will continue to be a pervasive problem in our industry."

It's an ongoing tension for CISOs, many of whom face boardroom pressures to deliver *visible* security more than *effective* security. Schneier's advice, implicit throughout the conversation, is to resist that pressure – or at least be aware of its consequences.

NSA Post-Snowden: A decade without reform

Asked directly about NSA reforms post-Snowden, Schneier was skeptical, responding: "Well, they haven't had any leaks of any magnitude since then, so hopefully they did learn something about OPSEC. But near as we can tell, nothing substantive has been reformed."

Schneier further clarified, "We should assume that the NSA has developed far more extensive surveillance technology since then," stressing the importance of vigilance.

He touched on the fusion of AI and democracy - a theme of his upcoming book *Rewiring Democracy* - noting that he didn't "think that AI as a technology will change how different types of government will operate. It's more that different types of governments will shape AI."

He is pessimistic that countries will harness AI's power to do good and help improving quality of life.

"It would be fantastic if governments prioritized these things," he said. "[This] seems unrealistic in a world where countries are imagining some sort of AI 'arms race' and where monopolistic corporations are controlling the technologies. To me, that speaks to the solutions: international cooperation and breaking the tech monopolies. And, yes, those are two things that are not going to happen."

The Ethics of Healthcare Data and the Illusion of Consent

As the Internet of Things (IoT) weaves itself into everything from heart monitors to insulin pumps, Schneier warned of privacy and integrity risks in healthcare. But the dilemma, he emphasized, isn’t just about safeguarding individual data – it’s about collective ethics.

“We want the data to be private, and we want it to be used collectively,” he said. “Navigating this will be a continual challenge, even more so as AI healthcare systems become prevalent.”

His solution? Not better design or voluntary compliance, but legislation – the one lever, Schneier noted with a hint of resignation, that the market systematically resists. “The market doesn’t reward companies that respect ‘user autonomy and dignity,’” he noted. “If we want those things, we need to compel companies to provide them.”

Rage fatigue in the face of constant chaos

Schneier addressed geopolitical risks and how tensions might affect cybersecurity and the broader IT ecosystem in light of Trump administration tariffs.

"The world's economies are deeply, inexorably international, and the current trade war is going to disrupt things in ways we are not anticipating," he cautioned. "And it's not going to be good," he wrote. "And when it gets better, it won't be in a world where the US is the dominant superpower."

That bleak prognosis came with a sliver of hope. Schneier's final takeaway was the growing awareness of these complex issues within society and the cybersecurity community. By openly addressing challenges and advocating for proactive, informed engagement, Schneier expressed confidence that collective action and intelligent solutions can ultimately enhance resilience and security.

Schneier was hopeful the development of multiple AI models will lead to a more diverse and distributed AI landscape. Development of diverse AI models is already a reality as the EU pushes for sovereignty in AI technology.

"I am optimistic about DeepSeek's demonstration that you don't need hundreds of millions of dollars to create a foundation mode," he wrote, adding that clever hardware optimizations and collaborative model training could foster robust competition. "Monopolization is the major enemy here," Schneier said. "Robust market competition is the solution."

Bruce Schneier will explore these critical themes further at the upcoming RSA Conference, discussing AI, trust, and data integrity.

17. India and Italy Sign Pact to Deepen Science Ties, Target Quantum, AI and Biotech

by Matt Swayne

https://thequantuminsider.com/2025/04/21/india-and-italy-sign-pact-to-deepen-science-ties-target-quantum-ai-and-biotech/?utm_source=resonance-newsletters.beehiiv.com&utm_medium=newsletter&utm_ca

mpaign=the-quantum-insider-weekly-quantum-rising-in-japan-billion-dollar-quarter-for-quantum-and-more-news&_bhlid=1f00de7e88a1681f19968317ba514042ada1d1f4

India and Italy have signed a fresh memorandum of understanding to deepen scientific cooperation across high-impact areas like quantum technology, artificial intelligence and biotechnology, signaling a growing alignment in emerging tech strategy between the two countries.

The agreement was formalized during a high-level meeting in New Delhi between Italy's Minister of University and Research, Anna Maria Bernini, and India's Minister of State for Science and Technology, Jitendra Singh. The meeting marked the latest step under a broader Joint Strategic Action Plan 2025–2029, which was first outlined by Prime Ministers Narendra Modi and Giorgia Meloni during the G20 Summit in Brazil.

The new memorandum was highlighted in a joint statement released following the meeting. It noted that both nations would implement the 2025–2027 Executive Programme of Cooperation (EPOC) for Scientific and Technological Collaboration. The statement said the EPOC would support at least 10 joint mobility research projects and 10 major collaborative research initiatives across sectors, ranging from big data and AI to biotechnology and digitalization.

According to the statement, over 150 joint Indo-Italian scientific projects have already been executed under previous iterations of the program. The renewed partnership aims to build on this legacy by integrating newer technologies and by leveraging both countries' academic and industrial strengths.

The two governments stressed that science and technology cooperation is a core pillar of the broader India-Italy relationship. The statement cited previous agreements and collaborations in infectious diseases, green hydrogen, renewable energy, cultural heritage technologies, and the blue economy. Emerging areas of focus now include Industry 4.0 and clean energy innovation.

Dr. Singh used the occasion to showcase India's recent technological achievements. These include the development of the world's first DNA-based COVID-19 vaccine, the launch of a homegrown HPV vaccine, and the rollout of Nafithromycin — an Indian antibiotic developed for respiratory infections. He also highlighted India's first successful gene therapy trial and the establishment of a national genome data bank.

India's strategic investments and policies are steering the nation toward becoming a global hub of emerging technologies, the statement quoted Singh as saying. He also drew attention to India's high-performance computing and artificial intelligence capabilities, adding that the nation now has the third-largest startup ecosystem globally.

Agriculture and health-related technologies were also featured prominently in the discussions. Singh mentioned India's Aroma Mission — also known as the Purple Revolution — which promotes floriculture and aromatic crop production. He pointed to the success of tech-enabled schemes like the Soil Health Card and Swamitva Yojana, which have deployed drones and GIS tools to transform Indian agriculture.

Singh emphasized that the country's innovation strategy includes preserving ancient knowledge through digital tools. The Traditional Knowledge Digital Library (TKDL), which documents traditional Indian medicine and practices in a searchable format, was cited as an example of integrating heritage and science.

In the realm of ocean exploration, Singh — who also oversees Earth Sciences — updated the Italian delegation on India's Deep Ocean Mission. The statement said India plans to send a submersible 6,000 meters below sea level, with a 500-meter test dive scheduled for next year.

The joint statement reaffirmed Italy and India's interest in working together on quantum technologies and advanced scientific applications, noting that these fields are now essential to both national innovation and global competitiveness. The agreement is seen as an extension of shared priorities laid out during G20 discussions and is expected to lead to further academic and industry linkages.

Senior Indian officials, including Dr. Rajesh Gokhale, Secretary of the Department of Biotechnology, and Prof. Abhay Karandikar, Secretary of the Department of Science and Technology, also participated in the meeting.

The joint India-Italy statement underscores both countries' intent to support startups and small businesses engaged in scientific innovation. It emphasized new opportunities for academic and industrial partnerships that can connect researchers, institutions and entrepreneurs across the two nations.

18. Quantum Contest Offers 1 Bitcoin for Cracking Encryption with Shor's Algorithm

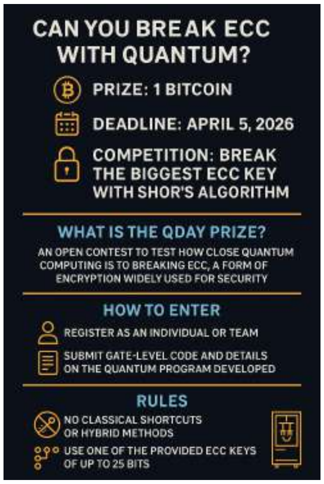
by Matt Swayne
https://thequantuminsider.com/2025/04/18/quantum-contest-offers-1-bitcoin-for-cracking-encryption-with-shors-algorithm/

A new competition is offering a single Bitcoin to anyone who can break elliptic curve cryptography using a quantum computer — no shortcuts allowed.

Launched by Project Eleven, an open science initiative focused on quantum and cryptographic challenges, the *QDay Prize* aims to test just how close quantum computing is to undermining one of the world's most widely used encryption schemes. The contest runs through April 5, 2026.

Elliptic Curve Cryptography, or ECC, secures a wide range of systems — from Bitcoin wallets and secure websites to messaging apps and government infrastructure. Its appeal lies in efficiency: a 256-bit ECC key delivers the same protection as a much larger 3,072-bit RSA key. And while classical computers struggle to crack ECC, quantum computing presents a real threat, if it can be made to work.

Right now, a Bitcoin is worth about $84,000.



CAN YOU BREAK ECC WITH QUANTUM?

PRIZE: 1 BITCOIN

DEADLINE: APRIL 5, 2026

COMPETITION: BREAK THE BIGGEST ECC KEY WITH SHOR'S ALGORITHM

WHAT IS THE QDAY PRIZE?

AN OPEN CONTEST TO TEST HOW CLOSE QUANTUM COMPUTING IS TO BREAKING ECC, A FORM OF ENCRYPTION WIDELY USED FOR SECURITY

HOW TO ENTER

REGISTER AS AN INDIVIDUAL OR TEAM

SUBMIT GATE-LEVEL CODE AND DETAILS ON THE QUANTUM PROGRAM DEVELOPED

RULES

NO CLASSICAL SHORTCUTS OR HYBRID METHODS

USE ONE OF THE PROVIDED ECC KEYS OF UP TO 25 BITS

PURE QUANTUM POWER

The challenge is simple in premise but formidable in execution: "Break the largest ECC key possible using Shor's algorithm on a quantum computer," according to Project Eleven. Submissions must demonstrate gate-level implementation of Shor's algorithm solving the elliptic curve discrete logarithm problem (ECDLP): "No classical shortcuts. No hybrid tricks. Pure quantum power."

Participants can register as individuals or teams, with no institutional affiliation required. Submissions must include quantum program code, a written explanation of the method, and details about the hardware used.

The quantum machine doesn't need to be publicly available, but the organizers emphasize transparency, adding they will share submissions publicly.

The project has prepared a set of ECC keys ranging from 1 to 25 bits for testing. That's well below the 256-bit keys used in actual Bitcoin wallets, but a successful attack – even at 3 bits – would mark a real milestone.

That's because Shor's algorithm, introduced in 1994, remains one of the most important theoretical breakthroughs in quantum computing. The algorithm allows a sufficiently large quantum computer to solve certain mathematical problems exponentially faster than any known classical method. Among them: factoring large integers and solving the ECDLP, which underpins ECC.

HOW SHOR'S ALGORITHM WORKS

Shor's algorithm works by turning the problem into one of finding the period of a mathematical function – a task quantum computers can solve efficiently using the Quantum Fourier Transform.

The algorithm creates a superposition of states, allowing it to explore many inputs at once and use interference to zero in on the correct answer. For elliptic curve cryptography, it targets the elliptic curve discrete logarithm problem, making it a powerful theoretical threat to modern encryption systems.

ERROR-PRONE QUANTUM SYSTEMS

Practical implementation of Shor's algorithm remains difficult. Today's quantum systems are error-prone and limited in scale. Running Shor's algorithm reliably requires high-fidelity qubits and error correction, both of which remain active areas of research.

"Today's qubits have 99% – 99.9% fidelity – is that good enough?" Project Eleven asks on the QDay Prize website.

Despite the limitations, quantum progress is accelerating. Companies and countries are advancing hardware steadily. Estimates suggest that around 2,000 logical (error-corrected) qubits may be enough to break a 256-bit ECC key, something researchers believe is achievable within the next decade.

That readiness has become a focus of international cryptographic communities. The U.S. National Institute of Standards and Technology (NIST) is already standardizing post-quantum algorithms, ones designed to resist quantum attacks. But until quantum systems are capable of breaking something real, no one knows exactly how urgent the threat is.

So far, no real-world ECC key has been broken by either classical or quantum methods. The best classical attacks remain exponentially slower than quantum ones in theory, and quantum demonstrations to date have only handled toy problems.

"Quantum computing is advancing fast, and the impact on cryptography is inevitable," the organizers say. "Instead of waiting for breakthroughs to happen behind closed doors, we believe in facing this challenge head on, in a transparent and rigorous manner."

19. Organizations Must Prepare Now for Q Day

by Kirsty Paine
https://www.iotworldtoday.com/quantum/organizations-must-prepare-now-for-q-day

Prioritizing post-quantum cryptography today is critical, even though threats may be years away. This allows companies to avoid rip-and-replace scenarios later.

Who wouldn't be animated by the prospect of uncrackable codes suddenly becoming vulnerable to a shadowy quantum supercomputer?

In preparing for the so-called 'Q Day' — whenever it happens — it's important that organizations maintain a sense of perspective over exactly what the threats posed to your business may be and prioritize accordingly, taking a measured approach. Worrying about your potential choice of post-quantum cryptographic algorithm while your critical assets remain unpatched is a bit like fighting over the vol-au-vents on the Titanic. There's no need for organizations to panic; just start thinking about migration strategies and planning.

I've previously stated that there's a Goldilocks zone for migrating to post-quantum cryptography — cryptography that isn't weakened or broken by a quantum computer. Move too soon, before the wider ecosystem is ready and standards have matured, and you could lack interoperability. Move too late, and you could be vulnerable to the quantum threat. So choose your post-quantum porridge to be "just right" and move at the right moment.

In preparing, it's key that businesses start by assessing which assets are vulnerable to the quantum threat. That is, data that could be stored today and later decrypted by a sophisticated adversary, data that needs to stay secret for decades, or cryptographically signed artifacts that need to be verified for years into the future.

Start by assessing assets that use public-key cryptography and are, therefore, vulnerable to Shor's algorithm. Consider rolling to using ephemeral, per-connection keys, which is good security practice anyway and will limit the exposure to the post-quantum threat. If someone cracks one key exchange, they only get one key. For signatures, as the lifetime is usually limited by certificate policies, you can de-prioritize signatures with a shorter lifespan.

For assets vulnerable to Grover's algorithm, i.e., those using AES, simply ensure the key size is at least 128 bits. This will make it impractically expensive to perform a quantum cryptographic attack.

At the heart of all this, there's a straightforward auditing job: Assess which data is most critical and which poses the greatest security, compliance or operational risk to your business, and how vulnerable it is, and prioritize that. Also, there's the time factor: what data and assets will be retired before quantum decryption becomes a reality? Most businesses don't need to plan to migrate 100% of what they have today, as assets get end-of-lifed.

Reimagining the CISO Role

Some companies are exploring ways to embed longer-term quantum planning into the chief information security officer function, whether through extending tenures, creating quantum-specific roles or engaging external experts.

If your organization is planning to hire a CISO with skills or a background related to quantum cryptography or post-quantum planning, as some are, there is a small—and, at the moment, practically non-existent—pool to draw on. Such an approach is also largely unnecessary. For most CISOs, preparing for quantum won't require deep knowledge of quantum mechanics. As outlined, CISOs can begin preparing a quantum-ready strategy by following relatively simple guidelines and best practices.

However, one factor that hasn't received nearly enough attention is CISO tenure. Quantum-readiness strategies require that businesses take the "long view." It's estimated that quantum readiness programs will take around five to 10 years from planning to implementation. However, the current average CISO tenure is just 18 months. In other words, your organization may see several CISOs come and go during this five to 10-year window, and filtering planning and execution through multiple CISOs isn't the most obvious formula for a coherent program. Each CISO will have different approaches and priorities and is unlikely to agree to, accept, and work with a strategy formulated wholesale by their predecessor.

One approach to solving this could involve the return of contracts – pinning CISOs down to longer, project-based tenures of, say, five years. Another might be the escalation of the quantum strategy to the board or, perhaps more usefully, a more specialist or focused function in the business. Whatever the approach, organizations need to consider this sooner rather than later.

20. Mind the quantum threat: Migration to post-quantum cryptography as essential step to safeguard sensitive data and protect critical systems

by Dr. Richard Weller, Andrey Bogdanov, Lucas Sy
https://www.linkedin.com/pulse/mind-quantum-threat-migration-post-quantum-essential-step-weller-ko7qf/

As we advance into the era of quantum computers, the most well-known application of these powerful machines – breaking the existing cryptographic systems such as RSA and ECC – is becoming a pressing concern. These systems are foundational to securing internet communications and protecting sensitive data. While conservative estimates suggest that quantum computers capable of compromising these cryptographic methods might emerge within 10 to 15 years, some experts also predict their availability by the early 2030s, so practically within the next five years. Regardless of the exact timing, the urgency of deploying countermeasures is clear, as it is high-value sensitive data and critical systems that are to be exposed.

Assessing the Need for Immediate Action

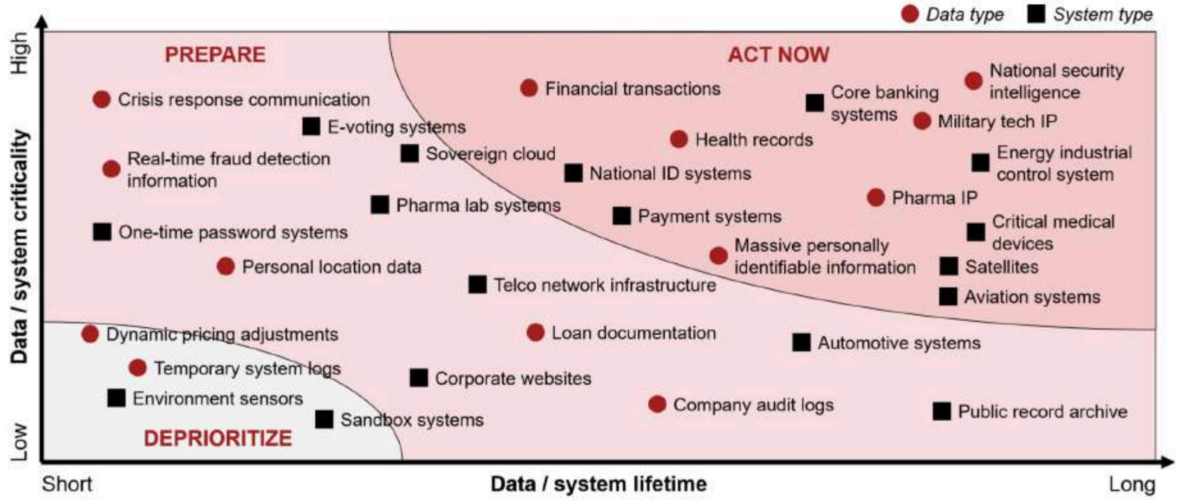


Figure 1: Quantum Impact Matrix to evaluate vulnerability of data and systems to the quantum threat with exemplary data and system types

Organizations must evaluate their need for quantum-safe cryptography by considering the longevity and sensitivity of their data and IT systems. A helpful framework is the Quantum Impact Matrix (QIM), assessing data and systems criticality against their lifetime (see Figure 1). Long-lifetime, high-sensitivity data, such as critical financial records or medical history, should be prioritized in the transition to quantum-safe cryptography. The same logic applies when evaluating the IT systems handling relevant data. Aviation systems, for example, are operated for tens of years and can be critical for flight safety, underlining the importance to already consider the quantum threat in today's system architectures.

For data and systems that need protection for more than five years, immediate action is essential. This urgency is underscored by the "harvest now, decrypt later" strategy that attackers can apply. Indeed, already today, adversaries can collect sensitive encrypted data, for instance, by intercepting and storing encrypted network traffic on the public Internet. Once a quantum computer of sufficient size and quality becomes available, the adversaries will be able to get access to this sensitive data.

Moreover, it's not just confidentiality that's at risk – authenticity is equally threatened. Digital signatures, which verify the origin and integrity of data, contracts, and communications, also rely on cryptographic methods and are susceptible to quantum attacks. If these signatures are compromised, it could lead to data tampering and fraud, undermining trust in digital transactions and communications. On a cryptographically relevant quantum computer, adversaries will be able to successfully forge the digital signature of another party under any document.

Embracing Post-Quantum Cryptography

Post-quantum cryptography (PQC) emerges as a critical solution in the face of the quantum threat. PQC methods are explicitly designed to withstand the capabilities of quantum computers, offering a robust alternative to vulnerable existing cryptographic systems. In August 2024, the US National Institute of Standards and Technology (NIST) released the first standards for PQC. These standards provide concrete, efficient, quantum-resistant mechanisms to replace today's vulnerable cryptographic methods. Thus, NIST plans to disallow all non-PQC methods in the US government's IT systems after 2035. The NSA has even mandated the migration of US national security systems to PQC already by 2030 for some applications.

By adopting PQC, businesses can ensure the authenticity and confidentiality of data in their digital infrastructure, safeguarding it against the advancing quantum frontier. To effectively mitigate the quantum threat, a comprehensive strategy is required. An effective approach involves the following five steps that organizations should consider:

1. **Build awareness and upskill staff:** Conduct workshops and training programs to educate staff, from executive management to technical teams, on the risks and mitigation options. Upskill in-house experts and ensure regular updates on the evolving PQC landscape.

2. **Update the data security strategy:** Perform an initial analysis of the IT landscape to identify risks and vulnerabilities. Develop or update a tailored data security strategy focused on post-quantum safety. Plan the integration of PQC solutions into their existing IT architecture, considering compliance and regulatory requirements.

3. **Assess systems & perform a crypto inventory:** Conduct a detailed analysis of systems and IT infrastructure to identify relevant data and controls. Create a comprehensive inventory of cryptographic controls in use, both for their own and third-party technology, assessing their quantum resistance and classifying data and systems based on criticality and lifetime.

4. **Implement PQC solutions and crypto-agility:** Implement standardized PQC where available, and, if necessary, design custom quantum-safe security controls. Develop a plan for cryptographic agility to adapt to evolving PQC algorithms.

5. **Monitor and react to the evolving landscape:** Continuously monitor and react to new standards, regulations, and advancements in quantum threats. Stay informed about updates in third-party products and advances in attacks on quantum-safe cryptographic mechanisms.

Conclusion

In as little as five years, quantum computers might be powerful enough to compromise our current data and system protection methods. Preparing for the quantum age is thus not merely about adopting new technology; it's about ensuring the continuity and security of an organization's most critical assets. By taking these steps now, organizations can mitigate quantum threats and position themselves for long-term success in a rapidly changing digital landscape.

21. The Critical Quantum Timeline: Where Are We Now and Where Are We Heading?

by Bernard Marr
https://www.forbes.com/sites/bernardmarr/2025/04/10/the-critical-quantum-timeline-where-are-we-now-and-where-are-we-heading/

Quantum computing might seem like “just another” new technology, like the internet, cloud computing and AI.

In fact, it’s something rather different – more similar to the leap forward from the earliest valve-based computers to modern transistors and microprocessors.

These paradigm shifts in computing don’t just bring us faster computers– they bring computers that work with data in entirely new ways. In the case of quantum computers, this means leveraging the weird and wonderful properties of quantum science, like superposition and quantum tunneling, to complete some tasks millions of times more quickly than classical computers.

Make no mistake – quantum computing is a big deal and will redefine the way we use computers to understand the real world. From simulating the complex interactions between molecules that make modern medicine possible to predicting the behavior of chaotic systems like financial markets and the weather.

Recent breakthroughs include the achievement of quantum supremacy — maybe (We'll explore this below.) But for most of us, quantum computing is far from an everyday part of life, and huge opportunities are still there for the taking.

So, let’s take a look at the major developments we can expect to see as the future unfolds.

Quantum Today

We start our roadmap with quantum computing, which has already achieved several significant milestones and is moving out of labs and into businesses. Media coverage often revolves around the issue of quantum supremacy – the point where quantum computers will perform tasks that would be impossible or impractical for "classical" computers.

Google claimed to have achieved it in 2019 with its 54-bit Sycamore quantum processor, but its performance was later beaten by classical computers. China's University of Science and Technology once again made the claim in 2020, and most recently, D-Wave, which sold the first commercial quantum computers in 2011, carried out a material simulation in 20 minutes that would take the most powerful supercomputers almost a million years.

As well as becoming more powerful, quantum is also starting to become accessible. Tech giants including Amazon, Google and Microsoft offer quantum-as-a-service, bringing the barrier to entry lower than ever, and paving the way for anyone with ideas to start building quantum applications to fit their needs.

Applied Quantum Supremacy

So, it's all well and good that quantum computers can beat classical computers at hugely complicated theoretical calculations in laboratory conditions. A more significant milestone will be reached when they offer real improvements when it comes to running practical applications.

Exactly when this will happen has been the subject of some debate. The CEO of Nvidia caused quantum computing stock prices to drop when he recently said practical quantum computing was "decades away" (he later admitted he might be wrong about this).

Google's director of Quantum AI, however, has said he believes it could be as little as five years until quantum computers become the go-to option for common tasks that they're more suitable for than classical computers.

Quantum Encryption

At some point in the not-so-far-off future, quantum computers will become powerful enough to easily crack many forms of digital encryption. Unfortunately, this includes some public key security protocols like RSA cryptography, which, among other things, is used to secure private conversations, financial transactions and government communications systems.

This is not unforeseen, and for some time, cybersecurity researchers have been working on the challenge of creating quantum-safe cryptography. Former U.S. President Joe Biden issued an executive order making this a national security priority.

As the era of useful, powerful, accessible quantum computing dawns, we will see a race to find and protect systems that could become compromised. Back in 2016, as the scope of the problem became apparent, Dr. Michele Mosca of the Institute For Quantum Computing estimated a one in seven chance that public key encryption would become worthless by 2026 and a fifty-fifty chance of it happening by 2031.

More Reliable Quantum Computing

Technically, the term is fault-tolerant quantum computing. The qubits that quantum computers use to process data have to be kept in a delicate state – sometimes frozen to temperatures very close to absolute zero – in order to stay stable and not "decohere". Keeping them in this state for longer periods of time requires large amounts of energy but is necessary for more complex calculations.

Recent research by Google, among others, is pointing the way towards developing more robust and resilient quantum methods. This includes trapped ion quantum computing, which isolates positively charged ions in a way that makes them stable for longer periods of time. Another technique demonstrated by scientists at QuTech involves measuring the spin of electrons inside diamonds. It's predicted that truly fault-tolerant quantum computers could be a reality by 2030.

Quantum AI

One of the most exciting prospects ahead of us involves applying quantum computing to AI. Firstly, many AI algorithms involve solving the types of problems that quantum computers excel at, such as optimization problems. Secondly, with its ability to more accurately simulate and model the physical world, it will generate huge amounts of synthetic data. This data will more closely resemble real-world data than existing synthetic data, down to the molecular or sub-atomic level, while also being far cheaper and easier to produce. Work is already ongoing to make this a reality – Quantinuum is focusing its efforts on developing the machine learning techniques needed for quantum-powered natural language processing. It's hard to put a timescale on this one as breakthroughs could occur any day, but I predict we can expect to see progress within five to 10 years.

Further Ahead

Looking beyond the next two decades, quantum computing will be changing the world in ways we can't even imagine yet, just as the leap to transistors and microchips enabled the digital world and the internet of today.

It will tackle currently impossible problems, help us create fantastic new materials with amazing properties and medicines that affect our bodies in new ways, and help us tackle huge problems like climate change and cleaning the oceans.

Key challenges, like the risk of exacerbating inequality if access is limited to the rich and the significant energy demands, will need to be addressed. But make no mistake, quantum computing is on its way, and its impact will be felt by us all. Those who don't want to risk missing out should start preparing for it now.

22.Quantum-resistant algorithms: Why they matter

by Michael Nadeau
https://www.techtarget.com/searchcio/tip/Quantum-resistant-algorithms-Why-they-matter

It's only a matter of time before quantum computers reach the point where they can break commonly used encryption algorithms such as RSA (Rivest-Shamir-Adleman), Diffie-Hellman, and AES (Advanced

Encryption Standard). We're entering the world of post-quantum cryptography, and the inevitable loss of protection for sensitive encrypted data now drives the development of new quantum-resistant algorithms.

Quantum-resistant algorithms offer new approaches using more complex mathematical problems that are not easily solved by quantum computers. Since no one knows how secure these new algorithms will be, multiple methods are available, should one or more be broken.

The importance of quantum-resistant algorithms

Cryptography algorithms currently in use are secure because computers need a long time to crack them -- possibly thousands of years. This is called *computational security*. With a quantum computer, that computational security goes away. A quantum computer with more than 4,000 stable quantum bits (qubits) would theoretically break Rivest-Shamir-Adleman (RSA) 2048 encryption in seconds.

No quantum computer today has more than a few dozen stable qubits, but predictions for when a cryptographically relevant quantum computer (CRQC) will arrive range from 2030 to 2035. That doesn't leave much time to prepare because it can take a large organization as much as 10 or more years to transition to a quantum-resistant algorithm.

Research in post-quantum cryptography (PQC) has been happening for years. In 1994, Peter Shor developed Shor's algorithm, the first quantum algorithm designed to break existing encryption algorithms. Since then, NIST has reviewed and certified four quantum-resistant algorithms, with a fifth pending to counter Shor's and other quantum algorithms.

"A realistic, near-term threat of quantum computing is its ability to break widely used public key cryptography systems, which jeopardizes the security and privacy of digital communications," said Nelly Porter, director of product management for confidential computing and encryption, Google Cloud.

Quantum computing also threatens the integrity of digital signatures, which verify the origin of a digital message or document and ensure that it hasn't been tampered with.

"This is crucial for establishing trust in digital communications," Porter said. "We have to ensure that we are preventing the forgery of digital signatures, especially for long-term firmware and software updates."

How do quantum-resistant algorithms work?

Today's encryption algorithms are based on creating private keys of two or more large prime numbers that are then multiplied together. The result becomes part of a public key that someone can use to encrypt a message they send to another person. The recipient can then decrypt the message using the original prime numbers. A quantum computer, however, can quickly calculate the private key from the public key.

RSA and other encryption algorithms have used progressively larger prime numbers to maintain computational security. That won't work when an adversary has a quantum computer, so the following alternative PQC methods are needed.

Lattice-based cryptography

LBC relies on complex mathematical problems using lattices -- think of an infinite grid of intersecting lines in multiple dimensions. The security of LBC depends on identifying specific points on this grid. One set of points could represent a private key while another is the public key. Deriving those key pairs would be relatively easy to do with only a few dimensions, so LBC would need hundreds of dimensions to stay ahead of the capabilities of a quantum computer.

Hash-based cryptography

Hash-based cryptography uses an algorithm called a *hash function* to convert a key, which can be any data, into a unique hash value. That hash value is a fixed-length string of alphanumeric characters called a *digest*. Hash-based one-time signature (OTS) schemes use a key pair only once to sign a message; otherwise, the OTS key pair is vulnerable to signature forgery

Code-based cryptography

Code-based cryptography relies on cryptographic systems that use error-correcting codes. The process creates a public key by mathematically creating an altered version of the private key -- essentially introducing errors. Those errors can be decoded only by the recipient. Code-based cryptography is considered particularly resistant to compromise by quantum computers.

Examples of quantum-resistant algorithms

NIST has released the following four PQC encryption standards. Some are general encryption standards, while others encrypt digital signatures.

1. **Federal Information Processing Standard (FIPS) 203** is the primary general encryption standard. It was selected partly for its relatively small encryption keys, which can be more easily exchanged, and its operating speed. FIPS 203 is a lattice-based algorithm based on the CRYSTALS-Kyber algorithm, now known as the Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM).

2. **FIPS 204** is the primary standard for protecting digital signatures and is also lattice-based. It uses the CRYSTALS-Dilithium algorithm, now known as the Module-Lattice-Based Digital Signature Algorithm (ML-DSA).

3. **FIPS 205**, also designed for digital signatures, is derived from the hash-based Sphincs+ algorithm, now known as the Stateless Hash-Based Digital Signature Algorithm (SLH-DSA). NIST intends FIPS 205 as a backup to FIPS 204.

4. **FIPS 206** is derived from the FALCON lattice-based algorithm. It is now referred to as FN-DSA, which stands for Fast-Fourier Transform over NTRU-Lattice-Based Digital Signature Algorithm. FIPS 206 is also intended for use with digital signatures.

The **Hamming Quasi-Cyclic (HQC) algorithm**, which has not been finalized, is intended as a general encryption standard to back up FIPS 203, should it become compromised. Like FIPS 203, HQC uses a key encapsulation method to create a shared secret key sent over public channels. However, HQC uses code-based cryptography, which offers high security but requires more computational overhead.

Some vendors have begun adopting NIST PQC standards into their products. For example, Google Cloud's Cloud KMS offers quantum-safe digital signatures employing FIPS 203, 204 and 205 using its API.

Challenges of developing quantum-resistant algorithms

The biggest and most obvious challenge of developing quantum-resistant algorithms is what researchers don't yet know. How capable will the first CRQC systems be, and how fast will they evolve? How far along are adversaries like China and Russia in their efforts to find vulnerabilities in quantum-resistant algorithms? This uncertainty is the reason NIST is certifying backup PQC encryption standards.

Quantum-resistant algorithms are likely to fail over time, said John Prisco, CEO of consultancy Safe Quantum. "No one knows if the Chinese have already broken the CRYSTALS lattice algorithms of NIST." Prisco recommends addressing such risks with a "defense in depth" approach using quantum science and mathematical algorithms.

What does the future hold for quantum-resistant development?

The primary goal of quantum-resistant development is diversity. Since none of the proposed algorithms can yet be tested in a CRQC environment, multiple options are needed should some become compromised. In the meantime, improvements will be made to existing PQC algorithms.

"Researchers will continue to work on post-quantum cryptography algorithms to make them more efficient, with smaller key sizes and faster computational speeds," Porter said. "This is particularly important for devices with limited resources."

Porter and others agree that quantum-resistant algorithms will do the following:

- Become more diverse, with some serving general-purpose encryption needs and others tailored to specific applications.
- Use more complex mathematical problems to develop stronger quantum-resistant algorithms.
- Integrate into current encryption practices, software, hardware and communication protocols.
- Combine with classical encryption algorithms to create hybrid cryptographic systems for greater security.

Prisco believes the best way to protect sensitive data in a PQC world is to combine quantum-resistant algorithms with quantum key distribution. QKD allows two parties to produce a shared random secret key that can then be used with a quantum-resistant algorithm to send encrypted messages securely. China is making a heavy investment in QKD, he said. "Like a Sputnik moment, that should wake up our U.S. quantum community to match the level of investment in QKD as well as PQC.

"Defense in depth is necessary to compete with today's security protection schemes," Prisco continued. "Information-theoretic is defined as an encryption technique that cannot be broken, given infinite time and infinite compute power to attempt a break. QKD is already information-theoretic and should be under increased deployment and development in the U.S.," he said.

However, QKD has a few drawbacks. It is relatively expensive, requires special equipment and dark fiber, and has distance limitations. IBM, which invented the QKD protocol BB84, is not doing much with it commercially. "QKD is good at solving certain types of problems, whereas post-quantum cryptography is a broad-based solution," said Ray Harishankar, IBM Fellow and lead for IBM Quantum Safe.

Quantum-resistant algorithms will go beyond corporate and government networks into devices businesses and consumers use. A particular quantum-resistant algorithm might not perform well in some of these devices.

"We have to look at alternates if you're looking at a smaller form factor, an ATM machine, an IoT device, something embedded in a car," Harishankar said. "There are so many places where encryption occurs. You may have medical devices that are encrypting information. There are so many scenarios where you will need different algorithms with different form factors. We'll find ways to improve the performance of existing algorithms, or we'll find newer algorithms that are more performant in the target device."

23. OpenSSH 10.0 Released to Better Fend off Attacks by Quantum Computers

by Michael Larabel
https://www.phoronix.com/news/OpenSSH-10.0-Released

OpenSSH 10.0 is now available for this widely-used SSH client/server implementation. There are a number of changes to find with OpenSSH 10.0 including better protections against possible attacks by future quantum computers.

OpenSSH 10.0 drops support for the weak DSA signature algorithm that had been deprecated already for the past decade. The SSH daemon (SSHD) also removes code responsible for the user-authentication phase of the protocol to a new "sshd-auth" binary to better segregate the pre-authentication attack surface.

OpenSSH 10.0 on the security side also fixes the "DisableForwarding" for X11 forwarding as it turns out it was failing to disable X11 forwarding and agent forwarding as documented.

For better protections in a quantum computing world, OpenSSH 10.0 now uses the hybrid post-quantum algorithm mlkem768x25519-sha256 by default for key agreement. The mlkem768x25519-sha256 algorithm is currently deemed safe against possible attacks by quantum computers and is considered faster than the prior default.

OpenSSH 10.0 also adds a work-in-progress tool for verifying FIDO attestation blobs. The experimental tool in OpenSSH 10.0 can be found under *regress/misc/ssh-verify-attestation* for experimenting but not installed by default.

24. Special delivery no longer needed for COMSEC keys

by Kathryn Bailey
https://www.army.mil/article/284517/special_delivery_no_longer_needed_for_comsec_keys

One Combatant Command now has a streamlined process for delivering cryptographic keys to remote sites across Latin America.

The U.S., its allies and partners use cryptographic keys to safeguard against unauthorized access to classified information. The keys were traditionally delivered using slower, more cumbersome key delivery methods – often loaded onto key fill devices and hand-delivered to Army Communications Security (COMSEC) personnel across all areas of operation.

To implement a more logistically friendly process, U.S. Southern Command (SOUTHCOM) requested assistance from Army COMSEC and crypto modernization personnel to activate Key Management Infrastructure (KMI)-aware features on a variety of their encryption devices around the world.

KMI is a National Security Agency (NSA)-led program responsible for all COMSEC key management and distribution. It supports Combatant Commands, Joint Services, DoD agencies, Federal agencies and coalition partners and allies.

"The Army will be upgrading a major portion of its network encryptors over the next two to five years, as part of the DoD's crypto modernization effort," said Brian Finley, assistant program manager for KMI within Product Manager COMSEC, assigned to Program Executive Office Command, Control, Communications, and Network (PEO C3N).

The biggest advantage to operating KMI-aware devices is increased key distribution options combined with enhanced security without the need of a fill device. Receiving keys directly from the KMI web-based storefront, hosted by the NSA, eliminates the risk of key exposure while in the field.

"When fully implemented, KMI-aware devices will drastically reduce the need for legacy key delivery methods, which will also reduce travel costs and risk to personnel – especially for those traveling to remote and sometimes unstable military or political locations," Finley said.

SOUTHCOM is the first major command the Army has enabled with KMI-aware over-the-network key capabilities, and the pilot effort showcased both increased security while reducing complexity and costs to the DoD.

The hands-on support provided by the COMSEC and the Cryptographic team included registering and initializing new KMI-aware High Assurance Internet Protocol Encryptor (HAIPE) devices, which adhere to the strictest cyber security standards and use advanced encryption techniques to safeguard sensitive data transmitted over networks.

“It's incredibly rewarding to see the KMI-aware features move from the lab to the operational environment in SOUTHCOM,” said Jennifer (Jenney) Mills, Key Management Group lead from Army Combat Capabilities Development Command (DEVCOM) C5ISR Center.

“My group dedicated the last few years diligently testing and reporting challenges to NSA, ensuring the seamless integration of KMI-aware devices.”

The technology will significantly contribute to cost savings, reduce logistical burdens, and most importantly, enhance the safety of our Soldiers and personnel, she said.

Once provisioned with the KMI storefront, SOUTHCOM COMSEC personnel shipped the devices to their remote locations. Authorized recipients can now access the storefront to retrieve cryptographic products specifically destined for their individual account and device.

Besides providing direct, safe access to crypto keys, KMI provides network management features and access to other cryptographic products, providing the user and account manager the flexibility to provide the most secure, most up-to-date network components.

“With national security refocusing on near-peer adversaries, the stakes continue to climb for those charged with protecting unauthorized access to classified communications,” Finley said. “These enhanced crypto mod products and processes are placing the Army’s most sensitive information in good hands.”

25. This More Than 380-Year-Old Trick Can Crack Some Modern Encryption

by Manon Bischoff
https://www.scientificamerican.com/article/this-more-than-380-year-old-trick-can-crack-some-modern-encryption/

Hardly anyone is interested in my tax return—there’s not much to it. And that’s a good thing, given that an attacker might have fairly easily intercepted the encrypted communication between my laptop and printer when I printed the return in recent years.

In early 2022 information technology security researcher Hanno Böck discovered that some of these encryptions could be cracked in a process that he went on to describe in a 2023 preprint paperposted to the International Association for Cryptologic Research’s Cryptology ePrint Archive. His method can be traced back to one developed by the French scholar Pierre de Fermat in the 17th century.

Fermat—most famous for his mysterious “last theorem,” which vexed experts for decades—contributed all kinds of useful things to the world of science in his lifetime. For example, he laid the foundations for the theory of probability and also worked a lot on prime numbers—those values that are only divisible by 1 and themselves.

Mathematicians suspected they could use Fermat’s work to break encryption—and Böck demonstrated that case.

Complex Problems for Security

Modern encryption systems are based on difficult math problems. They work like a padlock: the problem (the lock) cannot be solved without additional information (the key). A common procedure is so-called RSA cryptography, which is related to prime numbers. Decomposing large numbers into a product of prime numbers is difficult, making them useful keys.

Prime numbers are often referred to as the atoms of number theory—indivisible building blocks from which the natural numbers are constructed. Any other number can be written as a unique product of primes, for example 15 = 3 × 5 or 20 = 2 × 2 × 5. For small values, it is easy to determine the prime divisors. But what about, say, 7,327,328,314? So far, no computer program can quickly calculate the prime divisors of arbitrarily large numbers.

This limitation is precisely what RSA cryptography exploits. To understand how that kind of protocol works, consider a simplified example, where RSA is used to encrypt data with the help of large numbers. Suppose a person wants to send the word SCIENCE, which consists of seven letters, to a recipient in encrypted form. To do this, they use a large seven-digit number such as 6,743,214 and shift each letter of SCIENCE by the respective digit—so S shifts six letters over to become Y, C shifts seven letters to become J, and so on. The end result is the encrypted word CJMHPDI. A sender can now dispatch this to another person without a listener being able to decode the message.

The recipient, however, should be able to determine the original word SCIENCE, either with the key itself (6,743,214) or a clue for calculating the key. As the former always carries a risk—an attacker could eavesdrop on the communication between the two parties and thus intercept the key—RSA cryptography offers a way of reconstructing the key securely. The basic idea is that before sending the secret message, the sender and receiver jointly generate a key from publicly available information. Security is guaranteed by the fact that the sender and recipient each secretly use large prime numbers, which they multiply together, and only send each other the results of this calculation. An eavesdropper needs the prime numbers to generate the key. But because that person can only intercept the products and cannot factorize them, the eavesdropper is helpless. (The actual RSA protocol for the key generation is a bit more complicated, but that is the general idea behind it).

Fermat Factorization

Nearly four centuries ago, Fermat was working on related problems. He wanted to know how to factorize numbers into their prime number components. He did this purely out of mathematical curiosity—at the time, no cryptographic methods for secure key exchange were known.

And indeed, Fermat found a way to factorize even large numbers that are the product of two prime numbers. His method is not complicated; you can do it with a calculator (though Fermat, incidentally, did not have one). To impress his contemporaries, Fermat demonstrated the method using the example number *n* = 2,027,651,281.

Fermat factorization works as follows: You take the number *n,* in this case 2,027,651,281, and take the root of it. As a rule, this will result in an odd value, as is the case here: √2,027,651,281 ≈ 45,029.45. You round up to get 45,030. This number is squared, and the original value *n* is subtracted from the result: 45,030^2 –

2,027,651,281 = 49,619. Now you have to check whether the result is a square number. As it happens, 49,619 is not square.

So you continue. Start again with the rounded root 45,030, add 1 and then square the result in order to subtract the original value *n* from it—that is, 45,031^2 – 2,027,651,281 = 139,680—and check again whether the result is a square number. Once more, this is not the case.

So you repeat the whole thing. This time you add 2 to 45,030 and square the result, from which you subtract the original value *n:* 45,032^2 – 2,027,651,281 = 229,743. Again, this is not a square number.

Fermat must have had a lot of patience. In his example, you have to carry out the procedure a total of 12 times until you find a square number: 45,041^2 – 2,027,651,281 = 1,040,400 = 1,020^2.

And how does this help? In the above equation, a squared number *y*^2 (in this case 45,041^2) minus *n* equals another squared number *x*^2 (in this case, 10,20^2). The equation *y*^2 – *n* = *x*^2 can be rearranged as *y*^2 – *x*^2 = *n*. The left-hand side corresponds to an equation known as the third binomial formula, (*y* – *x*)·(*y* + *x*) = *n*. This automatically factorizes the number *n* into two numbers *y* – *x* and *y* + *x*. For the example with *n* = 2,027,651,281, the two factors are therefore 45,041 – 1,020 = 44,021 and 45,041 + 1,020 = 46,061. Both are prime numbers.

Attacking the Printer

In fact, this factorization method always works for odd *n*. But computers can only perform it fast enough if the two prime factors of *n* are not too far apart. And this was precisely the problem that Böck discovered in a program library used by various companies at the time. The prime numbers generated for encryption were not random enough, and the program often selected two prime numbers that were close to each other. This means that Fermat's factorization method can be used to circumvent the encryption.

Böck realized that the printers of certain companies used such inadequate encryption. They used RSA cryptography, for example, to protect confidential documents that were sent to the printer via a network.

After his finding in 2022, these companies issued alerts and fixes to address the problem. We can only hope that other companies have closed such security gaps.

In any case, many companies will have to rethink their encryption standards in the coming years. Even if ordinary computers fail to factorize large numbers, it will be different with powerful quantum computers. Fermat would never have dreamed that more than 380 years after his discovery, computers that rely on complicated principles of quantum mechanics for their calculations might make use of it.

26. AWS introduces post-quantum security with ML-KEM for TLS connections

by Mels Dees
https://www.techzine.eu/news/security/130431/aws-introduces-post-quantum-security-with-ml-kem-for-tls-connections/

ML-KEM (Module-Lattice-based Key Encapsulation Mechanism) is a post-quantum cryptographic algorithm designed to exchange keys in a way that is resistant to the expected—but still theoretical—threat of quantum computers. ML-KEM can then theoretically break traditional encryption, such as RSA.

The mechanism is based on CRYSTALS-Kyber. The American National Institute of Standards and Technology (NIST) chose it as the basis for its post-quantum cryptography standard. The final version of this standard will be announced in August 2024.

Harvest now, decrypt later attacks

Although quantum computers do not currently pose an active threat to cryptography, implementing quantum-safe algorithms is seen as a way to prevent future exposure to so-called harvest now, decrypt later attacks.

AWS indicated that it has chosen to secure the most critical services first: KMS, ACM, and Secrets Manager. These services already supported CRYSTALS-Kyber, which will be phased out in 2026.

AWS selected these three services because they are among the most security-critical AWS services, for which post-quantum confidentiality is most urgent. AWS stated that these three services had previously rolled out support for CRYSTALS-Kyber, the predecessor of ML-KEM. The company also stated that support for CRYSTALS-Kyber will continue until the end of 2025 but will be replaced by ML-KEM in all AWS services in 2026.

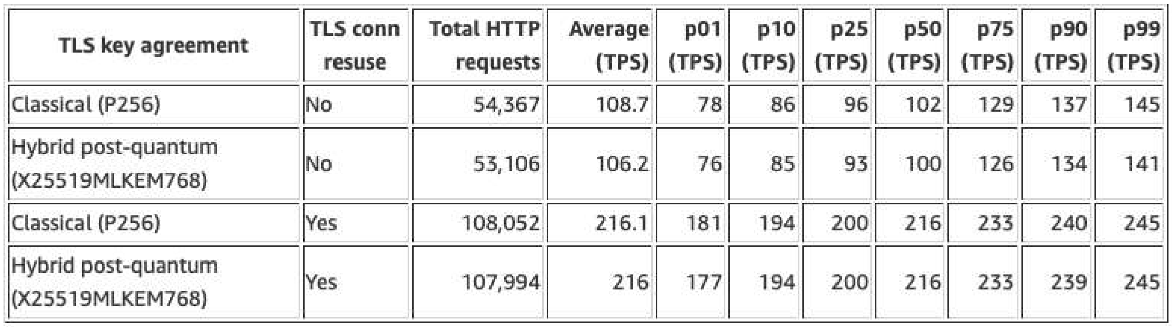
Instructions for enabling ML-KEM

Users must update their client SDKs and explicitly enable the feature to activate ML-KEM post-quantum TLS when using AWS services such as KMS, ACM, or Secrets Manager. AWS offers instructions for enabling ML-KEM for both the SDK for Java (from version 2.30.22) and the SDK for Rust.

The company also advises administrators to perform performance tests, benchmarks and connectivity tests within their environment to verify compatibility and performance.

AWS' own performance tests show that enabling ML-KEM hybrid post-quantum TLS has hardly any impact on performance, not even in the least favorable scenarios. When reusing TLS connections—the default setting in the SDKs—the performance loss is virtually nil. The decrease is then 0.05%. Without reuse, the performance decrease is approximately 2.3%. This is due to the additional 1,600 bytes that ML-KEM adds to the TLS handshake. This requires between 80 and 150 microseconds of additional computing time per connection.

In summary, enabling ML-KEM results in only a minimal performance loss for almost all applications. AWS recommends that users take advantage of this new security feature as soon as possible.



TLS key agreement	TLS conn resuse	Total HTTP requests	Average (TPS)	p01 (TPS)	p10 (TPS)	p25 (TPS)	p50 (TPS)	p75 (TPS)	p90 (TPS)	p99 (TPS)
Classical (P256)	No	54,367	108.7	78	86	96	102	129	137	145
Hybrid post-quantum (X25519MLKEM768)	No	53,106	106.2	76	85	93	100	126	134	141
Classical (P256)	Yes	108,052	216.1	181	194	200	216	233	240	245
Hybrid post-quantum (X25519MLKEM768)	Yes	107,994	216	177	194	200	216	233	239	245

27. Back to the future with block sizes

by Professor Nigel Smart
https://www.techradar.com/pro/back-to-the-future-with-block-sizes

The American NIST is rather busy on the cryptographic front these days. Not only has it been busy in the area of Post-Quantum Cryptography (PQC), it is also in the process of standardizing the lightweight cipher Ascon, and it is also embarking soon on a major effort to examine threshold cryptography, but in late 2024 it announced that it would be looking at standardizing a larger block size variant of the AES algorithm.

To understand what this proposal is, and why it is important, we need to dig a bit deeper into what a block cipher is, and the history of the AES algorithm.

Block ciphers explained

A block cipher is a mechanism to encrypt single blocks of data using a secret key. The two important characteristics of a block cipher are the number of bits needed to determine the key (the so-called key size) and the size of the data which each application of the block cipher encrypts (the co-called block size).

Children often encounter block ciphers as a first introduction to cryptography by making a table of letters, and then placing a random permutation of the letters underneath them such as

A - B - C - D - E - F - G - H - I - J - K - L - M
T - M- A - H - X - S - C - Q - N - R - P - D -E

So the word BAD would encrypt to the ciphertext MTH. In this example the key is the second row of the table (you need the second row to encrypt and decrypt). This gives a total number of keys of 26 · 25 · 24 ⋯ 3 · 2 · 1 ≈ 2^88.3 which corresponds to a key size of 88.3 bits. The block size is however only one letter, i.e. something which can be represented in bits. This key size is quite large, if I just gave you an encrypted message of three letters it would be hard to determine the key.

However, because the block size is small it is easy to break in practice, since a large encrypted text will reveal repeats of plaintext blocks. For example the words "HIDE ME" will encrypt to "QNHX EX", and we can see the repetition of X encrypting E. As we know E is the most likely letter in English this means it is likely that the attacker can guess X encrypts E.

Even if we were encrypting random messages (and not English) this repetition of blocks is a way for an attacker to attack any system which uses the block cipher. Due to the birthday paradox, if we have a block size of b bits, then we expect such a collision to occur after a few blocks. For the case of our toy cipher this means, for a random message, we expect a collision to occur after about 5 blocks.

AES

AES is a block cipher, which is the workhorse of almost all cryptographic systems in the world today. It was standardized by NIST in 2001, and has a variable key size of 128, 192 and 256 bits, but a fixed block size of 128 bits. This fixing of the block size was not originally on the cards.

In the original preliminary call for AES, NIST proposed having 128, 192 and 256 bit key sizes, with a fixed block size of 128-bits, but with the option for other block sizes.

However, as the process to choose AES progressed, in the official first call in 1997 NIST decided to focus only on 128 bit block sizes. In 2001 this block size seemed alright. After all, it means that for a random message we only expect output blocks to be identical after ciphertext blocks, or 256 Exabytes.

The problem is that this "seemed alright" was not quite true. AES was actually based on an algorithm called Rijndael (invented by two Belgian mathematicians called Joan Daemen and Vincent Rijmen). In its original design, submitted to NIST, Rijndael had three possible key sizes (128, 192 and 256 bits) and three possible block sizes (128, 192 and 256 bits).

As we just remarked, during the AES process, in order to simplify the competition, NIST decided that it would only focus on 128-bit block sizes. Thus the original Rijndael design was modified to only allow one block size.

Unfortunate consequences

The fact that collisions happen more likely with a smaller block size means that applications needed to limit the number of blocks they could encrypt. This means that we only use a single 128-bit key to encrypt a relatively small amount of data. In practice this limit on the amount one can encrypt with one key becomes blocks, or only 64 Gigabytes (which is less than most harddisks in a laptop these days) , when AES is used in its most popular scenario (called AES-GCM mode). Meaning we need to rekey our ciphers more often, or use another method of calling AES.

Due to AES being super fast in hardware it would be good if we could use AES to construct a hash function (which are very slow normally). One can use block ciphers to construct hash functions, but they are not very secure (or are more complex to construct) unless the block cipher has a big block size (such as 256 bits).

The mismatch between block size and key size for the AES algorithm led to a theoretical "attack" (in a very special situation) on the AES algorithm with 256 bit key size in 2009 due to Biryukov and Khovratovich. Thus AES-256, with its 128-bit block size, was not as good as one would expect. On the other hand using Rijndael with 256-bit key and 256- bit block size would have avoided this "attack".

Summary

Thus what NIST has announced is to revisit, what in hindsight, was the mistake it made back in 2001. AES should really have been standardized with a 256 bit block size variant.

If cryptographers had a DeLorean time machine they would go back about twenty five years, and modify the AES competition so that the final decision would have allowed AES to be used with a 256-bit block size.

28. Quantum Security: Chromebook Security and the Digital Trust of Tomorrow

by Dominic Reigns
https://www.aboutchromebooks.com/blog/chromebook-security-and-the-digital-trust-of-tomorrow/

Traditional encryption techniques struggle more as cyberattacks get increasingly complex. Ensuring data integrity against even the most sophisticated cyber attacks, quantum security is the next frontier in digital defense.

Known for its cloud-based security approach and built-in protections, Chromebooks are now leading the way in incorporating quantum-resistant features.

Encryption techniques that safeguard user data now could become outdated with quantum computing in the future. Employing advanced cryptographic techniques, quantum security technologies promise resistance against future attacks.

Rise of Quantum Computing: Why Security Must Evolve

By tackling difficult issues tenfold quicker than traditional computers, quantum computing is poised to transform sectors. However, the study also suggests that conventional encryption methods like RSA and AES may become vulnerable.

Renowned for their security-focused design, Chromebooks are investigating quantum-resistant encryption to prepare for this change.

Aiming to create encryption algorithms that even quantum computers cannot readily crack, post-quantum cryptography (PQC) indicates a proactive attitude to the next cybersecurity concerns. Google has already started testing quantum-resistant encryption in Google Chrome.

With their automated upgrades and sandboxing capabilities, Chromebooks are the perfect platform for combining these developing security solutions. Quantum-safe encryption will help Chromebooks continue providing robust threat prevention and guarantee digital confidence for users.

Chromebook Security: A Solid Foundation for Future Innovations

Chromebooks have always been built with security in mind. From certified boot processes to automated upgrades and sandboxing, they provide multi-layered security against cyber attacks. As quantum security develops, Chromebooks are ideally suited to include these new technologies.

Google's security system has continual background updates that prevent vulnerabilities, end-to-end encryption, and TPM (Trusted Platform Module) chips. These current protections provide Chromebooks with a favorable starting point for the next stage of digital defense—quantum-resistant security.

Google is aggressively working on improving Chrome OS with quantum-safe encryption methods, guaranteeing that Chromebook users stay safe from future cyber hazards as quantum dangers arise.

ChromeOS's Quantum-Safe Initiative

Aiming to protect its goods against developing cyber hazards. Google has been leading quantum security research. As part of its quantum-safe project, the firm has been testing and implementing post-quantum cryptography techniques to protect user data across its platforms, including ChromeOS.

One of the main developments in this project is the inclusion of hybrid encryption models. These models guarantee data stays safe even throughout the move to complete post-quantum cryptography by combining quantum-resistant strategies with traditional cryptographic approaches.

By progressively using these hybrid solutions, Google is making sure ChromeOS is robust against both present and future security concerns.

Google has also been working with worldwide cybersecurity experts to find and reduce weaknesses quantum computing may use. These initiatives seek to guarantee that ChromeOS users gain from state-of-the-art security measures long before quantum computers become commercially accessible.

Google's quantum-safe project is clearing the path for a safer, more robust digital environment through future-proof security. By including quantum-resistant encryption in ChromeOS, Google is establishing a new benchmark for cloud-based computer security.

Improving Chromebook Data Security with Quantum Key Distribution

Quantum Key Distribution (QKD) is an emerging technology that has the potential to transform the provision of secure communications in a post-quantum world. Contrary to conventional encryption based on mathematical intractability, QKD relies on principles of quantum mechanics for secure key distribution and generation.

One key benefit of QKD is that it can monitor eavesdropping in real time. A hacker stealing a quantum key alters the quantum state of particles, causing the receiver and sender to realize it immediately. This intrinsic security feature protects confidential information.

By including quantum-safe encryption with conventional security elements, ChromeOS may keep its standing as one of the most secure operating systems available.

In an increasingly digital world, where sensitive transactions and personal data are exchanged across various platforms, from online banking to e-commerce and even online casinos, robust security is paramount.

Chrome OS's Next Quantum Security Step

Quantum security in Chromebook protection will become more crucial as quantum computing develops—Google's continuous dedication to incorporating quantum-resistant cryptographic techniques into ChromeOS guarantees that customers will gain unmatched security.

Secure, forward-looking solutions will shape digital trust in the future. Chromebooks will stay at the forefront of safe cloud-based computing by including post-quantum cryptography, hybrid encryption models, and new technologies, including quantum key distribution.

Advancements in AI-driven security measures, quantum-proof authentication techniques, and real-time threat detection will strengthen Chromebook security even more in the following years. As cyber threats evolve into more advanced ones, a strong security system will be essential for protecting sensitive user information.

ChromeOS is uniquely poised to lead the charge on quantum-resistant computing with its cloud-first architecture, auto-updating, and active security. Quantum security and the techniques employed to provide a reliable and safe digital experience for Chromebook users worldwide will change.

29.DARPA backs multiple quantum paths in benchmarking initiative

by Maria Korolov
https://www.networkworld.com/article/3956149/darpa-backs-multiple-quantum-paths-in-benchmarking-initiative.html?utm_date=20250408132025&utm_campaign=Network%20World%20US%20First%20Look&utm_content=slotno-1-readmore-&utm_term=Networkworld%20US%20Editorial%20Newsletters&utm_medium=email&utm_source=Adestra&huid=ade0ec26-70d6-4372-b394-860dfbb7e8b5

The Defense Advanced Research Projects Agency has selected 15 quantum computing companies for its Quantum Benchmarking Initiative, to see if utility-scale quantum computers can be built by 2033.

Selected companies include IBM, HPE, Quantinuum, IonQ, Xanadu, Rigetti, and others from North America, Europe, and Australia and covers multiple approaches to quantum computing, including trapped ions, superconducting qubits, photonics, and silicon spin qubits.

"It's an honor to be selected to the first phase of QBI along with other leaders in the industry," says Xanadu founder and CEO Christian Weedbrook. "One of the challenges from a fundraising and business perspective is how can an investor or customer do due diligence on a quantum computing company." Programs like QBI provide that validation, he says.

"We're going to do whatever we can to show that these companies' plans won't work, but we're going to be honest brokers," says Joe Altepeter, QBI program manager at DARPA, in a video. "And if we find out that it does work after a lot of hard work, a lot of analysis, and a lot of independent testing, then we're going to tell the other agencies of the government who care about whether quantum computers work or not."

But it's not just validation the DARPA is offering. According to Nord Quantique, DARPA will provide substantial funding through the multi-stage initiative, with selected companies receiving $1 million to detail their quantum computing concepts – and that's just to start with.

Those advancing to the next stage could receive up to $15 million to develop comprehensive research and development roadmaps, followed by up to $300 million in the final stage, for building and demonstrating their utility-scale quantum systems.

Nord Quantique plans to use the money to expand its team, says Julien Camirand Lemyre, the company's president, CTO and co-founder. That's an opportunity to accelerate the development of the technology, he says.

"By extension, what this will mean for enterprise users is that quantum solutions to real-world business problems will be available sooner, due to that acceleration," he says. "And so enterprise customers need to also accelerate how they are thinking about adoption because the advantages quantum will provide will be tangible." Lemyre predicts that useful quantum computers will be available for enterprises before the end of the decade.

"In fact, there has been tremendous progress across the entire quantum sector in recent years," he says. "This means the industry needs to begin thinking seriously about how they will integrate quantum computing into their operations over the medium term."

"We're seeing, with the deployment of programs like the QBI in the US and investments of billions of dollars from public and private investors globally, an increasing maturity of quantum technologies," said Paul Terry, CEO at Photonic, Inc., which is betting on optically-linked silicon spin qubits. "Our architecture has been designed from day one to build modular, scalable, fault-tolerant quantum systems able to be deployed in data centers," he said.

He's not the only one to mention fault-tolerance. DARPA stressed fault-tolerance in its announcement, and its selections point to the importance of error correction for the future of quantum computing.

The biggest problem with today's quantum computers is that the number of errors increases faster than the number of qubits, making them impossible to scale up. Quantum companies are working on a variety of approaches to reduce the error rates low enough that quantum computers can get big enough to actually do real work.

Many of today's quantum computers are classified as noisy intermediate-scale quantum, or NISQ. They are useful for education, but won't lead to commercial value, said Juliette Peyronnet, US general manager at Alice & Bob, which makes fault-tolerant cat qubits. "The fact that DARPA is validating that we have to look at fault tolerance is another confirmation that this is where commercial enterprises should also focus," she says.

"Our roadmap is that by 2030 we'll have 100 logical qubits, and with 100 logical qubits, it's when you start scratching the tip of the iceberg in terms of creating value for very specific use cases," she said. "So we are not talking about full commercial interest, but starting to do things that are completely out of the realm of classical solutions."

The goal of the QBI is to select the quantum computing companies and technologies that have the best chance to succeed, says Xanadu's Weedbrook. "The fact that this program exists indicates that the quantum computing industry is maturing at an ever faster rate."

HPE is taking a consortium approach, partnering with six organizations including Qolab, Quantum Machines, and Applied Materials. The team is focusing on an approach combining quantum and classical computing.

"Working as a consortium, we came up with a less ambitious but more practical target of building high-performance quantum-classical coprocessors that could be met by employing state-of-the-art semiconductor fabrication and supercomputing," says Masoud Mohseni, an HPE Labs distinguished technologist, in a statement.

Full list of 15 companies DARPA selected:

- Alice & Bob – superconducting cat qubits.
- Atlantic Quantum – fluxonium qubits.
- Atom Computing – scalable arrays of neutral atoms.
- Diraq – silicon spin qubits.
- Hewlett Packard Enterprise.
- IBM – superconducting processors.
- IonQ – trapped-ion quantum computing.
- Nord Quantique.
- Oxford Ionics – trapped-ion qubits.
- Photonic-optically-linked silicon spin qubits.
- Quantinuum – trapped-ion qubits.
- Quantum Motion – silicon spin qubits.
- Rigetti Computing – superconducting tunable transmon qubits.
- Silicon Quantum Computing – precision atom qubits in silicon.
- Xanadu – photonic quantum computing.

There are also three other companies that have been selected, but not yet finalized, DARPA said, and their names will be released in the near future.

There is one big quantum computing player that's missing from the list – Microsoft. That's because Microsoft, as well as another quantum computing company, PsiQuantum, were already in the program. In fact, in February, DARPA announced that Microsoft and PsiQuantum had moved into the validation and co-design stage of the initiative, though the announcement didn't say how much money was involved.

30. China's Origin Wukong quantum computer becomes world's first to fine-tune billion-parameter AI model

by Zhu Lixin
https://www.chinadaily.com.cn/a/202504/07/WS67f3a2bba3104d9fd381df3e.html

A team of scientists and engineers in Hefei, Anhui province, recently used a quantum computer to fine-tune a billion-parameter AI model-marking a world-first achievement in AI and quantum computing integration, according to an announcement from the Anhui Quantum Computing Engineering Research Center on Monday (07 April 2025).

Fine-tuning involves training general large models (such as DeepSeek) on domain-specific data to optimize them for specialized applications—ranging from medical diagnosis to financial risk assessment. Traditional methods, like low-rank fine-tuning, often face performance bottlenecks and limited generalization capabilities.

Quantum computing, however, employs superposition and entanglement to explore vast parameter combinations simultaneously, according to Origin Quantum, the Hefei-based company behind this advancement. In other words, it is able to test many possible solutions at once to fine-tune AI models faster and more accurately.

Origin Quantum claimed that experimental results showed an 8.4% improvement in training effectiveness with a 76% reduction in the number of parameters.

The feat was accomplished using Origin Wukong, China's third-generation domestically developed superconducting quantum computer. The project was a collaboration between Origin Quantum, the Institute of Artificial Intelligence of the Hefei Comprehensive National Science Center and other partner institutions.

This breakthrough demonstrates quantum computing's feasibility for achieving lightweight large models (LLMs) and opens pathways to alleviate concerns over the "computing power anxiety" associated with large models, the company said.

Efficiently training and running large-scale AI models requires massive computing resources. As AI models grow in complexity and size, they need more computing power, memory and processing capabilities to function effectively.

"Our method is like equipping a classical large model with a 'quantum engine', enabling them to work together," said Dou Menghan, vice-president of Origin Quantum.

His team harnessed quantum computing to achieve intelligent fine-tuning, converting model weights into a hybrid of quantum neural networks and classical tensor networks.

Chen Zhaoyun, an associate research fellow at the Institute of Artificial Intelligence, said the breakthrough marks the first real-world large model task on quantum computing, demonstrating that existing hardware can preliminarily support large model fine-tuning.

Origin Wukong is powered by the Wukong chip, making it China's most advanced programmable and deliverable superconducting quantum computer. It can process hundreds of parallel quantum tasks for any given data set.

The Wukong chip comprises 72 computational qubits and 126 coupler qubits. Its name comes from the mythical Chinese character Sun Wukong, aka the Monkey King, who could assume 72 different forms. In this context, the name symbolizes the power and versatility of quantum computing.

A qubit (quantum bit) is the fundamental unit of quantum information, functioning similarly to a classical binary bit but capable of existing in multiple states simultaneously.

Since its launch last year, Origin Wukong has completed approximately 350,000 quantum computing tasks for users from 139 countries, covering diverse industries such as fluid dynamics, finance and biomedicine, according to Origin Quantum.

These tasks include the world's largest-scale quantum computing fluid dynamics simulation and integrating with the financial quantum cloud experimental platform to explore more efficient problem-solving solutions in the financial domain.

31. 9 steps to take to prepare for a quantum future

by Maria Korolov
https://www.networkworld.com/article/3954617/9-steps-to-take-to-prepare-for-a-quantum-future.html

Over the past year, vendor after vendor has reached the critical quantum-computing milestone where adding more qubits no longer adds a disproportionately higher amount of errors.

“For the first time, we can confidently say, the ‘zero to one’ moment has happened, and now we can look at scaling roadmaps instead of science roadmaps,” says Pranav Gokhale, vice president of quantum software at Infleqtion, which is focusing on the neutral atom approach to quantum computing.

It is similar to how fusion power reactors have been able to produce more energy than they use. Or the way a rocket hits escape velocity, says Gokhale. Infleqtion itself hit escape velocity this past December, he says, when its collaboration with Nvidia resulted in a six-fold improvement in accuracy.

Other companies that have recently hit escape velocity include Microsoft, Google, and QuEra, he says. (Read more: 10 quantum computing milestones of 2024)

For some companies, quantum computing is already here. Among 770 quantum computing researchers and professionals, 56% say that they’re already using quantum computing in their organization, according to a QuEra survey released in January. Of those, more than 80% say that they’re using it for scientific research and development, but another 50% are working on proof of concept or pilot projects. In addition, 10% are using quantum computing operationally, though without positive ROI – and 4% are already reporting positive ROI.

Typically, the way this works is that companies combine quantum computing with traditional high-performance computing and AI, so that the quantum computers – which are still tiny – tackle just the small, key components of a bigger puzzle that only they can handle.

HorizonX Consulting and The Quantum Insider, a market intelligence firm, launched the Quantum Innovation Index in February, ranking enterprises on the degree to which they've adopted quantum computing. In the automotive sector, for example, BMW, Volkwagen, and Toyota are taking the lead. In finance, JPMorgan, HSBC and Goldman Sachs are the furthest along in quantum proofs of concept.

On the quantum computing vendor side, 39% expect their customers to be using quantum computers in production in 2026, according to an Omdia survey released in October. In addition, 14% expect their technology to be ready for production use in 2025 – and 4% said it was ready in 2024.

"A quantum computer is not simply a faster classical computer, just like a plane is not just a faster car. With a plane you can fly over the ocean. What are you going to do if you have flying abilities?" – Sridhar Tayur, Carnegie Mellon University's Tepper School of Business.

Another sign that quantum computing is about to make a big impact on the world? In October, Chinese researchers used D-Wave's quantum annealing computer to break RSA.

Before everyone panics, this was just a 22-bit key, not the 2048-bit keys commonly used in RSA encryption today, so it was more of a proof of concept than a quantum apocalypse. Still, Gartner predicts that, by 2029, most conventional asymmetric cryptography won't be safe to use. In fact, quantum computing will force organizations to delete the majority of personal data rather than risk exposure, the research firm says.

But you don't have to wait until 2029 for quantum decryption to be a threat because of "harvest now, decrypt later" attacks. Adversaries that can afford storage costs can vacuum up encrypted communications or data sets right now.

"The technology doesn't exist to decrypt the data today," says Doug Saylors, partner at ISG Research. "But they might be exfiltrating the data today and they can archive data streams… and they could potentially decrypt it later."

1. Take cryptographic inventory

To get ahead of the quantum cryptography threat, companies should immediately start assessing their environment.

"What we're advising clients to do – and working on with clients today – is first go and inventory your encryption algorithms and know what you're using," says Saylors. That can be tricky, he adds.

For example, asymmetric encryption – such as the public key exchange methods used to safeguard online communications – are most vulnerable to quantum decryption.

“But because of the way cryptography works, most organizations don’t know if, say, their Oracle databases are using symmetric or asymmetric encryption,” he says. “They don’t know what their Apache servers are doing.”

In addition, most encryption is layered, and includes both symmetric and asymmetric parts. A single credit card transaction could have 37 points of encryption, he says. “That’s a large number of touchpoints that most people don’t know exist – not even the IT professionals we talk to.”

2. Prioritize

Because of the complexity of the tasks, ISG’s Saylors suggest that enterprises prioritize their efforts. The first step, he says, is to look at perimeter security. The second step is to look at the encryption around the most critical assets. And the third step is to look at the encryption around data backups.

All of this needs to happen as soon as possible. In fact, according to Gartner, enterprises should have created a cryptography database by the end of 2024. Companies should have created cryptography policies and planned their transition to post-quantum encryption by the end of 2024, the research firm says.

“You should start today,” says Gartner analyst Mark Horvath. “It’s going to take longer than you think.”

All of today’s encryption will need to be replaced over the next five to seven years, Horvath says. “It seems easy to do but it’s actually catastrophic.”

3. Pursue cryptographic agility

Once companies have figured out which assets and communications they need to protect first, how do they actually go about switching to quantum-safe cryptography?

NIST released four algorithms in 2024, and more are expected to arrive soon. But enterprises shouldn’t just pick one of these algorithms and swap out all their old encryption.

First, the new algorithms aren’t a simple replacement for the old ones, says Gartner’s Horvath. “They don’t perform the same as the old ones do. Key generation times are different. Key sizes are different.”

So everything will have to be carefully tested and some cryptographic processes may need to be rearchitected. But the bigger problem is that the new algorithms might themselves be deprecated as technology continues to evolve.

Instead, Horvath and other experts recommend that enterprises pursue quantum agility. If any cryptography is hard-coded into processes, it needs to be separated out. “Make it so that any cryptography can work in there,” he says. “You don’t want to be dependent on any specific implementation.”

And a company might use different cryptography based on levels of risk, or based on whether partners and customers and platforms support particular standards. After all, not everyone will move forward with quantum-safe encryption at the same pace or with the same set of algorithms.

According to Gartner, companies should have started on their crypto agility police by the of 2024, start implementing it in 2024 and 2025, and have it in production by the end of 2027.

And, by 2027, companies should begin phasing out applications that can't be upgraded to crypto agility and begin enforcing strong, safe cryptography for all data. One particular area that enterprises should pay attention to is IoT devices, says Aisling Dawson, an analyst at ABI Research.

"Those devices might exist for several years," Dawson says. "Make sure those devices have post-quantum capabilities and make sure when you need to update them, that it can be done, other than having to rip and replace those devices."

Another potential blind spot is SaaS applications, she says. "I can see that becoming a problem as companies might want to skirt admitting how far behind they are," she says.

It can take money and personnel to fix encryption, and not all providers will have the resources or the interest in making it a priority.

On the plus side, there's more than just customer demand forcing them to step up. Some jurisdictions, including Europe, are mandating changes. And the US federal government is requiring its vendors to have quantum-safe encryption in place by 2030, Dawson says.

4. Consider quantum key distribution

As an alternative to exchanging keys with quantum-safe encryption – or in addition to it – some companies are already experimenting with quantum key distribution. This is where quantum entanglement is used to send paired photons, either through space, as with quantum communication satellites, or through fiberoptic lines. If the communication is interfered with in any way, the entanglement breaks.

This is great for security, since nobody can listen in. But it's bad for bandwidth and latency, since the individual photons can be knocked out of entanglement by heat, vibrations, or just by interacting with the fiberoptic cables themselves.

"There's not enough entanglements per second – bandwidth – to send gigabits," says Jim Ricotta, CEO and chairman at Aliro Quantum Technologies.

But encryption keys are, relatively speaking, pretty short, making them a good fit for the first quantum networks. "Keys are the number one use case," says Ricotta. "Super secure sharing of keys."

Companies that should be looking at quantum key distribution today are those most at risk of being hacked, or who have highly sensitive data, especially that of interest to state actors. "The machines are very affordable," says Holger Mueller, an analyst at Constellation Research Inc.

There's a lot of activity going on right now with quantum networking companies setting up links between different locations. "Investors are buying up data centers to create a Pony Express quantum signal to go coast-to-coast," he says. "They're buying up under-utilized or distressed assets."

5. Identify quantum opportunities

Beyond quantum-safe encryption, and quantum key distribution, there's quantum computing itself. While full-scale quantum computing is still a few years away, there are already areas in which the technology is showing value.

"If you're in the pharma or chemical industry, they're using it already," says Constellation's Mueller. "You have to look into it," Mueller warns.

And quantum computers are already playing an important role in protein folding, he says. "Quantum qubits are taking over traditional architectures for protein folding and mapping," he says. "There, you must do something in 2025."

According to a Boston Consulting Group projection from July of 2024 – from before the latest round of quantum computing breakthroughs – the technology will create between $450 and $850 billion of economic value globally by 2024.

Other experts are even more optimistic. A September report from The Quantum Insider, a market intelligence firm, forecasts that quantum computing will contribute $1 trillion in value creation by 2035. Finance, defense, life sciences, telecommunications, and manufacturing are expected to benefit the most from quantum technologies.

And when looking for opportunities, companies should do more than just think about the calculations that a quantum computer can do faster than a classical one, says Sridhar Tayur, professor of operations management at Carnegie Mellon University's Tepper School of Business.

"A quantum computer is not simply a faster classical computer, just like a plane is not just a faster car," he says. "With a plane you can fly over the ocean. What are you going to do if you have flying abilities?"

The earliest use cases, according to Infeqtion's Gokhale, lie in simulating physical processes.

Today, when a company needs to work with a physical process – say, developing a new kind of rubber for sneakers, or a new chemical or a new drug – a lot of time-consuming laboratory work is required. That's because classical computers are limited in what kinds of physical processes they can simulate, and in how accurate they can be.

"All of that can shift to being computational," Gokhale says. This has the potential to be very disruptive, he adds. "Any real-world process that can be simulated, will be simulated." Drug discovery timelines can be dramatically compressed, he says, subject to government regulation.

Another use case for simulating physical processes is to generate training data for AI systems. This is already being done to a limited extent with classical computers. For example, robotics companies are doing early-stage training for the robots in virtual environments before finishing up the training in the real world. This use case can expand dramatically with quantum computing.

"A lot of tasks are bottlenecked by a shortage of training data," Gokhale says.

6. Consider using classical computers to simulate quantum machines

Even for use cases where quantum computers aren't yet ready for prime time, there might be value in simulating their capabilities, says Tayur. "You don't have to keep waiting for the real machine," he says.

"You might be able to get something going now."

There are two ways this can work. First, there are quantum-inspired algorithms, where the principles of quantum computing inspire novel approaches to hard problems. "We're going to solve it with classical computers, but not the way we'd normally solve it," he says.

Another is using classical computers to simulate quantum machines, running the same algorithms a company would run on quantum hardware. "Then, when a real quantum computer comes along, you just swap out the simulator for the real machine," he says.

He recently worked with one hedge fund looking to solve an optimization problem, where the simulated quantum computer actually gave them better answers than what they were getting before.

7. Don't forget quantum sensors

Speaking of quantum technologies that can already be put to work, quantum sensors are real and are being deployed. The same things that make quantum computers so unreliable, such as their sensitivity to heat, vibrations, and environmental noise of all kinds, makes them perfect for industrial sensors.

"Position, navigation and timing are common applications," Eric Ostby, chief product officer at Aliro Quantum Technologies. "The US government has made proposals to increase the sensitivity and ability of navigational sensors to operate without GPS."

This can be useful where GPS doesn't work or isn't reliable, he says – or in areas where GPS signals are being actively jammed, such as war zones. There are also biomedical applications of quantum sensors, he says, "for example, for imaging of the heart."

8. Build quantum expertise

Companies that want to be early adopters should start developing quantum talent today, if they haven't already.

"If you're in financial services, defense, or logistics, or you have problems where you're currently using Monte Carlo simulations or high performance computing, it's probably worth your time to take some people and have them learn about quantum computing," says Gartner's Horvath. "Having someone on your staff who knows that they're capable of doing and being able to identify a problem where a quantum computer can be useful is a big deal."

But, except for the most cutting-edge companies, being able to actually run a quantum computer locally isn't going to be necessary. "Most quantum companies have quantum computing as a service," says Horvath. "With IBM, for example, you can go and just use one of their computers online."

In addition, the big hyperscalers all offer cloud-based quantum computing access, partnering with multiple quantum hardware manufacturers so that enterprises can easily try out different quantum computers.

9. Build partnerships

The last step that enterprises can take today is to build partnerships with key players in the quantum computing space. That could be quantum computing manufacturing themselves and platform providers like hyperscalers. Pharma companies, for example, are hedging their bets, says Constellation's Mueller, working with both hyperscale providers and individual quantum startups like Rigetti and D-Wave.

And then there are universities and other research firms, as well as consultants and other experts.

"Quantum technologies have the potential to transform nearly every industry, but harnessing that potential requires a breadth and depth of talent that is challenging to recruit and retain," says Jordan Kenyon, chief scientist at Booz Allen Hamilton's quantum practice.

Strategic partners can fill that gap, he says, and help companies adopt quantum technologies until they reach sufficient internal capacity themselves.

32. Utimaco Launches Post Quantum Security App Package

by Greg Bock
https://thequantuminsider.com/2025/04/03/utimaco-launches-post-quantum-security-app-package/

Utimaco, a leading global provider of IT security solutions, has announced the launch of Quantum Protect, the Post Quantum Cryptography application package for its u.trust General Purpose HSM (Hardware Security Modules) Se-Series.

The advent of quantum computers poses a threat to today's cryptographic landscape. A cryptanalytically relevant quantum computer that could break common public key schemes such as RSA or ECC is expected by 2030. That may seem far away, but organizations need to plan their migration to Post Quantum Cryptography (PQC) now in order to stay secure. Last year, the National Institute of Standards and Technology (NIST) not only standardized quantum-secure algorithms but also set a timeline of 2030 for their implementation and the depreciation of currently used cryptographic methods like Elliptic Curve DH, MQC, Finite Field DH, MQV, RSA etc.

Utimaco has been working for a long time on solutions that give its customers a head start in the migration to PQC. It received Frost & Sullivan's 2024 Global Competitive Strategy Leadership Award in the Post-Quantum Cryptography industry in recognition of its efforts. The launch of Quantum Protect, and the free, fully functional Quantum Protect simulator, marks the next milestone in Utimaco's PQC development.

Quantum Protect

- Supports the PQC algorithms ML-KEM and ML-DSA, standardized by NIST
- Supports mature stateful hash-based signature schemes LMS and XMSS (and their multi-tree variants HSS and XMSS-MT)
- Used with Utimaco's u.trust General Purpose Hardware Security Module, Quantum Protect implements all algorithms defined by the Commercial National Security Algorithm Suite (CNSA) 2.0 as mandatory for certain use cases by 2025:
- LMS, XMSS, ML-KEM, ML-DSA, AES, SHA
- Includes a patented solution for state management of stateful hash-based signatures
- Is based on a PKCS #11 integration

The Quantum Protect application package can be activated in-field, a hardware exchange is not necessary. Further PQC algorithms (such as SLH-DSA) are on the roadmap for future releases. It can be added to Utimaco's next-generation Hardware Security Module (HSM) which is built on future-proof hardware featuring an advanced FPGA chip, ensuring seamless hardware acceleration ready for quantum-resistant use cases.

Additionally, Utimaco is the only Hardware Security Module (HSM) vendor offering a free, fully functional simulator for the new PQC standards that allows users to test how the algorithms serve their use cases in their environment before buying. The Quantum Protect simulator is especially valuable because the algorithms are still new to the market and there is only limited practical experience with them. Using the simulator saves time in project evaluation and development as the APIs, configuration and management processes are identical to using the hardware and can easily be transferred to a production environment.

Cindy Provin, CSO, Utimaco, said: "We are very excited to launch our new Quantum Protect solution as it underlines the crypto agility and future-readiness of Utimaco and our HSM portfolio. It extends the use cases of our HSMs and equips our customers and partners with the crypto-agility capabilities and quantum security they need to secure the future of their products and services. With further algorithms already on the roadmap, our u.trust GP HSM Se-Series + Quantum Protect are an investment for a secure future, making Utimaco the best choice as a strategic partner for PQC migration and implementation."

"We have been using Utimaco's products for years to secure our cryptographic applications, and they continue to prove themselves as a trusted partner in post quantum cryptography. We have already used their pre-release version of Quantum Protect and benefited from the latest NIST ML-KEM and ML-DSA algorithms in specific projects. With Utimaco's crypto agile and PQC-ready HSMs, we are enabling quantum-secure firmware updates for our chips and semiconductors, ensuring a seamless transition to a post-quantum secure era," said Stephan Zimmermann, Head of NXP's Trust Provisioning Service.

33. Enhancing Quantum Key Distribution with Trusted Nodes and Post-Quantum Cryptography in Paris

by RUSTY FLINT

https://quantumzeitgeist.com/enhancing-quantum-key-distribution-with-trusted-nodes-and-post-quantum-cryptography-in-paris/?utm_source=substack&utm_medium=email

On April 2, 2025, a notable advancement in quantum communication was published under the title Quantum Key Distribution with Efficient Post-Quantum Cryptography-Secured Trusted Node on a Quantum Network. This research addresses the scalability and security limitations of Quantum Key Distribution (QKD) by introducing trusted nodes secured through post-quantum cryptographic techniques successfully implemented within a fibre optic network in Paris.

The research presents an efficient Quantum Key Distribution (QKD) scheme that addresses inherent limitations in distance and scalability by introducing a trusted node with reduced privacy requirements. Leveraging post-quantum cryptographic techniques, the proposed method enhances security while maintaining practicality. Implementing a deployed fiber optic network in Paris demonstrates its real-world applicability, offering a scalable solution for secure communication infrastructure.

Paris Quantum Network

In a significant stride towards advancing secure communication technologies, the Paris Quantum Network has emerged as a cutting-edge platform for quantum key distribution (QKD). This network, comprising 11 nodes across Paris and its suburbs, is spearheaded by eight prominent academic and industrial partners. Its establishment underscores Europe’s commitment to leading in quantum technology development, offering a robust framework for testing and implementing next-generation secure communication systems.

Technical Infrastructure and Performance

The network features eight main nodes located at key institutions and companies, including the Laboratoire Matriaux et Phénomènes Quantiques (MPQ) and Orange Innovation. These nodes utilize both discrete-variable and continuous-variable QKD systems, ensuring versatility in testing various quantum communication protocols. The network’s performance metrics, such as secret key rates, quantum bit error rate (QBER), and visibility, have been meticulously monitored to assess the efficiency of secure key exchange over fiber-optic links with specific loss characteristics.

Applications and Current Utilization

The Paris Quantum Network is a vital testbed for benchmarking quantum technologies. It facilitates interoperability testing between different QKD systems, ensuring seamless communication across diverse platforms. Additionally, the network explores the coexistence of quantum and classical data transmission, paving the way for integrated communication networks. Future endeavors include entanglement distribution and the integration of quantum memories, enhancing the network’s capabilities for long-distance secure communication.

Strategic Importance and Future Prospects

The Paris Quantum Network is pivotal in shaping Europe's quantum strategy, positioning Paris as a global hub for quantum innovation. By fostering collaboration among academic and industrial entities, it accelerates advancements in quantum technologies with potential applications across various sectors. As the network evolves, it promises to unlock new possibilities in secure communication, solidifying Europe's leadership in this transformative field.

In conclusion, the Paris Quantum Network exemplifies the convergence of technological innovation and strategic foresight, setting a benchmark for future developments in quantum communication. Its success enhances secure data exchange and underscores the importance of collaborative efforts in driving technological progress.

34. The Rise of Quantum-Resistant Cryptography – Preparing for a Post-Quantum World

by Anuj Khurana
https://dailyhodl.com/2025/04/03/the-rise-of-quantum-resistant-cryptography-preparing-for-a-post-quantum-world/

The digital world is on the cusp of a major transformation with the rapid advancement of quantum computing.

While this breakthrough technology promises unprecedented computational power, it also poses a significant threat to current encryption systems.

Cryptographic methods that secure our financial transactions, communications and sensitive data may become obsolete.

This has led to the emergence of quantum-resistant cryptography, a crucial field focused on safeguarding digital assets against quantum-based attacks.

Understanding the quantum threat

Classical encryption methods, such as RSA and ECC (elliptic curve cryptography), rely on complex mathematical problems that would take traditional computers thousands of years to solve.

However, quantum computers leverage Shor's algorithm, which can break these encryptions within hours or even minutes.

This means that once quantum computing reaches a practical level, many of today's security protocols will no longer be viable.

The urgency to develop post-quantum cryptographic solutions has never been higher.

What is quantum-resistant cryptography

Quantum-resistant, or PQC (post-quantum cryptography), refers to cryptographic algorithms designed to withstand attacks from quantum computers.

Unlike traditional encryption, PQC methods do not rely on integer factorization or discrete logarithm problems, which are vulnerable to quantum attacks.

Instead, they utilize advanced mathematical principles such as the following.

- **Lattice-based cryptography** – Uses complex lattice structures that even quantum computers struggle to solve.
- **Hash-based cryptography** – Relies on the security of cryptographic hash functions, which remain resistant to quantum attacks.
- **Multivariate polynomial cryptography** – Uses multivariable equations that are difficult to reverse engineer.
- **Code-based cryptography** – Implements error-correcting codes to create secure encryption schemes.

The urgency for adoption

Governments and organizations worldwide are already preparing for the post-quantum era.

The NIST is in the process of standardizing quantum-resistant algorithms to replace current cryptographic systems.

Financial institutions, healthcare providers and technology companies are also investing in post-quantum security measures to future-proof their infrastructure.

A major concern is the concept of 'harvest now, decrypt later' attacks.

Malicious entities can collect encrypted data today and decrypt it in the future once quantum computing becomes powerful enough.

This makes it essential to implement PQC sooner rather than later to protect sensitive information from future threats.

Current market trends and statistics

According to a recent Allied Market Research report, the global quantum cryptography market was valued at $89 million in 2020 and is projected to reach $214 million by 2026, growing at a CAGR of 19.1% during the forecast period.

The rising demand for cybersecurity solutions in industries such as finance, healthcare and government is driving this growth.

Another study by Deloitte estimates that more than 25% of all encrypted data on the internet could be at risk once quantum computers become powerful enough.

This alarming statistic underscores the urgency of transitioning to post-quantum cryptographic methods.

Challenges in implementing PQC

Despite its potential, quantum-resistant cryptography comes with its own set of challenges.

- **Computational overhead** – Some PQC algorithms require significantly more processing power, making them less efficient for low-power devices.
- **Compatibility issues** – Existing digital systems must be upgraded or redesigned to accommodate new cryptographic methods.
- **Standardization delays** – The process of establishing universally accepted quantum-resistant algorithms is still ongoing, slowing down widespread adoption.
- **Cost of migration** – Transitioning to post-quantum security involves significant investment in infrastructure and training.

Industries at high risk

Some industries are more vulnerable than others to quantum threats due to their reliance on secure communications and data protection.

- **Financial services** – Banks and payment processors rely on encryption for transactions. A breach due to quantum attacks could lead to financial chaos.
- **Healthcare** – Patient records and medical data must remain confidential. Quantum computing could make it easier to breach these databases.
- **Government and defense** – National security agencies depend on cryptographic security to protect classified information.
- **Cloud computing** – Cloud storage providers need quantum-resistant encryption to ensure data remains safe from future threats.

Steps to prepare for a post-quantum world

Organizations must take proactive steps to integrate PQC into their cybersecurity strategies. Steps include the following.

Identifying vulnerable encryption methods in current systems.
Testing and integrating post-quantum cryptographic algorithms into applications.
Collaborating with cybersecurity experts and regulatory bodies to stay ahead of emerging threats.
Educating stakeholders about the risks of quantum computing and the need for cryptographic transition.
Adopting hybrid cryptographic solutions that combine classical and quantum-resistant encryption during the transition phase.

The road ahead

As quantum computing continues to advance, the race for quantum-resistant security solutions is intensifying.

Companies like IBM, Google and Microsoft are heavily investing in quantum research, which means the reality of breaking current encryption standards is approaching faster than anticipated.

The need for action is clear – organizations must prioritize quantum-resistant cryptography to protect their digital infrastructure.

Conclusion

Quantum computing is no longer a distant future – it's an imminent reality that requires immediate attention.

The shift toward quantum-resistant cryptography is not just an option but a necessity for ensuring the security of digital assets.

Businesses, governments and individuals must act now to protect their data before quantum computers render current encryption obsolete.

The future of cybersecurity hinges on this transition, and those who prepare today will have a significant advantage in the post-quantum world.

35. Alice & Bob Selected by DARPA for the Quantum Benchmarking Initiative

by Niccolò Coppola
https://alice-bob.com/newsroom/alice-bob-for-darpa-qbi/?utm_source=LinkedIn&utm_medium=Social&utm_campaign=QBI

Alice & Bob, a leader in fault-tolerant quantum computing, today announces its selection as a performer in the U.S. Defense Advanced Research Projects Agency's (DARPA) Quantum Benchmarking Initiative (QBI). Under this program, Alice & Bob will contribute to QBIs mission of verifying and validating whether fault-tolerant quantum computers can achieve utility-scale operation—where computational value exceeds costs—by 2033.

Under the agreement, Alice & Bob can advance through three critical stages, with each phase contingent on the successful completion of the previous one. In Stage A, the company will detail the concept of a utility-scale quantum computer based on cat qubits, already a goal of the French startup's ambitious roadmap to 2030 published last December. If selected for Stage B, Alice & Bob will develop a detailed R&D plan for building such a machine, identifying key risks, necessary prototypes, and the steps required to advance fault tolerance. Finally, Stage C will involve close collaboration with DARPA's test and evaluation team to rigorously verify and validate that Alice & Bob's quantum computing approach can be constructed and operated as intended at scale.

The Department of Energy's (DOE) Office of Science plays a key role in QBI providing critical tools, infrastructure, and expertise to rigorously evaluate, co-design and determine useful quantum computers' feasibility for real-world applications.

Alice & Bob will leverage its proprietary cat qubit technology to build scalable and useful fault-tolerant quantum computers. The company's approach, which inherently suppresses bit-flip errors, dramatically reduces the hardware needed for quantum error correction, one of the primary challenges in quantum computing. Given their fundamental characteristics that promote error correction at scale, cat qubits are conceived to reach large scale quantum computing more efficiently at a fraction of the footprint, and costs of alternative approaches.

"Alice & Bob has always been solely focused on building a universal, fault-tolerant quantum computer," said Théau Peronnin, CEO and Co-founder of Alice & Bob. *"The DARPA QBI contract is a major validation of our approach, allowing us to work on the real-world impact of quantum computers in high-technology domains, including chemistry and materials science."*

DARPA's interest in utility-scale quantum computing reflects the growing recognition of its strategic importance in advancing computing, and scientific discovery. By participating in QBI, Alice & Bob strengthens its position at the forefront of global quantum innovation.

The company has recently obtained a $100 million Series B funding round and has been selected for PROQCIMA, the multi-million quantum computing procurement program by the French government.

"Alice & Bob's selection for the QBI program underscores the transformative potential of our cat qubits," said Raphaël Lescanne, CTO and Co-founder of Alice & Bob. *"With DARPA's and the QBI teams' support, we will keep innovating quantum error correction and sustain our momentum towards practical quantum computing."*

36. Quantinuum's 'Quantum Origin' Becomes First Software Quantum Random Number Generator to Achieve NIST Validation

by Quantinuum
https://www.prnewswire.com/in/news-releases/quantinuums-quantum-origin-becomes-first-software-quantum-random-number-generator-to-achieve-nist-validation-302418007.html

Quantinuum, the industry leader in quantum computing with the world's highest performing quantum computer, today announced that Quantum Origin, the company's software Quantum Random Number Generator (QRNG), has received National Institute of Standards and Technology (NIST) validation. Quantum Origin is the first software QRNG to achieve this validation, establishing it as a crucial tool for federal agencies and agency partners in their mandated migration to post-quantum cryptography (PQC) under National Security Memorandum 10. This achievement will help strengthen cybersecurity in the age of PQC.

Quantum Origin generates mathematically proven randomness — a capability unmatched by hardware-based QRNGs or traditional pseudo-random number generators. Unlike hardware solutions that require specialized equipment and can be affected by environmental factors, Quantum Origin delivers consistent, proven randomness through flexible software deployment. Proven quantum randomness is an essential foundation for comprehensive quantum security strategy alongside PQC.

"The evolving threat landscape demands a new era of cybersecurity solutions for governments, enterprises, and critical infrastructure," said Dr. Rajeeb Hazra, President and CEO of Quantinuum. "Quantinuum is at the forefront of this transformation, driving innovation in quantum cybersecurity. Our recent certified randomness demonstration with JPMorganChase, and our NIST-validated Quantum Origin platform are just two examples of how we are deepening our portfolio to meet this critical need."

Quantum Origin is delivered entirely as self-contained software, making it adaptable to diverse environments from cloud solutions to highly sensitive systems. It can be deployed with zero network connectivity, enabling protection for air-gapped networks and confidential environments where traditional hardware-based QRNGs cannot operate effectively. It provides quantum-enhanced security without impacting the size, weight, and power (SWaP) requirements of existing systems, a critical consideration for resource-constrained deployments.

U.S. made using Quantinuum's quantum computers based in Colorado, Quantum Origin helps mitigate supply chain risks associated with foreign-sourced hardware components. It is designed to integrate seamlessly with existing NIST-approved cryptographic systems without requiring recertification. With this NIST validation, organizations can now accelerate their adoption of quantum-enhanced security within existing compliance frameworks.

37. SandboxAQ quantum-resistant encryption algorithm approved by NIST

by Anthony Kimery
https://www.biometricupdate.com/202504/sandboxaq-quantum-resistant-encryption-algorithm-approved-by-nist

Palo Alto, California-based SandboxAQ has achieved a significant milestone with the National Institute of Standards and Technology (NIST) having officially selected its Hamming Quasi-Cyclic (HQC) algorithm as the fifth algorithm in its suite of post-quantum cryptographic (PQC) standards.

Out of these five algorithms, three will be used for digital signatures, while HQC and ML-KEM will serve as the NIST-approved solutions for ensuring the confidentiality of communications across the internet, cellular networks, payment systems, and other critical infrastructure. ML-KEM has been standardized by NIST as a post-quantum secure key encapsulation mechanism (KEM) that can be used for key establishment between two parties.

The HQC algorithm is a code-based post-quantum encryption scheme that is designed to withstand quantum computing attacks. It is structured around error-correcting codes, particularly leveraging quasi-cyclic codes, to provide secure encryption mechanisms that are resistant to quantum threats.

The selection of HQC represents SandboxAQ's second major contribution to NIST's post-quantum standardization effort, and a critical step in the global transition toward a quantum-safe encryption, providing robust protection against emerging threats posed by quantum computing advancements.

HQC's inclusion in NIST's suite reinforces the necessity of transitioning away from traditional encryption methods such as RSA and elliptic-curve cryptography, which will be rendered obsolete by sufficiently powerful quantum computers.

HQC is a key encapsulation mechanism designed to secure the exchange of encryption keys in a quantum-resistant manner. Unlike conventional public-key encryption systems, HQC is built on the mathematical foundation of error-correcting codes, which are resistant to quantum attacks.

In its final selection report, NIST highlighted HQC's robust security and its ability to balance computational efficiency with key size, making it a viable option for large-scale deployments. This achievement follows multiple rounds of rigorous cryptanalysis and peer review.

Prior to HQC's selection, SandboxAQ played a critical role in the development of SPHINCS+, one of the digital signature algorithms included in NIST's initial set of PQC standards in 2022. With HQC now added to the standardization process, SandboxAQ has contributed to two of the five essential PQC standards, solidifying its leadership in quantum-resistant cybersecurity solutions.

Taher Elgamal, a senior advisor at SandboxAQ and a partner at Evolution Equity Partners, emphasized the significance of HQC's selection, noting that its foundation in coding theory offers strong theoretical and practical protections against quantum decryption methods. Additionally, HQC's efficient performance profile makes it suitable for widespread adoption.

"HQC has foundations in coding theory that offer strong theoretical and practical protection against known quantum decryption methods, while its efficient performance profile makes it well-suited to real-world adoption," Elgamal, a partner at Evolution Equity Partners and senior advisor at SandboxAQ.

"This is not just a milestone for SandboxAQ, it's a win for global security in the face of future quantum disruption," he adds.

Carlos Aguilar Melchor, chief cybersecurity scientist at SandboxAQ, said the development of HQC dates to the 2000s, with critical breakthroughs in the 2010s addressing long-standing challenges in code-based key exchanges. Melchor said HQC is now one of only two protocols securing the confidentiality of global communications, an achievement that speaks to SandboxAQ's ongoing commitment to shaping the future of cryptography.

"Today, HQC stands as one of only two protocols securing the confidentiality of nearly all global communications" Melchor said, adding that "we've long championed the importance of standardization, and contributing to two of the five NIST PQC standards reflects our commitment to shaping the future of cryptography."

NIST's decision to standardize HQC reflects the broader global effort to prepare for the eventual emergence of large-scale quantum computers. Quantum computing poses a fundamental threat to existing encryption methods by enabling adversaries to break widely used cryptographic protocols. NIST has been leading the charge in developing quantum-resistant encryption standards to ensure that sensitive data – including internet traffic, financial transactions, and national security communications – remain secure in a post-quantum world.

Last year, NIST finalized ML-KEM as the primary quantum-resistant encryption standard. HQC now serves as a backup mechanism, ensuring an alternative approach is available should ML-KEM face unforeseen vulnerabilities in the future.

Dustin Moody, head of NIST's Post-Quantum Cryptography project, reaffirmed the importance of diversifying cryptographic solutions to mitigate emerging threats, emphasizing that organizations should continue migrating to the already established PQC standards while preparing for the eventual deployment of HQC.

Encryption systems rely on complex mathematical problems that are infeasible for conventional computers to solve within a reasonable timeframe. However, quantum computers could rapidly solve these problems using Shor's algorithm, undermining the security of current encryption methods. ML-KEM and HQC provide quantum-resistant alternatives by leveraging different mathematical principles — ML-KEM is based on structured lattices, whereas HQC relies on error-correcting codes. This diversity in cryptographic approaches is critical for ensuring long-term security in an era of advancing quantum technologies.

HQC's standardization follows a rigorous selection process conducted by NIST's Post-Quantum Cryptography project, which has been evaluating quantum-resistant cryptographic solutions since 2016. Alongside HQC, NIST previously selected four other algorithms: ML-KEM for general encryption and CRYSTALS-Dilithium, FALCON, and SPHINCS+ for digital signatures.

ML-KEM is the foundation of FIPS 203, while CRYSTALS-Dilithium and SPHINCS+ are incorporated into FIPS 204 and FIPS 205. A forthcoming standard, FIPS 206, will feature the FALCON digital signature algorithm, rounding out the suite of approved post-quantum cryptographic solutions.

Incorporating HQC into the NIST PQC standards ensures an additional layer of security, addressing potential future cryptanalysis breakthroughs that could weaken existing encryption mechanisms. NIST plans to release a draft standard for HQC in about a year, followed by a 90-day public comment period. The finalized HQC standard is expected to be released in 2027.

HQC, like ML-KEM, operates as a key encapsulation mechanism, facilitating the secure exchange of encryption keys over public networks. NIST has issued draft guidelines for implementing KEMs, detailed in *Special Publication 800-227*, which outlines best practices for deploying key encapsulation mechanisms in secure environments.

The U.S. Department of Commerce has also emphasized the importance of quantum-resistant encryption in maintaining national and economic security. Deputy Secretary of Commerce Don Graves said the role of quantum technology is shaping the future of cybersecurity, and reaffirmed NIST's commitment to safeguarding confidential digital information.

Laurie E. Locascio, who left the role of under secretary of commerce for standards and technology and NIST director in January, said proactive measures are essential to mitigate the risks posed by quantum computing advancements.

The finalization of post-quantum encryption standards marks a critical juncture in the evolution of cybersecurity. The threat posed by quantum computing is no longer theoretical; it is an impending reality that requires immediate action. NIST's selection of HQC, alongside ML-KEM and other PQC standards, provides a strong foundation for securing sensitive data against future threats. NIST has said that organizations need to begin prioritizing the integration of quantum-resistant encryption protocols to ensure long-term data security.

38. Commission unveils ProtectEU – a new European Internal Security Strategy

https://ec.europa.eu/commission/presscorner/detail/en/ip_25_920

Today (01 April 2025), the European Commission is presenting ProtectEU — a European Internal Security Strategy to support Member States and bolster the EU's ability to guarantee security for its citizens. The strategy sets out an ambitious vision and workplan for the years to come, with a sharper legal toolbox, increased information sharing and deeper cooperation.

In a changed security environment and an evolving geopolitical landscape, where hybrid threats by hostile foreign states and state-sponsored actors are growing, where powerful organised crime networks are proliferating and criminals and terrorists are operating increasingly online, Europe needs to review its approach to internal security. Announced by President von der Leyen in the political guidelines, the Strategy will upgrade the Union's response to new and traditional threats to internal security.

The Strategy aims to foster a change of culture on internal security, with a whole of society approach involving citizens, businesses, researchers and civil society. Security aspects will be mainstreamed in the development of new initiatives, and a new European internal security governance framework will support the implementation of the Strategy.

As Ursula von der Leyen, President of the European Commission said: *"Safety is one of the key prerequisites for open, vibrant societies and a flourishing economy. That's why we are launching today an important initiative to better tackle security threats like terrorism, organised crime, surging cybercrime and attacks against our critical infrastructure. We will strengthen Europol and give law enforcement up-to-date tools to fight crime. But also researchers, businesses and even citizens can contribute to greater safety for all."*

The European Internal Security Strategy complements the Preparedness Union Strategy and the European Defence White Paper. Together with the forthcoming European Democracy Shield, they form a comprehensive framework for a safe, secure and resilient EU.

Key objectives and actions

A new European internal security governance

The new threat landscape requires a change in mindset and an upgraded EU approach to internal security:

- Identifying security and preparedness implications of Commission initiatives from the start and throughout the negotiation process,
- Regular threat analyses related to internal security to support the work of the Security College and exchanges in the Council,
- Regular reporting to the European Parliament and the Council to track and support the implementation of key initiatives.

Anticipating security threats through new ways of sharing intelligence

As security starts with effective anticipation, the EU must rely on high-quality situational awareness and threat analysis:

- Develop regular overviews of the EU internal security threat landscape, building on various risk and threat assessments done notably by EU agencies,
- Enhance intelligence-sharing by Member States with the EU's Single Intelligence Analysis Capacity (SIAC),
- Ensure better information sharing by Member States with EU agencies and bodies.

More effective tools for law enforcement and stronger JHA agencies

Law enforcement needs the right tools to be effective. And with 85% of criminal investigations relying on digital information, this includes lawful access to data:

- A new mandate for Europol to turn it into a truly operational police agency to reinforce support to Member States,
- Strengthening Frontex, Eurojust and ENISA and ensuring close cooperation between agencies,
- Enhancing operational capabilities with a new Critical Communication system to allow for cross border communication between different authorities,
- A Roadmap on lawful and effective access to data for law enforcement,
- A Technology Roadmap on encryption, and an impact assessment with a view to updating the EU's data retention rules.

Building resilience against hybrid threats

The EU must enhance its resilience against hybrid threats by protecting critical infrastructure, reinforcing cybersecurity and combatting online threats:

- Member States to fully implement the CER and NIS2 Directives,
- A new Cybersecurity Act, and new measures to secure cloud and telecom services and developing technological sovereignty,
- Measures to reduce dependencies on single foreign suppliers and de-risk our supply chains from high-risk suppliers including revision of procurement rules,
- Reinforce the security of transport hubs, with an EU Ports Strategy, and new reporting systems to strengthen aviation security, transport and supply chains,
- An Action Plan against chemical, biological, radiological and nuclear (CBRN) threats.

Fighting serious and organised crime

Stronger rules are needed to fight organised crime networks. Law enforcement must be able to go after their money. Children must be better protected from organised crime:

- A new legal framework on organised crime, with stronger rules on investigations,
- A new Strategy and Action Plan on Drugs and Drugs Trafficking,
- An Action Plan on the Protection of Children against Crime,
- Strengthening the ‘Follow the Money' approach, including by full transposition of the new rules on asset recovery and confiscation,
- New legislation against firearms trafficking; new EU Strategies on Trafficking in Human Beings and on Victims' Rights.

Combatting terrorism and violent extremism

With the terrorist threat level in the EU remaining high, the EU needs to be well equipped to anticipate threats, prevent radicalisation, protect citizens and respond to attacks:

- A new EU Agenda on preventing and countering terrorism and violent extremism,
- A new toolbox to prevent radicalization,
- Feasibility study for a new EU-wide system to track terrorist financing.

The EU as a strong global player on security

To counteract the impact of global instability, the EU needs to actively defend its security interests beyond its borders, by boosting international cooperation on security and:

- Strengthening partnerships with key regions such as Latin America and the Mediterranean region,
- Concluding international agreements by Europol and Eurojust including to establish joint operational teams with local law enforcement authorities,
- Strengthening information exchange with trusted third countries,
- Completing the revision of the Visa Suspension Mechanism and addressing security considerations in the upcoming Visa Strategy.

39.What Does Security Look Like in a Post-Quantum World? ST Looks Ahead

by Duane Benson
https://www.allaboutcircuits.com/news/what-does-security-look-like-post-quantum-world-st-looks-ahead/

At Embedded World 2025, STMicroelectronics delivered a conference session where it introduced solutions targeted at risk prevention in a post-quantum cryptography world. Post-quantum cryptography (PQC) refers to the expected ability of quantum computers to easily crack conventional cryptographic security.

In the near future, today's world's best encryption may be vulnerable to attacks from powerful quantum computers. ST is among a group of companies already developing security solutions resistant to quantum cracking.

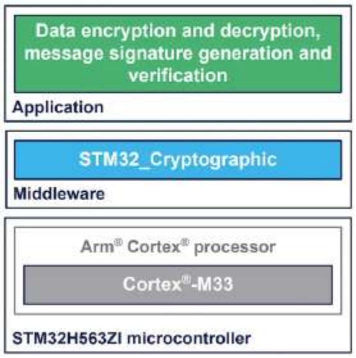
What Is Post-Quantum Cryptography?

Quantum computing, like so many other technologies, is a double-edged sword with opportunities for good and bad. Current cryptography, which secures financial transactions, classifies nuclear weapon launch codes, and prevents digital eavesdropping, is based on public key encryption. With public key encryption, two very large prime numbers are multiplied together, and the product is used as the encryption seed. The level of security is based on how long a conventional computer takes to determine what the prime numbers are.

Quantum computing can solve problems millions or billions of times faster than conventional computing. Once fully realized, decryption attacks that, in today's digital world, are effectively unsolvable due to the time and resources required may be solvable in seconds or less. When that happens, the best encryption humanity has will be null and void.

ST Fortifies Its Post-Quantum Assets

Fortunately, cryptographers are not sitting back and waiting for the end to come. They are working on algorithms and joining with silicon companies to develop cryptographic systems secure against both conventional and quantum decryption attacks.


Data encryption and decryption, message signature generation and verification
Application
STM32_Cryptographic
Middleware
Arm® Cortex® processor
Cortex®-M33
STM32H563ZI microcontroller

ST's PQC solutions include cryptographic algorithms integrated into general-purpose microcontrollers (MCUs), secure MCUs, and automotive MCUs. Additionally, ST has introduced hardware cryptographic accelerators and associated software libraries.

The libraries come in the form of X-CUBE-PQC, a firmware library for use with STM32Cube, ST's Eclipse-based development environment for writing and managing C/C++ code for STM32 microcontrollers and microprocessors.

PQC in the MCUs of Today and Tomorrow

Researchers at the National Institute of Standards and Technology (NIST) and private companies have been developing cryptography standards for the post-quantum world.

The Keccak algorithm, developed by ST researchers, is based on quantum-difficult math. NIST released key PQC standards based on Keccak in August 2024. These new NIST algorithms will eventually replace the current go-to standards, RAS and ECC. NIST's latest PQC standards, FIPS-203 (ML-KEM) for key encapsulation, FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA), can be executed on many of today's 32-bit microcontrollers.

ST is shipping PQC-ready Arm Cortex-M and Cortex-A STM32 MCUs and MPUs that can use PQC libraries. SPC5 32-bit and Stellar 32-bit automotive MCUs come with an SHA-3 accelerator to support PQC.

Though quantum computers may be years to decades away from breaking cryptography, many embedded devices have life-cycles long enough that deployed products may someday exist in a PQC world. Although no one knows when PQC will arrive, by implementing PQC algorithms now, devices developed today will not need to be replaced when it does.

The other risk comes from what the industry refers to as “harvest now, decrypt later” (HNDL). Encryption is not just used to protect real-time assets. Many files are encrypted and then stored for later use or reference. A bad actor or adversary can steal such files even if they can't decrypt them today. When PQC happens, they might decrypt a file and, if the data is still relevant, cause new security risks. By encrypting for PQC now, fewer of these files will be at risk from HNDL attacks.

With its Embedded World announcement, ST hopes to provide present and future risk mitigation. X-CUBE-PQC is available for download now. ST also has a number of Arm products for commercial, automotive, and high-reliability applications available for PQC development.