Crypto News

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

January 06, 2025

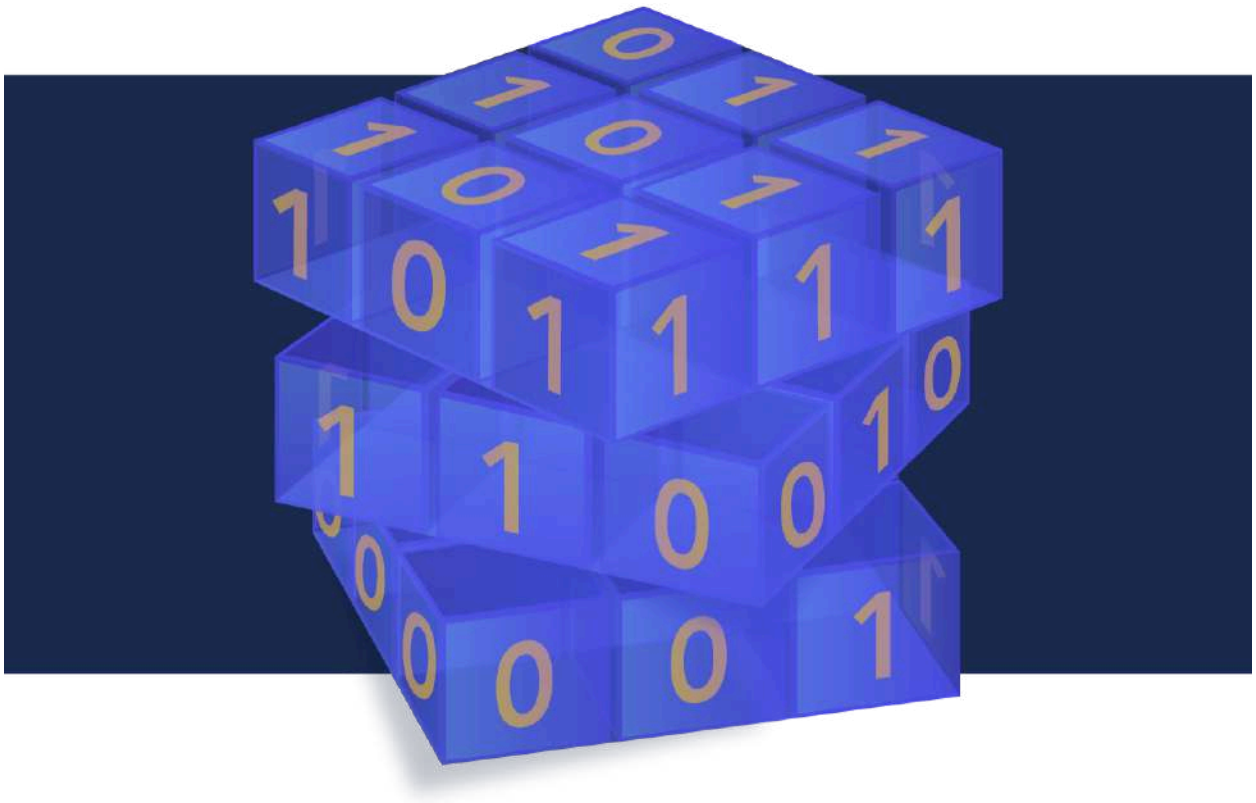


Table of Contents

Editorial

Happy New Year Readers! I hope you were able to celebrate while also getting some well-deserved rest and relaxation. Now it's time to get back in the swing of things and what better way to catch up than with this issue of Crypto News. Let's dive right in and talk to our colleagues in charge of public TLS certificate rotation. In preparation for Post-Quantum Cryptography (PQC), both Google and Apple will be significantly reducing public TLS certificate lifespans over the next 6-12 months. Get ready to rotate Google certificates every 90 days and Apple certificates every 90 days to start and then every 47 days by 2028. 74% of leaders say the Google requirement will cause chaos at their organizations and 67% dread the day their organizations will ask about PQC. Are you amongst these leaders? Read article 4 for more information and what you can do to reduce the stress you may be feeling with these quickly approaching changes.

Interested to know what other timelines you're working with? Make your way to article 7 to learn about what different quantum industry leaders have planned and their timelines to get it done. From increasing the number of qubits utilized to achieving fault tolerance, different organizations have different goals but they're all working towards the same goal of quantum supremacy.

One of the updated roadmaps is from Google after the release of Willow last month. As some background, Willow is Google's quantum chip with 105 qubits which claims to reduce errors exponentially while adding more qubits. Additionally, they claim that errors can be corrected in real time. Though the problem Willow performed a computation for in 5 minutes to showcase this important step forward would have taken the largest supercomputer 10 septillion (that's 10 to the 25th power) years to compute, the problem was specifically created for a quantum computer to solve 30 years ago. So, in all fairness, our classical computers never stood a chance. However, Willow is still a large step forward in addressing the issue of "noise" in quantum computing even if there are no commercial applications … yet.

Speaking of Willow, you'll also want to take a look at article 22 to learn more about what the cryptocurrency world is saying about the claims Willow will break bitcoin. Judge for yourself and take steps accordingly. As always, happy reading!

The Crypto News editorial is authored by the co-Chair of the Quantum-Safe SecurityWorking Group (QSS WG) of the Cloud Security Alliance (CSA), Mehak Kalsi, MS, CISSP, CISA, CMMC-CCP and it is compiled by Dhananjoy Dey. Both are active members of the CSA QSS WG. The guiding principle of the QSS WG is to address key generation and transmission methods and to help the industry understand quantum-safe methods for protecting their networks and their data.

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. 2025 Expert Quantum Predictions – PQC And Quantum Cybersecurity

by Matt Swayne
https://thequantuminsider.com/2024/12/31/2025-expert-quantum-predictions-pqc-and-quantum-cybersecurity/

We had so many submissions for our 2025 Expert Predictions that were mainly focused on post-quantum cybersecurity issues that we broke this out for a separate column. The following provides a curated list of just some of those experts who submitted their key insights and emerging trends that may shape post-quantum cybersecurity for 2025.

BEN PACKMAN, CSO OF PQSHIELD

NIST in 2025

PQShield co-authored the PQC standards released by NIST this summer, and he has worked with The White House, the European Parliament, and the likes of AMD and Microchip Technologies to support the implementation of this technology.

Ben Packman, CSO of PQShield, made this prediction for 2025:

In 2025, enterprises will start deploying post-quantum cryptography at scale – moving out of the "discovery" phase at the start of their adoption roadmaps.

After NIST's PQC standards were finalized in summer 2024, the conversation around PQC became more definite and adopting PQC became about compliance. For most businesses, the first phase to compliance was cryptographic discovery, in which they identified where their most critical data with the longest half-life lay and understood their vulnerabilities and their vendors' as well.

Now, most enterprises are entering 2025 with a greater understanding of what the transition to PQC means and how they can manage their assets to enter the "deployment" phase. At the same time, the pathway to compliance will become clearer as industry bodies align on a standard method for achieving "hybrid" protection, between PQC and traditional cryptography (PQ/T). As a result, enterprises will find it easier to stay one step ahead of the attackers and modernize their cryptography.

ROB STEVENSON – BACKUPVAULT

I believe 2025 will be a crucial year for quantum computing. The transition from physical qubits to logical qubits will fundamentally redefine what quantum technology can achieve, opening doors that were previously locked by high error rates and scalability limitations.

From a cybersecurity perspective, this evolution demands urgent attention. Quantum computers will eventually have the capability to break current encryption standards, making quantum-safe cryptography a critical focus for businesses and governments alike.

In 2025, I believe organizations should prioritize understanding and adopting post-quantum cryptographic algorithms to future-proof their data. Look for partnerships between quantum hardware providers and cybersecurity firms aimed at developing robust encryption methods.

Beyond security, quantum technology's advancements will influence industries such as renewable energy, drug discovery, and supply chain optimization. For example, quantum simulations will accelerate breakthroughs in battery technologies and renewable energy systems, key to achieving global sustainability goals. Businesses in these sectors should be prepared to integrate quantum-powered solutions as they become commercially viable.

Another trend to keep an eye out for is the rise of neutral-atom quantum computing. This approach not only promises scalable performance but also a smaller ecological footprint compared to traditional quantum systems. As the tech industry grapples with sustainability challenges, neutral-atom computing's energy efficiency could make it a preferred choice.

JOHN PRISCO, TOSHIBA CONSULTANT AND CEO OF QUANTUM SAFE

As we approach 2025, the quantum technology industry is on the cusp of transformative breakthroughs. It's crucial to highlight technologies that can address the growing cyber risks of tomorrow. Quantum Key Distribution (QKD) offers a vital layer of protection in a world where there's a surge of data breaches and cyber attacks. It's estimated that one cybersecurity attack occurs every 39 seconds, according to recent data.

That's why quantum-safe cryptography must become a priority in 2025. By adopting QKD, organizations can not only secure their communications today but also safeguard them against the emerging threats of quantum computing. This can be done by establishing encryption protocols that are safe from quantum attacks and by partnering with QKD service providers. Typically, a phased approach is recommended, which involves securing critical communication channels first and then gradually expanding the security measures to cover the broader IT infrastructure.

Additionally, quantum computer development will focus on error correction, thus creating logical qubits instead of simply adding non-corrected qubits like in previous years. This approach will eventually lead to

cryptographically relevant quantum computers which will demand quantum protection provided by QKD and PQC.

Lastly, QKD is a strong tool for protecting sensitive communications in industries such as finance, healthcare, and government. It ensures that any attempt to intercept the key will alter the quantum state and be instantly detectable. This makes QKD a powerful method for safeguarding sensitive communications and can help organizations future-proof their cybersecurity strategies and reduce the risks posed by quantum-enabled cyber threats.

KURT THOMAS, SENIOR SYSTEM ENGINEER AT FORTRA

Adoption of the new NIST-approved encryption algorithms for post-quantum cryptography for data in transit has started and will slowly climb in 2025, starting first in the especially risk-aware sectors like defense and finance. This will reduce the risk of harvest-now-decrypt-later attacks on confidential data.

DR. AVESTA HOJJATI, VP OF ENGINEERING AT DIGICERT

Last year, we predicted that ongoing advances in quantum computing would motivate executives to learn more about its risks and accelerate their investments in post-quantum cryptography (PQC). We predict that 2025 will be the year that PQC takes a major leap forward, from abstract line items on IT roadmaps to deployed operational solutions.

We're already seeing the first steps toward putting PQC into play. The U.S. National Security Agency (NSA) is expected to announce CNSA 2.0 algorithms for critical NSS networks. We predict adoption of quantum-resistant cryptography will grow, with advanced encryption becoming available in hardware security modules (HSMs) and applications.

As its adoption accelerates, PQC will also evolve to become a regulatory compliance imperative. Global organizations have acknowledged the need for a quantum-secure economy, and compliance standards and regulations are in process for financial services organizations as well as healthcare providers.

TODD MOORE, VICE PRESIDENT, DATA SECURITY PRODUCTS AT THALES

Post-Quantum Cryptography will spotlight crypto agility.

Earlier this year, NIST released its first sets of post-quantum encryption algorithms. Before these standards were released, many enterprises needed help grasping the need for PQC. NIST's standards have brought urgency to address the impact of quantum advancements and the need to address these threats. Even though the TLS and SSH protocols have been updated to meet NIST's new standards, NIST is already working on its next set of algorithms, meaning that the algorithms implemented today will be different by the time the threat of quantum computing arrives. This points to the importance of crypto agility in adapting to these evolving security recommendations.

While TLS and SSH protocols are being updated to meet NIST's standards, enterprises will need to embrace crypto agility in 2025. The biggest barrier will be ensuring they have the time and resources to identify their exposure, take inventory of their assets, and employ crypto discovery. This will manifest in a steady rise of crypto centers of excellence among major enterprises. Enterprises must place agility at the center of their quantum readiness, ensuring crypto-agile solutions are leveraged to keep pace with emerging quantum-resistant cryptography.

BILL WISOTSKY, PRINCIPAL TECHNICAL ARCHITECT, SAS

Quantum computing is set to make significant advancements in error mitigation and correction, substantially increasing the number of computational qubits. This progress will continue to revolutionize the data and AI industry. The fields of quantum machine learning, quantum optimization, and quantum chemistry and biology stand to benefit the most.

Quantum computing will also advance in its hybrid development, with Quantum Processing Units (QPUs) being further integrated with CPUs, GPUs, and LPUs. QPUs will be employed for specialized problem classes or formulations. This hybridization will inspire new approaches to classical algorithms, leading to the development of superior quantum-inspired classical algorithms. Looking ahead, investing in quantum computers promises once-in-a-century breakthroughs, unlocking unprecedented solutions and discoveries in science and physics, akin to the impact of electricity.

TOMAS GUSTAVSSON, CHIEF PKI OFFICER, KEYFACTOR

The National Institute of Standards and Technology (NIST) recently released its initial public draft of a post-quantum cryptography (PQC) timeline – a huge milestone that will have massive influence in the next several years. With this new development, NIST has established a clear timeline for organizations to transition away from RSA and ECC, answering one of the most common questions around PQC, with expectations that other compliance frameworks will soon align with this guidance. For example, Federal Information Processing Standards (FIPS) are U.S. government-issued guidelines for ensuring security and interoperability in computer systems used by federal agencies and contractors, ranging across a variety of sectors including like the financial industry, telecom, automotive, manufacturing, rail, etc. Therefore, every sector and business must consider these timelines, and it is impossible to ignore them.

Given that previous transitions, like SHA-1 to SHA-2, took over a decade, starting early is essential as the timeframe for PQC adoption is much shorter. With real, tangible deadlines to work against, organizations can't afford to postpone their journeys to quantum-resiliency. They must take action now to ensure their systems comply with standards, which will aid in managing the migration of legacy systems and the development of new ones.

2. "Impossible" success: Quantum teleportation on normal internet cables is set to change the world

by Eric Ralls
https://www.earth.com/news/quantum-teleportation-communication-achieved-on-regular-internet-cables/

Northwestern University engineers made a remarkable advance in quantum computing and communication, demonstrating quantum teleportation over a standard fiber optic cable that already carries everyday Internet traffic.

This development shows that quantum communication might not require dedicated lines, which clears the path for easier and more widespread integration of quantum and classical data sharing.

Path for quantum networking

The news centers around the idea that quantum signals – information carried by delicate particles of light known as photons – can travel alongside everyday Internet traffic without losing their integrity.

This breakthrough demonstrates quantum teleportation, a process where the state of a particle (like a photon) is transferred to another distant particle without the initial particle moving physically.

Science behind quantum teleportation

By using entangled photons, this method enables secure, near-instantaneous data sharing and paves the way for future quantum networks.

The research team successfully tested a setup that allows quantum information to weave through the bustling flow of regular Internet data without interference.

This achievement overcomes one of the biggest hurdles in making quantum networks a practical reality.

Prem Kumar, who oversaw the research, is a professor of electrical and computer engineering at Northwestern's McCormick School of Engineering.

He is known for his contributions to quantum communication and serves as the director of the Center for Photonic Communication and Computing.

In their recent work, Kumar and his collaborators introduce a new way of thinking about quantum signals alongside their classical counterparts.

Entanglement in quantum communication

Quantum teleportation stands out because it uses entanglement as a way to exchange information without physically sending matter across a distance. The concept traces back to Einstein, Podolsky, and Rosen in 1935.

Scientists have since tested quantum entanglement in labs, culminating in the formal proposal for quantum teleportation in 1993.

One of the biggest appeals of quantum teleportation is that it can occur almost as fast as light travels. Photons can become entangled so that performing a measurement on one instantaneously affects its partner, no matter how far away it is.

"This is incredibly exciting because nobody thought it was possible; our work shows a path towards next-generation quantum and classical networks sharing a unified fiberoptic infrastructure. Basically, it opens the door to pushing quantum communications to the next level," enthused Kumar.

Protecting delicate photons

Securing a clear route for single photons involves more than just adding them to an active cable. Ordinary Internet traffic typically relies on millions of light particles, so a handful of quantum photons can easily get lost or overwhelmed.

The Northwestern team performed detailed studies on how light scatters inside the cable to see if there was a specific wavelength that experiences less clutter.

They pinpointed that sweet spot and added special filters to reduce the noise generated by normal data traffic.

"Quantum teleportation has the ability to provide quantum connectivity securely between geographically distant nodes," said Kumar.

Past work suggested that large-scale quantum networks might need specialized systems. Now, his findings reveal that this might not be strictly necessary, if signals are positioned in just the right place in the spectrum.

First test run in busy channels

Earlier demonstrations of quantum teleportation typically involved pristine settings or dedicated fibers.

Some researchers believed that real-world cables, teeming with signals, would smother the faint quantum light. That assumption has been proven wrong.

In tests at Northwestern, the researchers ran quantum signals and classical communications over the same fiber optic cable without them colliding.

They measured how well the quantum information arrived at its destination and confirmed that it was still correct at the other end.

"Our work shows a path towards next-generation quantum and classical networks," Kumar summarized.

Real-world infrastructure

The immediate plan is to scale the system to longer runs and then transition to underground fiber connections.

The group believes that an eventual shift to real-world cables could be next. Building on single-pair teleportation, they also want to experiment with multiple pairs of entangled photons to achieve another crucial step known as entanglement swapping.

If that milestone is reached, quantum networks could begin to take shape across regions rather than only between two points.

For critical operations in finance, defense, and data management, such networks could offer more secure connections thanks to the inherent secrecy of quantum methods, where any tampering is immediately noticeable.

Broader applications

The capacity to support quantum connections without setting up special cables makes many new ideas more viable.

Distributed quantum computing, which relies on linking multiple quantum computers in different locations, would be simpler to establish.

Distance-sensing tasks and advanced metrology could also benefit from more stable quantum links.

Even beyond computing, quantum networks have the potential to spur new technologies in encryption, imaging, and fundamental physics experiments.Researchers have also discussed using quantum entanglement to synchronize distant clocks or to share random numbers for cryptography at unprecedented levels of security.

Significance of quantum teleportation

Quantum teleportation has matured from a fascinating theory to a tool that is becoming more practical.

While it is never straightforward to integrate delicate quantum signals, the Northwestern group's accomplishment raises confidence that such integration is within reach.

Many experts have believed that building specialized infrastructure was an unavoidable cost of quantum networking. According to Kumar's report, if wavelengths are picked carefully, classical signals and quantum information can coexist just fine. This line of thinking spares organizations from installing entire new grids of cables.Future work on quantum teleportation

In upcoming work, the researchers plan to expand the scope of their approach in longer segments to confirm that the method remains stable as cables stretch far past the lab. They will also design a multi-node demonstration to verify it can handle more than a single link. There is much excitement that existing communication channels, once tuned just right, could carry quantum data to distant points.

With such possibilities on the horizon, quantum teleportation may shift from a theoretical concept to a tool that transforms communication.

The future might see quantum and classical networks working side by side in ways that once sounded unlikely.

3. This Cryptographer Helps Quantum-Proof the Internet

by EDD GENT
https://spectrum.ieee.org/post-quantum-cryptography-2670649921

Users of Google's Chrome browser can rest easy knowing that their surfing is secure, thanks in part to cryptographer Joppe Bos. He's coauthor of a quantum-secure encryption algorithm that was adopted as a standard by the U.S. National Institute of Standards and Technology (NIST) in August and is already being implemented in a wide range of technology products, including Chrome.

Rapid advances in quantum computing have stoked fears that future devices may be able to break the encryption used by most modern technology. These approaches to encryption typically rely on mathematical puzzles that are too complex for classical computers to crack. But quantum computers can exploit quantum phenomena like superposition and entanglement to compute these problems much faster, and a powerful enough machine should be able to break current encryption.

That's why in 2016 NIST launched a competition looking for new encryption approaches resistant to quantum computers. In 2022, the agency announced the first round of winners, which included the CRYSTALS-Kyber scheme coauthored by Bos, who is technical lead of the post-quantum cryptography team at NXP Semiconductors in Leuven, Belgium.

Today, Bos is focused on integrating the algorithm into NXP's portfolio of embedded hardware products, which includes chips for credit cards, contactless payment terminals, Internet of Things devices, and cars.

As someone who loves solving puzzles, Bos was well suited to a career in cryptography, he says. The fact that he can help make the world a safer place while doing something he enjoys is a massive bonus.

"If doing this research was practically useless, I would probably still do it," he says. "But it's super cool that you can work on interesting math puzzles, and then, in the end, it will have a very positive impact on everybody around you."

Discovering Cryptography

Bos grew up in a small town close to Haarlem in the Netherlands and was fortunate to have an early introduction to technology. His father worked at a bank and had a desktop computer at home. Bos started using it to play video games but became fascinated by the underlying technology and quickly picked up coding skills. By the age of 15, he was already doing freelance programming jobs for various companies.

In high school, he learned about more formal computer science topics, such as algorithms and computational complexity. He found these subjects fascinating and in 2001 enrolled at the University of Amsterdam to pursue a bachelor's degree in computer science. After graduating in 2004, he stayed on to get a master's degree in grid computing, which he completed in 2006.

While working on his master's, Bos says he found himself drifting toward algorithm design and more math-heavy computer science, but he was also eager to continue working on practical problems. Then he discovered cryptography, which bridges his interests. "It's really at the intersection of engineering, computer science, and mathematics," he says.

This realization prompted Bos to apply for a Ph.D. program in the lab of renowned cryptographer Arjen Lenstra at the École Polytechnique Fédérale de Lausanne in Switzerland. Bos was accepted and started in 2007, just as the lab began investigating the use of unconventional hardware—such as gaming consoles—to do cryptanalysis, the process of breaking encryption.

His Ph.D. project involved building a cluster of more than 200 PlayStation 3 consoles and using it to crack a popular encryption scheme based on the mathematics of elliptic curves. The consoles' multicore processors used the Cell architecture developed by IBM, Sony, and Toshiba, which was well suited to running lots of computing processes in parallel, as is required in cryptanalysis.

Learning About Lattices

During his Ph.D. studies, Bos worked on a summer project with another acclaimed researcher, Peter Montgomery, who was at Microsoft Research at the time. The pair clicked, says Bos, and he was invited to become a postdoctoral researcher in Montgomery's lab in Redmond, Wash., after completing his Ph.D. in 2012.

Shifting from academia to corporate R&D was an invaluable experience, says Bos, as he got to see how research is translated into real-world products. "That was really motivating," he says. "If you design a cool algorithm, it could end up in the crypto library of Microsoft, which then gets used by hundreds of millions of people worldwide."

While at Microsoft, Bos began working on an emerging approach known as lattice-based cryptography, which depends on the mathematics of vectors in a grid. These schemes were promising because they could be used for both quantum-secure encryption and fully homomorphic encryption, a technique that makes it possible to carry out computations on encrypted data without first decoding it.

But after two years in the United States, Bos and his wife wanted to be closer to home. So in 2014, he took a job as a cryptography researcher at NXP and moved to Belgium. He joined the company's innovation team, which comes up with features for products several years down the company's product road map.

By then, advances in quantum computing made it clear that more secure encryption approaches would be important, says Bos. So working in collaboration with researchers from Arm, IBM, SRI International, and various universities, he helped design the lattice-based CRYSTALS-Kyber encryption scheme, which was submitted to NIST in 2017.

From Cryptography Research to Products

Since then, Bos has focused on implementing the algorithm in NXP's embedded hardware. Lattice-based encryption requires considerably more memory than older approaches do, which makes it tricky to run on smaller chips like those found in ID cards or IoT sensors. His team had to make changes to the underlying mathematics of the algorithm and redesign it to run on these specialized chips.

Bos says his job has evolved significantly over the years. He's gone from conducting pure research to leading a team and collaborating closely with other departments to translate their innovations into actual products. He had to work hard to develop the skills to act as an interface between engineers and business-focused teams, he says.

Being team leader is a high-pressure role, he says, because NXP has to stay ahead of the curve when it comes to post-quantum encryption. The chips it designs are used at the start of a long supply chain, he explains, as they have to be integrated into larger systems made by component manufacturers. Those

systems are then sold to device makers or automotive companies that have to integrate them into the final products.

Each of those steps can take years, says Bos. That means NXP's chips need to be quantum secure *now* so that the end users can meet government-recommended deadlines to migrate to post-quantum encryption by the early-2030s.

A Friendly Field

One of the things Bos likes the most about cryptography is that the field is relatively small and welcoming. "Everybody's super friendly," he says. "If you go to a crypto conference, the big names, the folks who really invented crypto in the '70s, they still come to these events and you can meet them in person."

The size of the field also means cryptography experts are in short supply, Bos adds, so it's a discipline with great career prospects. While many roles require strong math skills, there are plenty of opportunities for those with a more conventional computer science background, and companies are always looking for electrical engineers to build cryptographic hardware.

A postgraduate degree in one of those fields is a bonus, but companies like NXP do a lot of internal training so it's not strictly necessary, Bos says. Taking cryptography or security courses online or while at university can be a great differentiator, he adds. But most important is the right attitude. "You just need to be motivated and curious and willing to learn," says Bos. "I think these are really the biggest factors."

4. Using Shorter Public Certificate Lifespans to Prepare for Post-Quantum Cryptography

by Kevin Bocek
https://www.infosecurity-magazine.com/opinions/public-certificate-post-quantum/

The cybersecurity industry is about to face two major changes in the machine identity world. Within the next 6–12 months, both Google and Apple will cut the lifespan of public TLS certificates to 90 days or less, with Apple proposing further reductions to 47 days by 2028.

In the longer-term, post-quantum cryptography (PQC) looms large. A generational change in the digital world that will takes years to play out and impact the most foundational parts of the digital world: it's almost certain quantum computers will be able to break today's cryptography and allow attackers to spoof machine identities, decrypt data and make ransomware run.

Given the scale of these challenges, security leaders are rightly concerned. Three quarters (74%) say that Google's plans will cause chaos, whilst 67% dread the day their board asks them about PQC. But, without having exact timelines for either, these may seem like problems that can be kicked down the road.

Organizations should be preparing now, and while these two initiatives may seem disparate, they have more in common than meets the eye. In fact, preparing for shorter public certificate lifespans is a crucial first step in being quantum-ready.

The Good, the Bad and the Unprecedented

Positively, both of these developments will improve security. Google and Apple's intended changes to certificate lifespans will help to lessen the amount of time an adversary has to take advantage of a compromised certificate. PQC will raise the bar, revolutionizing encryption so that machine identities remain secure once powerful quantum computers are in adversaries' hands.

However, the transition to new standards of machine identity security could cause short-term pain for those who are unprepared. Every business with a website uses public TLS certificates and will be impacted by shorter lifespans. To adjust to Google's 90-day certificates, organizations will need to replace TLS certificates five-times as often as they do now. Apple's 47-day certificates will need to be replaced almost 10-times as often.

This presents a greater chance that a certificate will expire before being replaced – which could result in a costly outages. Although not certificate-related, the July 2024 CrowdStrike outage gave us a taste of how damaging these incidents can be, and if organizations aren't prepared, similar scenarios could occur daily.

Failing to prepare for PQC could have an even more devastating impact. If a quantum computer capable of cracking encryption is created, then the world will be turned upside down – nothing will be secure. Organizations will be at the mercy of adversaries, who'll be able to crack machines open in the blink of an eye. All data across the entirety of the internet will be at risk.

Worst of all, we do not know when this may happen, organizations may have the act very fast to migrate to new encryption standards.

There have been instances in the past – such as the infamous Heartbleed vulnerability in 2014 – where it's been necessary for organizations to replace all their machine identities. But it's never been on this scale. The emergence of cloud native solutions and technologies like AI mean organizations have many thousands more identities in use than ever.

Each and every identity, of which there are thousands or even hundreds of thousands in an enterprise's system, will be a potential point of failure if they're not managed and secured adequately.

Preparing for the Future Today with a Business Case

To avoid costly outages and devastating cyber-attacks, organizations need to know where all of their machine identities are, what they're used for, when they're set to expire and have the ability to swap them

rapidly before they trigger an outage or cyber-attack. But, managing and securing all the machine identities across an organization manually is impossible, particularly if they're expiring five-times faster or are infinitely more complex.

Not only is this laborious process time consuming and unreliable, but it runs the risk of human error. When the stakes are so high, it's simply not acceptable to leave machine identity security to chance.

Therefore, organizations must use automation to solve this complex problem. This empowers security leaders to take control over their machine identities. In the short term, automation will be vital towards preparing organizations for reduced public certificate lifespans, ensuring no machine identities ever slip through the cracks, avoiding the ensuing outage.

In the long term, organizations will need to go through the exact same process of discovery and replacement of machine identities for PQC. Preparing for shorter public certificate lifespans today will future-proof organizations for what's coming tomorrow.

Getting Ahead While We Can

The scale of the task posed by Google and Apple's plans for shorter public certificate lifespans and PQC is unprecedented, and without automation, there'll be chaos in the machine. While these challenges aren't happening tomorrow, they are coming.

The good news is that now is the time for security leaders to make machine identity security urgent in order to protect their organizations and the customers they serve from emerging threats.

Those that do take the necessary steps to automating machine identity security will be well-placed to tackle 90-day certificates and PQC head on. Those that don't could be left facing daily outages and will leave themselves powerless to repel cyber-attacks.

5. How Quantum Computing Is Reshaping Cryptography

by Kapil Kondam
https://itmunch.com/quantum-computing-reshaping-cryptography/

Introduction

Quantum computing is poised to revolutionize various fields, with cryptography standing out as a domain especially vulnerable to its advancements. By leveraging the principles of quantum mechanics, quantum computers can perform calculations at unprecedented speeds, fundamentally altering how data security is

approached. As classical methods of encryption face significant threats from quantum algorithms, understanding the implications of this shift becomes imperative for organizations relying on data integrity and security. This article delves into the relationship between quantum computing and cryptography, highlighting the risks and emerging solutions that promise a secure digital future.

1. Introduction to Quantum Computing and Cryptography

Quantum computing employs quantum bits, or qubits, which differ radically from classical bits. While classical bits can only be in a state of either 0 or 1, qubits can exist in multiple states simultaneously due to the phenomenon of superposition. This unique property enables quantum computers to carry out complex computations more efficiently than traditional systems, thus presenting a formidable advantage in processing power. Algorithms such as Grover's and Shor's highlight this potential, raising concerns about existing security practices.

Classical cryptography encompasses various algorithms, including RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography), and AES (Advanced Encryption Standard). These encryption standards depend on the mathematical difficulty of certain problems, such as factoring large numbers or solving discrete logarithms, to ensure data security. However, as quantum technology advances, the conventional mathematical foundations of cryptography become increasingly susceptible to rapid computation enabled by quantum algorithms.

The dual nature of quantum capabilities poses challenges and opportunities for the future of cryptography. On one hand, the ability of quantum computers to dismantle existing security protocols threatens organizations and individuals who rely on classical encryption methods. On the other hand, this technological evolution drives the development of quantum-resistant algorithms, potentially leading to a new era of secure communication. Understanding this dynamic can help professionals navigate the complexities of cybersecurity in a quantum computing landscape.

2. The Quantum Threat to Classical Cryptography

The emergence of quantum computing presents a direct threat to classical cryptographic protocols that have underpinned secure communication for decades. Shor's algorithm, which efficiently factors large integers, poses a significant challenge to widely used encryption techniques such as RSA. For instance, while breaking RSA encryption with classical computers would require an astronomical amount of time, a sufficiently advanced quantum computer could achieve this in a matter of minutes or seconds.

Similarly, ECC, which relies on the mathematical difficulties associated with elliptic curves, is also vulnerable to Shor's algorithm. This vulnerability underscores the urgency for organizations to reassess their security protocols, particularly in industries such as finance and government where sensitive data is routinely transmitted and stored. The implications of an effective quantum attack on these systems are dire, potentially leading to widespread data breaches and loss of privacy.

Even symmetric key algorithms like AES, although somewhat resistant to quantum attacks, are not invulnerable. Grover's algorithm can effectively reduce the security of symmetric encryption by halving the effective key length, prompting a need for longer keys to maintain a comparable level of security. This shifting threat landscape necessitates proactive measures to transition towards quantum-resistant protocols, making it crucial for industries to consider the short and long-term implications of quantum computing on their cryptographic practices.

3. Understanding Post-Quantum Cryptography

Given the challenges presented by quantum computing, researchers are focusing on advancing post-quantum cryptography (PQC). PQC encompasses a range of cryptographic algorithms designed to resist the vulnerabilities introduced by quantum computing. These algorithms rely on mathematical problems deemed to be hard for both classical and quantum computers, ensuring the integrity of sensitive data even in a quantum environment.

Various PQC candidates have emerged, focusing on diverse mathematical structures such as lattice-based cryptography, hash-based signatures, and multivariate polynomial cryptography. For example, lattice-based cryptographic algorithms like NTRU and Learning With Errors (LWE) provide robust security foundations against potential quantum attacks. These methods are currently being evaluated and standardized to replace insecure classical algorithms, reflecting an essential phase in the ongoing battle for secure data encryption.

The transition to PQC is not merely an academic exercise but a critical reality for organizations seeking to protect their assets. As evidenced by ongoing initiatives from organizations such as the National Institute of Standards and Technology (NIST), a global standardization for post-quantum algorithms is well underway. Ensuring compliance with these new standards will be vital for maintaining data security as quantum computing becomes more accessible.

Conclusion:

Quantum computing undeniably reshapes the landscape of cryptography by posing significant threats to established encryption protocols while simultaneously inspiring the development of innovative solutions. Addressing the challenges posed by quantum capabilities necessitates a strategic embrace of post-quantum cryptography to safeguard the integrity of sensitive data. As organizations increasingly prepare for a quantum future, the need for a proactive approach to security is more critical than ever.

Top 5 FAQs About How Quantum Computing Is Reshaping Cryptography

What is quantum computing?

Quantum computing harnesses the principles of quantum mechanics, utilizing qubits that can exist in multiple states simultaneously. This capability vastly increases processing power and efficiency over classical computers, enabling faster computations for complex problems.

How does quantum computing threaten classical cryptography?

Quantum computing poses a significant risk to classical cryptographic methods like RSA and ECC due to algorithms such as Shor's, which can efficiently factor large integers and compute discrete logarithms. This effectiveness undermines the foundational security principles of these protocols.

What is post-quantum cryptography?

Post-quantum cryptography (PQC) involves developing cryptographic algorithms that are secure against the potential threats posed by quantum computing. These algorithms focus on difficult mathematical problems that remain challenging for both quantum and classical computers.

Are symmetric encryption algorithms like AES safe against quantum attacks?

While symmetric encryption methods such as AES are more resilient than asymmetric algorithms, they are not entirely secure. Grover's algorithm can reduce the effective key length by half, necessitating longer keys to maintain equivalent security levels.

What actions should organizations take to prepare for quantum computing?

Organizations need to transition to post-quantum cryptographic protocols, assess their existing cryptographic practices, and stay informed about developments in quantum technology. Emphasizing education and strategic planning will be crucial to mitigate risks and safeguard data integrity.

6. Cryptographic protocol enables secure data sharing in floating wind energy sector

by IMDEA Networks Institute
https://techxplore.com/news/2024-12-cryptographic-protocol-enables-energy-sector.html

Floating wind power offers enormous potential for deepwater offshore energy development. However, the management and secure exchange of data between stakeholders represents a key challenge for its evolution.

A new cryptographic framework, proposed by researchers Claudia Bartoli (IMDEA Software) and Irene Rivera-Arreba (Norwegian University of Science and Technology, NTNU), presented at WindTech 2024 Conference, tries to solve this problem with a data sharing scheme that guarantees data integrity without

compromising privacy. This breakthrough seeks to foster collaboration between industries and academia, driving innovation in floating wind technologies.

Floating wind power is positioned as a promising frontier in the renewable energy sector, enabling the expansion of offshore wind power to areas of greater depth. To harness this potential, it is essential to share reliable data between parties such as companies and academics.

Access to datasets is crucial at all stages of development, from site selection to maintenance. In addition, sharing data fosters innovation, attracts investment and strengthens trust among stakeholders. However, handling large volumes of data and protecting intellectual property pose significant challenges.

The current approach relies on data certified by certification bodies, but these often lack critical details to optimize system performance. In response, the researchers have described a cryptographic protocol that enables the secure exchange of critical data, ensuring privacy and integrity through advanced tools such as zero-knowledge proofs.

The protocol proposed by Bartoli and Rivera-Arreba has been designed to facilitate interactions between the various parties involved in offshore wind energy development. It has the potential to transform data sharing in the wind energy sector, improving collaboration between industry and academia since it ensures data integrity between parties without disclosing additional information.

With the implementation of this protocol, "Through the use of techniques such as Multi Party Computation (MPC), this approach allows the analysis of encrypted data, ensuring the confidentiality of the information while sharing the results obtained by such analysis" assures Claudia, lead researcher of the article.

In addition, the system incorporates cryptographic signatures and succinct commitment schemes to reduce costs and facilitate the management of large databases. These innovations open up new possibilities to overcome current limitations in data availability without compromising data privacy.

The implementation of this cryptographic protocol could mark a step forward in the development of floating wind power. By enabling the confidential exchange of data, it fosters innovation and contributes to bridging the gap between privacy and availability.

This breakthrough represents a promising solution to address technological and regulatory challenges on the road to a sustainable future in the renewable energy sector and paves the way for future research in this regard.

7. 2024: The Year of Quantum Computing Roadmaps

by GQI

https://quantumcomputingreport.com/2024-the-year-of-quantum-computing-roadmaps/

2024 has seen an unprecedented wave of quantum computing roadmaps, with thirteen players either announcing new development paths or significantly updating existing ones. Never before has the industry seen such a concentrated period of concrete technical commitments and public timelines, marking a shift from general promises to specific, measurable goals.

Recent Roadmap Announcements

The following list summarizes this year's developments:

New Roadmaps

- QuEra Computing (January 2024): Three-year roadmap through 2026, targeting 100 logical qubits.
- Infleqtion (February 2024): Four-year roadmap through 2028, planning for over 100 logical qubits with 40,000 physical qubits.
- Pasqal (March 2024): Five-year roadmap through 2028+, targeting fault-tolerant quantum computing with 128 logical qubits.
- Riverlane (July 2024): Through 2026, focused on error correction technology targeting 1 million QuOps.
- Quantinuum (September 2024): Five-year roadmap through 2029, culminating in the Apollo processor with hundreds of logical qubits.
- Quandela (October 2024): Six-year roadmap through 2030, focusing on achieving fault tolerance using spin-optical quantum computing.
- IQM (November 2024): Six-year roadmap through 2030 with plans to scale to 1 million physical qubits and thousands of logical qubits.
- Alice & Bob (December 2024): Five-year roadmap through 2030, aiming for 100 logical qubits.

Adjusted Roadmaps

- Microsoft (H2 2023) (we include it for completeness): Unveiled a six-stage roadmap toward a quantum supercomputer, focusing on topological qubits with a goal of achieving 1 million rQOPS and 10^-12 logical error rates.
- D-Wave (July 2024): Enhanced focus on quantum AI and machine learning applications.

- IonQ (July 2024): Accelerated timeline targeting 99.999% logical two-qubit gate fidelity by 2025.
- IBM (November 2024): Continued execution of existing roadmap with significant runtime performance improvements and new technical milestones.
- Google (December 2024): Updated Milestone 3 target following Willow's below-threshold demonstration, aiming to achieve 10^-6 logical error rates with 1,500 physical qubits.

Strategic Expansion

- PsiQuantum (April 2024): While not a traditional roadmap, announced a landmark AU$940 million (US$620M) project to deliver a 1-million physical qubit system in Brisbane, Australia by 2027, representing one of the most ambitious quantum computing goals announced to date.

Key Performance Indicators for Quantum Computing Progress

Studying the announced roadmaps it can be observed that the industry has coalesced around several standardized metrics to track quantum computing progress. At the physical layer, two-qubit gate fidelity serves as a fundamental benchmark, with leading platforms now targeting the 99.9% to 99.99% range. Error rates are typically measured at both the physical and logical level, with logical error rate targets extending to 10^-6 or better. System performance is increasingly measured through operational metrics like Circuit Layer Operations Per Second (CLOPS), maximum circuit depth (number of sequential gate operations possible), and quantum volume. For error-corrected systems, the ratio of physical to logical qubits (often called the overhead factor) has become a critical metric, alongside the achievable logical operation rate measured in QuOps (Quantum Operations per second). Additional technical parameters include coherence times, gate speeds, mid-circuit measurement capabilities, qubit connectivity (average number of direct connections per qubit), and system cycle times. For scaled systems, interconnect performance metrics such as coupling fidelity, connection speed, and maximum distance are becoming increasingly important benchmarks.

A New Era of Accountability

What makes these 2024 roadmap announcements particularly significant is their level of technical detail and specific performance targets. This transparency creates a new framework for accountability in several ways:

1. **Quantifiable Progress:** Instead of vague promises of "quantum advantage," companies are now committing to specific numbers for error rates, qubit counts, and operational metrics.
2. **Technical Transparency:** The inclusion of architectural details and specific implementation strategies allows for better evaluation of the feasibility of these roadmaps.

3. **Time-Bound Commitments:** Most roadmaps now include specific yearly milestones through 2025-2030, creating clear checkpoints for progress assessment.

The next five years (2024-2029) will be crucial for the quantum computing industry. With these detailed roadmaps now public, the industry has entered what could be called an "era of delivery." Success or failure will no longer be judged on incremental progress or isolated demonstrations, but on the ability to meet these published technical milestones on schedule. This new accountability framework will likely accelerate both technology development and industry consolidation, as it becomes clear which approaches are successfully meeting their stated goals.

How to evaluate published roadmaps – GQI's take

In our recent report "The Road to Shor Era Quantum Computing," published December 6th, 2024 in partnership with NATO Innovation Fund, GQI presents an updated framework for evaluating quantum computing roadmaps. We combine two key assessment tools: the GQI Hardware Stack, which examines technical progress across different components of quantum systems, and Secondary Competitive Differentiators, which analyze practical aspects like cost and operational efficiency.

For the unprecedented wave of 2024 roadmap announcements, we've enhanced our evaluation framework to focus on three fundamental challenges that must be overcome before quantum computing reaches its "Sputnik moment":

1) achieving reliable error suppression through scalable error correction,
2) building universal fault-tolerant circuits that operate at practical speeds, and
3) demonstrating that platforms can scale to commercially useful sizes.

This enhanced framework specifically evaluates each company's roadmap against their capability to eventually build a cryptographically relevant quantum computer (CRQC) – one powerful enough to break RSA 2048 encryption within a day.

8. Turkcell and Nokia Trial Quantum-Safe Cryptography for Mobile Networks

by SRIKAPARDHI
https://telecomtalk.info/turkcell-nokia-trial-quantum-safe-cryptography-mobile/986638/

Turkcell and Nokia have demonstrated quantum-safe IPsec network cryptography for mobile subscribers. This achievement enhances mobile network security against the evolving threat of quantum computing, which could render traditional cryptography methods vulnerable. **Nokia** calls the demonstration a world-first ability, marking a critical step in securing mobile networks against future threats posed by quantum computing.

Quantum-Safe Cryptography

As quantum computers advance, conventional cryptographic protections may be compromised, making it essential for networks to evolve. The demonstration was conducted with Nokia's IPsec Security Gateway, which integrated quantum-safe cryptography into Turkcell's mobile transport network, **Nokia** explained.

Securing Networks for the Future

By implementing advanced cryptography techniques now, both Nokia and Turkcell are ensuring their networks are secure today while also preparing for future advancements in technology.

Turkcell Chief Network Technologies Officer said: "As part of our strategy to continually enhance the security of our mobile network, this collaboration with Nokia provides us with the confidence that our transport security can withstand the challenges of the quantum era. By demonstrating these quantum-safe cryptography capabilities today, we are preparing our network for the future."

Senior Vice President of Network Infrastructure Europe at Nokia said: "This initiative is part of our ongoing commitment to safeguard the privacy and integrity of mobile technology. Our solutions provide a proactive defense-in-depth crypto-resilient approach against future network security challenges, ensuring that Turkcell's network remains secure for years to come."

Ensuring Future-Proof Mobile Security

For end users, this means continued confidence in the security of their mobile communications. They can be assured that their data will remain protected not just in the present, but also as the landscape of technology evolves over time, the companies said in a statement on December 20.

9. Here's why it's important to build long-term cryptographic resilience

by Michele Mosca and **Donna Dodson**
https://www.weforum.org/stories/2024/12/cryptographic-resilience-build-cybersecurity-nist/#:~:text=By%20embracing%20the%20long%2Dterm,on%20in%20the%20short%2Dterm.

The UN has proclaimed 2025 to be the International Year of Quantum Science and Technology. With increased qubit counts, improvements in error correction and cloud access to quantum platforms, we saw many practical gains in quantum computing in 2024. As progress accelerates, industries are exploring applications where quantum computing can solve challenges beyond the capabilities of advanced classical computers and AI, such as modeling complex molecular interactions.

While quantum computing promises many benefits, its rapid advancement also poses a significant threat to the current cryptographic applications and infrastructures upon which the global economy relies.

As we stand on the brink of a quantum revolution, the urgent need to migrate our cryptographic infrastructure to a quantum-safe framework has never been more critical to ensure the security, privacy and availability of global digital communications.

Cryptography is an indispensable cybersecurity control providing confidentiality and integrity for information, systems and communications. In the 1990s, public key cryptography revolutionized our digital infrastructure by enabling secure and confidential communication over the internet, allowing for the safe exchange of information, digital signatures and the establishment of trust in online transactions without the need for a shared secret key. Today, we rely on cryptography more than ever before. However, a sufficiently powerful quantum computer could render much of our traditional cryptography obsolete.

On August 13, 2024, the US National Institute of Standards and Technology (NIST) announced three post-quantum cryptography (PQC) standards designed to replace current public key standards. This announcement marked a significant first step toward achieving cryptographic security in the quantum age, following eight years of dedicated international collaboration.

While PQC is crucial for safeguarding our digital future, the real challenge lies in effective risk management and implementing a more robust, proactive approach to protecting data, systems and infrastructure from all evolving threats. AI and quantum computing significantly enhance the capabilities of malicious actors, exacerbating the challenge of maintaining secure cryptographic solutions. To create a resilient cryptographic framework for both the present and future, it is crucial to consider all quantum-safe technologies and develop solutions that promote agility and the principles of defence in depth.

Cryptographic agility implies the ability to quickly respond to an algorithm being broken by switching to an alternative with minimal disruption. Because PQC algorithms are relatively new, crypto-agility is a key pillar of resilience in the quantum age. But agility won't prevent losses and damage incurred before a break is detected and the switch is eventually made. The second pillar is a defence-in-depth approach, employing multiple security layers to prevent catastrophic outcomes should any one point of security fail. By implementing such a resilient cryptographic infrastructure, organizations can enhance their security posture, providing robust protection against a wide array of potential vulnerabilities. This strategy not only prepares organizations for the quantum future but also strengthens their defences against current and unforeseen challenges.

Many government entities and global businesses are advocating this multi-pronged approach. The US National Security Agency (NSA)'s Commercial Solution for Classified program specifies the use of symmetric key solutions using pre-shared keys as a substitute for or in conjunction with public key cryptographic solutions, especially when long-term data protection is required. The Monetary Authority of Singapore issued an advisory to financial institutions recommending that, in addition to PQC, they explore

complementary quantum-safe strategies such as Quantum Key Distribution (QKD). JPMorgan Chase and other organizations across critical industries are also pursuing such a dual-remediation strategy.

As highlighted in the joint statement by 18 EU nations, Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography, "organizations and governments should start the transition now." NIST has recognized that, historically, it has taken 10 to 20 years to fully implement cryptographic migrations. Compared to previous migrations, cryptographers worldwide have emphasized that transitioning to a quantum-safe infrastructure presents a far more complex challenge. Instead of merely swapping out algorithms, this transition requires revamping key management solutions, communication protocols, applications and systems that rely on or incorporate cryptography.

The stakes of a quantum-enabled cyber attack are potentially existential for businesses and exacerbated by the systemic nature of cryptographic vulnerabilities. It is imperative for senior business leaders to collectively champion the transition to a quantum-safe and resilient cryptographic infrastructure as a business requirement and empower their cybersecurity, IT, innovation and other teams to achieve it together. This strategic shift not only safeguards an organization's data and systems but also reinforces trust and confidence among customers and stakeholders. It also protects the organization from the risk of non-compliance as regulatory standards evolve. By taking ownership of this transition and working with technology experts to understand the organization's path to quantum safety, leaders can ensure that their businesses remain secure and resilient.

Because of the complexity of cryptographic migrations and the speed at which quantum computing is progressing, leaders must consider that they may not have an advanced warning of cryptographic failure. In April 2024, a paper was published purporting to have identified a vulnerability in lattice cryptography, a family of algorithms central to PQC. The claim was eventually disproved, but the possibility remains that unforeseen weaknesses in PQC could one day be exploited.

For that reason, business executives and security leaders must collaborate to probe the full extent of their resilience beyond merely adopting PQC algorithms and begin this process now. To guide this discovery phase, leaders should be asking:

- What are the implications for our organization if new PQC algorithms are broken without advanced warning?
- Do we have sufficient defence in depth so that short-term losses and disruptions would be survivable? Do we have alternative cryptographic capabilities to support our needs and protect our data?
- Do we have a recovery strategy that allows us to return to full operation in an acceptable amount of time?

Building a resilient cryptographic infrastructure and preparing for a world comprised of quantum computers and advanced AI is a long-term and ongoing endeavour requiring continual reassessment.

Executives must initiate this transition now to ensure preparedness for future challenges. By embracing the long-term imperative of building a resilient and quantum-safe cryptographic infrastructure, organizations can secure their operations and maintain trust with stakeholders in an evolving digital landscape they can more aggressively capitalize on in the short-term.

10. Post-quantum cryptography gains traction across sectors

by Shannon Williams
https://itbrief.com.au/story/post-quantum-cryptography-gains-traction-across-sectors

Insights from Keyfactor's leadership suggest significant shifts in data security practices are anticipated for 2025, particularly in response to advancements in quantum computing.

Ted Shorter, Chief Technology Officer at Keyfactor, predicts that post-quantum cryptography (PQC) will see increased adoption within highly regulated sectors such as government, finance, and telecommunications. "In 2025, highly regulated industries like government, finance, and telecommunications will lead the adoption of post-quantum cryptography (PQC) solutions to safeguard sensitive data and comply with stricter regulatory mandates," he stated. Shorter emphasised that industries handling sensitive data will be early adopters of PQC to protect critical infrastructure and maintain consumer trust. "As quantum computing advances, these sectors will face heightened risk to data security, prompting stricter regulatory mandates and early adoption of PQC," he added.

From the perspective of Tomas Gustavsson, Chief PKI Officer, organisations will need to prioritise agility in their encryption strategies to align with the shortened transition timelines set by the National Institute of Standards and Technology (NIST). "Organizations will prioritize agility in their 2025 encryption strategies, leveraging emerging post-quantum cryptographic (PQC) standards to prepare for the shortened transition timeline set by NIST," he commented. Gustavsson noted that as NIST progresses with finalising post-quantum cryptographic standards, companies face no option but to initiate the transition promptly, referring to past experiences where delays postponed cryptographic adaptations.

He further illustrated the significance of industries such as the Internet of Things (IoT) in adopting tailored quantum-safe solutions to counter evolving threats. "Industries such as IoT, with diverse use cases and unique security demands, will increasingly adopt tailored quantum-safe solutions to address evolving threats," he noted, indicating the disruptive innovation in cryptographic practices.

Ellen Boehm, Senior Vice President, IoT Strategy and Operations, stressed the importance of adopting proactive IoT security measures in 2025. As threats evolve with quantum computing advancements, robust IoT security practices become crucial. "In 2025, proactive IoT security practices and layered roots of trust will become critical for organizations to withstand escalating threats and regulatory pressures," she

explained. Boehm pointed out that organisations must reinforce their IoT security supply chains to preempt sophisticated threats, emphasising the importance of layered trust systems.

Moreover, the Cyber Resilience Act (CRA) is identified by Boehm as a significant motivator compelling developers and Original Equipment Manufacturers (OEMs) to embed security throughout the IoT device lifecycle. "From a product security perspective, developers and OEMs designing IoT devices will need to embed security at every stage of the product lifecycle, ensuring hardware and software integrity before devices even reach the market," Boehm highlighted. The CRA's stricter cybersecurity mandates necessitate such actions to mitigate regulatory and reputational risks.

11. SEALSQ and Hedera Collaborate to Develop Quantum-Resistant Semiconductors for Secure Post-Quantum Cryptography

by GQI
https://quantumcomputingreport.com/sealsq-and-hedera-collaborate-to-develop-quantum-resistant-semiconductors-for-secure-post-quantum-cryptography/

SEALSQ Corp has announced a strategic partnership with Hedera, a leading decentralized blockchain network, to create next-generation quantum-resistant semiconductors. This collaboration aims to integrate quantum-resistant security solutions into critical infrastructures, ensuring protection against the emerging risks posed by quantum computing.

The partnership will focus on SEALSQ's QS7001 quantum-resistant hardware platform, which is currently undergoing testing and validation ahead of its production launch in 2025. The quantum-resistant chips developed through this collaboration will safeguard digital infrastructure, including blockchain and cryptographic systems, from the potential vulnerabilities introduced by quantum computing.

As quantum computers advance, traditional cryptographic systems may become susceptible to attacks, particularly in tasks like integer factorization and discrete logarithms. SEALSQ's quantum-resistant hardware, along with Hedera's blockchain/distributed ledger technology (DLT), will help future-proof critical communication and transaction systems against these threats. SEALSQ's products, such as the QS7001 Open Platform and QVault Trusted Platform Module (TPM), are designed to integrate with Hedera's network, reinforcing long-term security standards.

This partnership represents a crucial step in the ongoing efforts to create quantum-secure infrastructures for industries reliant on digital transactions and data integrity. SEALSQ and Hedera's joint efforts will not only strengthen the security of current systems but also pave the way for more robust, future-proof technologies in a post-quantum world.

12. CISA: How post-quantum cryptography safeguards against quantum threats

by Dr Garfield Jones
https://www.innovationnewsnetwork.com/cisa-how-post-quantum-cryptography-safeguards-against-quantum-threats/54045/

The rise of quantum computing promises transformative advancements across industries, but it also introduces profound security challenges. At the heart of these concerns lies the vulnerability of our current cryptographic systems – frameworks that protect everything from personal data to critical infrastructure. As quantum technology advances, the encryption methods we rely on today could soon become obsolete, leaving sensitive information exposed to unprecedented risks.

Enter post-quantum cryptography, the field dedicated to developing cryptographic algorithms capable of withstanding the computational power of future quantum machines. This emerging discipline is not just a technical necessity but a critical frontier in the fight to safeguard global security. Governments, industries, and researchers are racing against time to ensure our digital infrastructure is ready for a post-quantum world.

In this interview, CISA's Dr Jones delves into the pivotal role of post-quantum cryptography in securing the digital landscape. From addressing vulnerabilities in public key infrastructure (PKI) to the efforts being led by global and national organisations, the conversation focuses on what it will take to protect our systems in an era defined by quantum innovation. As the quantum revolution accelerates, understanding and adopting these next-generation solutions is more crucial than ever.

As quantum computing advances, what potential security issues does the technology pose?

This is a question we get quite frequently. The primary risk we're looking at is authentication. When we consider cryptographic vulnerabilities, the most significant threat is to authentication mechanisms. This includes business transactions, secure communications, digital signatures, and customer information.

These areas are critical because authentication is central to identity verification and secure key transport, whether symmetric or asymmetric. Essentially, it threatens the entire PKI. A cryptographically relevant quantum computer (CRQC) could compromise all the secure communications we rely on today, breaking the encryption that underpins PKI.

This isn't just about quantum computing as we know it today. It's specifically about CRQCs – error-correcting quantum computers capable of breaking PKI. Such systems would endanger sensitive information secured with PKI, including business transactions, communications, and long-term intelligence.

An adversary with access to a CRQC could decrypt data collected now or in the future under the "harvest now, decrypt later" approach. This makes the threat very real and urgent.

Anything using cryptography, especially asymmetric cryptography, is at risk. Symmetric cryptography has a bit more time before being significantly threatened, but asymmetric cryptography faces an immediate issue with CRQCs. Fortunately, the National Institute of Standards and Technology (NIST) has released quantum-resistant standards to help mitigate or delay the problem.

What are the primary goals of CISA's Post-Quantum Cryptography Initiative, and how do you see its impact on securing critical infrastructure?

The goals are multi-faceted but centre around analysis, testing, and standardisation of new cryptographic primitives. For instance, CISA is focused on guiding and supporting critical infrastructure sectors to mitigate risks in existing systems. Education is the first priority: ensuring that teams and organisations understand the threat and how to address it.

Next, we evaluate the sensitivity of organisations' data and assets – identifying what's at risk and for how long. This includes inventorying IT and OT systems and working with vendors to implement and validate standards. It's not just about rolling out new standards but ensuring that vendors and third-party suppliers meet these standards accurately.

Budgeting is another critical aspect. Organisations need to allocate resources for necessary hardware, software updates, or replacements to transition to post-quantum cryptography. This includes updating lifecycle plans for IT and OT systems and ensuring state, local, tribal, and territorial (SLTT) entities are part of the preparation process.

Finally, we emphasise the cyclical nature of this work – monitoring and adapting as new standards emerge. NIST has already released 14 new standards under review, and as cryptographic needs evolve, so will the standards we must implement.

It seems like two key challenges are ensuring no one is left behind in this transition and keeping up with the constantly changing landscape?

That's absolutely right. This isn't a "drop the mic and walk away" situation. Cryptography is inherently mathematical, and over time, even classical algorithms are broken. The same will apply to quantum algorithms as CRQCs grow more capable. This is why crypto agility – our ability to adapt to new and stronger algorithms – is critical.

How does CISA assess vulnerabilities across the 55 national critical functions?

That's primarily handled by the National Risk Management Center (NRMC). They assess vulnerabilities by analysing cross-sector interdependencies and prioritising outreach based on stakeholder feedback.

Each critical infrastructure sector has unique risks, so we must work closely with stakeholders to understand their priorities and address vulnerabilities effectively. It's about balancing the categorisation of critical functions with real-world input from those directly involved.

You mentioned NIST. How do you collaborate with other agencies to streamline this transition?

We collaborate extensively with agencies like the Office of Management and Budget (OMB), the Office of the National Cyber Director (ONCD), NSA, and others. We aim to speak with one voice across agencies, ensuring consistency and coordination. For instance, we work closely with NIST to assess cryptographic discovery and inventory tools, which help identify cryptographic elements in systems.

International collaboration is also essential because divergent standards can create operational challenges. We engage with international partners and the private sector, emphasising the importance of adopting NIST's standards. This unified approach ensures that we're moving forward collectively.

This is not just CISA leading the charge – it's a joint effort involving NIST, CISA, NSA, and other agencies like the Department of Energy (DOE), Department of Justice (DOJ), and the Department of Health and Human Services (HHS). Together, we're ensuring this transition is a coordinated and comprehensive process.

How do you drive awareness and engagement with the private sector?

We engage the private sector through regular meetings and participation in industry conferences. We've noticed a shift – initially, most conferences focused on AI, but now more are recognising the quantum threat. We're getting invited to larger platforms, like RSA, where we can reach broader audiences.

Awareness is growing, but it's still like turning an aircraft carrier – it takes time. Once the industry fully grasps the threat, we expect momentum to build rapidly.

How will you measure the success of the Post-Quantum Cryptography Initiative?

It's essential to examine how organisations are implementing these practices in terms of awareness and preparation.

In terms of inventory discovery and risk assessment, understanding the risks within an organisation is a crucial measurement. For instance, if organisations can start generating policies that cover implementation, validation, and testing for quantum readiness, that's a positive step forward.

Vendor management is another critical aspect. It's vital to ensure that vendors are engaged effectively to update and align products with the necessary specifications.

Additionally, awareness and preparedness play significant roles. Executing early actions, such as establishing policies addressing the quantum threat, is essential. These policies should guide how organisations should approach the challenges posed by quantum technologies.

While NSM 10 was a solid starting point, follow-up policies are necessary to build on that foundation. Creating comprehensive roadmaps is also important. We already have some roadmaps in place, but the level of effort required for each milestone on those roadmaps is a key factor to consider.

Finally, I would like to highlight the incredible work of NIST, CISA, and other agencies over the past few years. We've made tremendous progress in getting quantum threats on senior management's radar. A few years ago, this wasn't even part of the conversation, but now it's front and centre. That's a huge accomplishment, and it's critical we keep building on this momentum.

13. Australia moves to drop some cryptography by 2030 – before quantum carves it up

by Thomas Claburn
https://www.theregister.com/2024/12/17/australia_dropping_crypto_keys/

Australia's chief cyber security agency has decided local orgs should stop using the tech that forms the current cryptographic foundation of the internet by the year 2030 – years before other nations plan to do so – over fears that advances in quantum computing could render it insecure.

The Land Down Under's plans emerged last week when the Australian Signals Directorate (ASD) published guidance for High Assurance Cryptographic Equipment (HACE) – devices that send and/or receive sensitive information – that calls for disallowing the cryptographic algorithms SHA-256, RSA, ECDSA and ECDH, among others, by the end of this decade.

Bill Buchanan, professor in the School of Computing at Edinburgh Napier University, wrote a blog post in which he expressed shock that the ASD aims to move so quickly.

"Basically, these four methods are used for virtually every web connection that we create, and where ECDH is used for the key exchange, ECDSA or RSA is used to authenticate the remote server, and SHA-256 is used for the integrity of the data sent," he wrote. "The removal of SHA-256 definitely goes against current recommendations."

The ASD's stated reason for disallowing these algorithms in HACE systems by 2030 is "projected technological advances in quantum computing."

Quantum computing has been deemed a sufficiently plausible threat to legacy encryption schemes that the US National Institute for Standards and Technology (NIST) in 2016 issued a call for quantum-resistant algorithms. The Institute's concern is that some future quantum machines may be able to crunch numbers so efficiently that current encryption – applied with the assumption that data protection will last decades – could be easily cracked.

In August 2024, three post-quantum cryptographic algorithms – ML-KEM [PDF], ML-DSA [PDF], and SLH-DSA [PDF] – were approved by NIST in the hope they can keep encrypted data safe from anticipated code cracking capabilities.

Three months later, NIST published draft guidance for the "Transition to Post-Quantum Cryptography Standards" in a bid for public comment. The proposal deprecates certain standards by 2030 – among them the RSA algorithm – and disallows them by 2035.

As with the ASD, NIST's guidelines aim to mitigate the risk that cryptographic standards "could be vulnerable to an attack by a Cryptographically Relevant Quantum Computer (CRQC)" by 2035. That's according to US National Security Memorandum (NSM) 10.

The National Security Agency (NSA) issued similar guidance [PDF] in September, and also set 2035 as the transition date, per NSM 10.

Australia – as a member of the Five Eyes intelligence sharing alliance – aims to move more quickly than NIST (at least for HACE devices) by declaring that various legacy cryptographic algorithms "will not be approved for use beyond 2030."

Whether Aussie government agencies will be afforded the flexibility to upgrade their cryptography-dependent kit after the 2030 deadline remains to be seen. It may be that systems not deemed HACE could get a bit more wiggle room.

With regard to the algorithms used to hash data – particularly SHA-224 and SHA-256 – Buchanan expressed surprise that neither will be approved for use beyond 2030.

"The migration within five years will not be easy, as every single web connection currently uses ECDH and RSA/ECDSA," he wrote. "These methods are also used for many other parts of a secure infrastructure."

Looks like we could be in for interesting times.

14. Banco Sabadell Collaborates with Accenture and QuSecure to Advance Quantum Safe Infrastructure

by Alison Geib, Denise Berard, Dan Spalding, and **Banco Sabadell**
https://newsroom.accenture.com/news/2024/banco-sabadell-collaborates-with-accenture-and-qusecure-to-advance-quantum-safe-infrastructure

Banco Sabadell has successfully completed a joint project with Accenture and QuSecure to explore the adoption of Post-Quantum Cryptography (PQC) technologies in the bank's infrastructure. This project is a significant step forward in bolstering resistance to quantum attacks, with Banco Sabadell leveraging QuSecure's software for crypto agility and open-source libraries to modernize and orchestrate encryption.

The collaboration between Banco Sabadell, Accenture and QuSecure resulted in a comprehensive understanding of the steps required for the bank to become quantum-resilient and provided an initial estimation of how quantum security technologies can be adopted. The successful completion of the four-month project further demonstrates the organization's commitment to staying ahead of advancements in the quantum security race.

"Cryptography plays a crucial role in banking, securing processes such as payments, digital interactions with customers and communications with market infrastructure. It is also essential for protecting sensitive information. As we transition into a post-quantum computing era, the challenges include identifying the use of cryptographic methods vulnerable to quantum attacks and transitioning to quantum-safe cryptography with agility and efficiency," explains Joan Puig, Group CISO of Banco Sabadell. "This project, in collaboration with Accenture and QuSecure, has allowed us to explore the impact of the adoption of post-quantum cryptography technologies on the bank's infrastructure."

According to the Financial Services Information Sharing and Analysis Center (FS-ISAC) the transition to crypto agility must start immediately and is a long-term strategy, not a one-time implementation.

"We are excited to be collaborating with Banco Sabadell and QuSecure on this groundbreaking project," said Tom Patterson, emerging technology security lead at Accenture. "Our expertise in quantum risk and our quantum security test labs enabled Banco Sabadell to gain a competitive edge with a clear and proven roadmap for transitioning to quantum-safe technologies incorporating the latest NIST PQC standards. This collaboration underscores our commitment to helping organizations safeguard their data from emerging threats posed by the rapid quantum computing advancements."

"QuSecure is advancing encryption agility and security at the network layer," said Elizabeth Green, SVP of Customers and Ecosystems at QuSecure. "This is the fastest and easiest way to protect enterprises without having to rip and replace existing infrastructure. Working with Accenture and Banco Sabadell was a delight and proves that mitigation of existing encryption to Post Quantum Standards for complex

environments is possible and can be achieved expediently this decade, in advance of NIST recommended deprecation of many major algorithms."

The rise of quantum computing challenges modern-day cryptography. Preparing and adapting cryptographic methods to withstand the power of quantum technologies involves developing quantum-resistant algorithms and reevaluating current security protocols. Proactively addressing these concerns is crucial for maintaining the integrity and confidentiality of digital communications in the quantum era.

15. IoT device security platform for post-quantum cryptography

by Seb Springall
https://www.electropages.com/2024/12/iot-device-security-platform-post-quantum-cryptography

Crypto Quantique, a provider of quantum-driven security for the IoT, has upgraded its QuarkLink IoT device security platform with a hybrid post-quantum cryptographic algorithm.

QuarkLink is an integrated, scalable, cloud-based software platform that decreases the time and expense of implementing all necessary security functions in embedded devices (IoT) and industrial PCs by up to 10X. It integrates client libraries for popular MCU families, supports Linux distributions in industrial PCs, and manages device identities. It also manages security keys, digital certificates, and Public Key Infrastructure (PKI) and supports secure boot and FOTA updates.

The hybrid key encapsulation mechanism adopted by QuarkLink is X25519Kyber768Draft00. This combines the classical elliptic curve Diffie-Hellman key exchange X25519 with the post-quantum secure algorithm Kyber (ML-KEM). This hybrid approach delivers immediate security against classical attacks and future protection against quantum computer-based threats. It also ensures protection against 'store-now/decrypt-later' attacks in which cybercriminals collect and store encrypted data to decrypt it in the future when more advanced capabilities become available.

QuarkLink hybrid-PQC is now available for MPUs running Embedded Linux, and support for MCUs will become available in Q1 2025.

Shahram Mossayebi, Crypto Quantique's CEO, commented: "This development is a further demonstration of Crypto Quantique's technology leadership in IoT device security. Companies adopting the QuarkLink platform today are not only able to save substantial time and cost in their embedded development work but can achieve quantum-resilient security against current and future attacks."

16. Firm using cryptography to keep AI accountable joins World via TFH acquisition

by Joel R. McConvey
https://www.biometricupdate.com/202412/firm-using-cryptography-to-keep-ai-accountable-joins-world-via-tfh-acquisition

Tools for Humanity (TFH), which calls itself a "contributor" to the World ID iris biometrics and digital identity project, has a new limb. A Substack post from Modulus Labs' Daniel Shorr says his company is joining TFH "to build the largest network of real humans on the planet."

Modulus Labs reportedly developed its product, Accountable Magic, in response to the increasing dysfunctionality of the internet: "misinformation, bots and scammers, the anger economy." Their cryptographic system is "a way to prevent the manipulation of AI algorithms – mathematically." Specifically, it focuses on "machine-learning accountability" using zero-knowledge proof (ZKP) protocols.Now, it will be integrated into World's system for collecting iris biometrics and creating a World ID, thereby recording and verifying "humanness."

'Accountable AI' system like a blue check for algorithmic content

According to its website, Accountable Magic provides "AI security through novel cryptography." In practical terms, it is an edge-based system to verify that AI algorithms have not been manipulated – "like Twitter's blue check but for AI outputs."

Per Shorr's blog, "zero-knowledge AI will deliver private and verifiably secure authentication on the user's personal device, playing an important role through Personal Custody."

"Along with the Orb and innovations like AMPC (anonymized multi-party computation), this technology will play an important role in distinguishing between bots and humans at the scale of billions. That means online interactions that are safer and more accountable. It means digital authorship that's verifiable. And it means bringing new communities to the astonishing power of digital currencies."

Use AI to fight AI to enable further use of AI...

A 2023 Fortune Crypto article about the startup says that through zero-knowledge proofs, "outside observers can verify that companies or developers used a promised AI algorithm. For example, OpenAI, the juggernaut that developed ChatGPT, can prove that its chatbot wrote a poem without revealing the algorithm's 'weights,' or what an A.I. model learns after training on copious amounts of data."

Its proposition, then, is that using cryptography to keep algorithms accountable will enable developers to "build wildly expressive services that never betray our trust." A graphic on its site cycles through use cases: NFT appraisals, private identity authentication, AI game economies, "tamper-proof intelligent finance," "authentic machine artists."

And so do forces continue to muster in the escalating war between AI algorithms that could lead to harm and tech tools to temper them – so that even more exciting algorithms can be developed.

17. Quantinuum Demonstrates Record GHZ State of 50 Entangled Logical Qubits

by GQI

https://quantumcomputingreport.com/quantinuum-demonstrates-record-ghz-state-of-50-entangled-logical-qubits/

Perhaps it's best to start off by explaining what a GHZ state is and why it is an accomplishment to create one that uses 50 qubits. Most people are familiar with two entangled qubits known as a Bell pair such that the state of these qubits are linked such that when one changes a state the other one will also change it state even if these entangled qubits may be far away from each other without any connection. Einstein used to call this "Spooky action at a distance". A GHZ state is an extension of this such that you have more than two qubits entangled to each other such that all the qubits in the GHZ state will change together. In a perfect GHZ state, each of the qubits will be in the superposition of "0" and "1" state and when measured all will collapse together to either the "0" state or the "1" state. The picture above shows the results of Quantinuum's experiment that show some errors as represented by the bars in the middle of the chart. If there were no errors, 50% of the time the measured results for all the qubits would be in the far left bar (0000....) and the other 50% of the time, the measured results for all the qubits would be in the far right bar (1111...).

Quantinuum has taken their 56 qubit H2-1 processor and created a 50 qubit GHZ state with the help of a [[52,50,2]] error detection code. This code utilized 52 physical qubits to create 50 logical qubits with a code distance of 2 between codewords. Note that this code only provides the capability of detecting error, but not to correct errors on the fly. However, if an error is detected, the quantum processor can repeat the operation until no errors are detected. In the chart above, the orange bars shows the results without using the error detection code while the blue bars show the results using this error detection code. So as we would hope, it does show improved results when the error detection code is turned on.

The Quantinuum results more than doubles results reported last month by Microsoft and Atom Computing who were able to demonstrate 24 entangled logical qubits. Microsoft and Atom used a [[4,2,2]] code which provides error and loss detection. That demonstration was performed on Atom's 256 qubit neutral atom based processor and used about 48 physical qubits to create 24 logical qubits with a code distance of two.

So, like many things in the competitive quantum computing ecosystem, vendors are vying to set new performance records for many different performance measures. Although this demonstration from Quantinuum sets a new record for the GHZ state in 2024, we fully expect that in coming years others will be able to raise the bar even further with larger and more powerful quantum processors along with more advanced error detection and correction codes.

For more information about Quantinuum's advancements in logical quantum computation, we refer you to a presentation made at the recent Q2B Silicon Valley conference by David Hayes, Quantinuum's Director of Computational Theory and Design. You access it here.

18. I Think the 2035 Post-Quantum Preparation Date Is Insane

by Roger Grimes
https://www.linkedin.com/pulse/i-think-2035-post-quantum-preparation-date-insane-roger-grimes-yote e/

One of my favorite parables is the one where someone is assigned an important daily job for 30 days and then asked if they would prefer $1M at the end of the job or a penny on the first day, which then doubles over and over for the next 29 days. This means the employee would get $0.01 on the first day, $0.02 on the second day, $0.04 on the third day, $0.08 on the fourth day, and so on for 30 days. Most people unfamiliar with the parable easily would take the $1M, but because of the way "compounding" works, if they took the penny that doubles each day method, they would have had $5,368,709.12 by the end of the 30th day instead!

It's meant to teach the value of compounding interest and investing, but it has a bunch of other applications.

It's with this parable in mind that I write this article.

The US government has placed 2035 as the year when most organizations should be post-quantum ready, meaning having replaced their quantum-susceptible cryptography with quantum-resistant cryptography. You can find a few different "official post-quantum prep" dates, but the US National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems is the authoritative resource, for now, for US organizations and much of the world.

Note: That long memo name is shortened to National Security Memorandum 10 (NSM-10) in quantum discussion circles.

The National Institute of Standards & Technology provides some more detail in their NIST Transition to Post-Quantum Cryptography Standards document, discussing what cryptography will be deprecated in 2030 versus 2035.

If you are not aware, we have been on the road to making "sufficiently-capable" quantum computers for a few decades. We've been making slow, but steady progress. One day, some world's government or organization will develop a quantum computer that is capable of rendering much of our most important modern-day cryptography (e.g., RSA, Diffie-Hellman, El-Gamal, Elliptic Curve Cryptography, etc.) useless. Before then, the world was supposed to migrate all software and firmware from quantum-susceptible cryptography to quantum-resistant cryptography.

NIST (and other countries) have been holding contests and developing post-quantum cryptography. In the last year or so, NIST has formally selected at least four cryptographic algorithms that we need to move to, with more on the way. If you want more information about the NIST post-quantum cryptography developments, go here: https://csrc.nist.gov/projects/post-quantum-cryptography.

I've been writing about this coming quantum cryptographic break for decades, even since it was announced by Peter Shor in 1994 that if we had quantum computers, it would invalidate much of our modern-day cryptography. It was big news even back then, when we didn't have a single quantum computer. But by 1999, the first very rudimentary quantum computers started to be developed. By 2015, we had made enough progress that quantum computer news began to show up in regular computer security news feeds. In 2019, I wrote a book on the subject, Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto

I'm on a few quantum preparation groups, such as the Cloud Security Alliance's Quantum Safe Secure working group. I spend a fair amount of time trying to educate people about the topic and get companies to prepare for the coming post-quantum work that needs to be done.

To be clear, your organization needs to have a post-quantum project already and be preparing for the day when you need to upgrade most of your cryptography. I still think that my book or this free whitepaper that I was the lead author on, Practical Preparations in a Post-Quantum World is a great guide to get you started.

I Think the 2035 Post-Quantum Preparation Date Is Insane

I regret the day the US stated that 2035 was the year when organizations had to complete their post-quantum migrations. I think it borders on malfeasance. Time will tell.

First, I think there is a decent shot that the coming quantum crypto break could happen before then, if it hasn't already happened and we just don't know about it. Although most quantum computer scientists don't give strong support to the idea that the quantum crypto break may have already happened, I give it a 15% chance. The world's leading cryptography intelligence agencies (e.g., NSA, etc.) have a long history of achieving historic cryptographic landmarks years before publicly revealing that we did.

But the biggest reason why a 2035 date pisses me off is that it almost certainly means most organizations won't be doing anything about it anytime soon. The quantum crypto world thinks all companies have already started up internal post-quantum projects and have been working on them for years. When I tell them that most companies haven't even heard of it, much less are actually forming official projects to tackle it, they look at me dumbfounded. Huge disconnect.

Job number one for the quantum crypto community is just to make people aware of the coming HUGE Y2K-like project that every organization and person will be involved in. It's going to be a massive effort that involves inventorying and upgrading or replacing every bit of hardware and firmware you have.

And when the US government says organizations have till 2035 to be quantum prepared, that virtually kills that we will be doing anything about now. We have ransomware, password stealing trojans, and AI-deepfakes to worry about TODAY! If you tell me I've got another problem coming in ten years, that virtually guarantees it won't get any attention right now. And if the US government said to be prepared by 2028, we'd probably still be trying to make it happen in 2030. Set a 2028 deadline date and maybe meet the 2035 objective.

Don't we all have that spouse or friend who we lie to a little bit about the arrival time of a party just so we can get them there somewhere near the appointed time?

Then, a few days ago, Google announced its progress on its latest quantum chip called **Willow**. Even Elon Musk said, "Wow!"

I don't think Musk is a quantum-following guy. He probably just knows the basics. He's a busy guy. But there have also been dozens of quantum advancement announcements over the years, including plenty from Google, the world's smartest and richest man has never stopped for a second, read the story, and said, "Wow!" Something has changed.

I don't think Google's announcement is earth-shattering. It isn't announcing that they have achieved sufficiently-capable quantum computers that can break today's crypto. But it was a strong, strong push of forward progress on everything needed to achieve that. It's harder to see what Google and the thousands of other companies are trying to be the first to achieve quantum supremacy, as anything other than that penny that is getting doubled every day.

There are thousands of companies developing their own quantum computers, most of which are making steady progress every day. The best and biggest companies in the world each spend billions on it. It takes only one company to make a consequential leap forward discovery and breakthrough to wipe away existing deadlines that are built on the expectation of forever slow plodding. I think it's insane to understand that reality and keep a 2035 deadline.

Every single quantum challenge I'm aware of (e.g., qubits, stability, error-correcting, coherence, number of logic gates, photonics, silicon-based quantum chips, etc.) is making constant progress. And as they learn

how to overcome those challenges, they can quickly go from one of something to a million of that thing. The hard part is in the first overcome.

Four other important points:

- **One, Peter Shor's algorithm,** which is the standard that tells us how many stable quantum bits (qbits) we need to break today's encryption, is the ceiling of what we need, not the floor. There have been many other improvements and other algorithms that have significantly reduced the quantum resources needed to break encryption. I've gotta guess that there are even better algorithms in secret places that we don't know about. So, if you're looking at Shor's algorithm as the gatekeeper, you'll surely be mistaken.

- **Second, all the quantum improvements and dates** are based on the progress that generalized quantum gate computers are making. These are basically widely capable quantum computers that can do lots of things. The NSA and the rest of the nation-state crypto world don't use general-purpose computers to crack crypto. They build specialized machines with the bare minimum basics needed to break crypto. It allows them to crack secrets many orders of magnitude faster than a general computer device can. I've got to think that the NSA and other countries are spending much of their time figuring out and building specialized quantum-cracking computers versus building generic quantum computers. And if this is true, and it likely is, what does that mean for the 2035 preparation date?

- **Third, there is a chance that your adversaries are sniffing your currently encrypted** (quantum-susceptible) data now and storing it for decrypting when they have achieved the necessary quantum sufficiency. It is happening in the real world today. NIST has publicly stated that it is happening (although I don't have the link handy). There is a near 100% chance NSA is doing this to our adversaries. If you have important data you want to protect and you think an adversary might be sniffing and saving it just in case, well, your post-quantum timeline is today.

- **Fourth and last, as infamous quantum scientist Dr. Michele Mosca's Inequality** "theorem" reminds us, it takes time to migrate to post-quantum protection, and during all that time your data is at risk.

  In 2015, Dr. Mosca, who has probably thought about the issue of when we need to be quantum prepared more than anyone, stated, "There is a 1 in 7 chance that some fundamental public-key crypto will be broken by quantum by 2026 and a 1 in 2 chance of the same by 2031."

I'm not sure if he still stands by this statement today...but it seems to me that I'm not alone in being worried that a 2035 post-quantum prep date is risky.

Some of Dr. Mosca's latest thoughts on the post-quantum date are covered in a recent report he helped author, Quantum Threat Timeline Report 2024 .

Yes, I think the 2035 date posted by the US government as the year when we all need to be post-quantum prepared is insane. Yes, I think there is a 15% chance the post-quantum break has already happened somewhere, and we just don't know about it. But my biggest problem with the 2035 date is that most organizations aren't doing anything TODAY to prepare. And you should be. You should at least be doing a cryptographic inventory of all cryptography in all your software and firmware.

And it just seems very risky...too risky...to be telling people they have 10 years to prepare for something that has a decent chance of happening today. I'm not sure if I can think of a similar scenario where our government saw a big risk and went...eehh...take 10 years to get there.

19. Nokia and SK Broadband deploy quantum secure network to protect Korea Hydro and Nuclear Power's IT infrastructure

https://www.nokia.com/about-us/news/releases/2024/12/11/nokia-and-sk-broadband-deploy-quantum-secure-network-to-protect-korea-hydro-and-nuclear-powers-it-infrastructure/

Nokia today (11 Dec 2024) announced that Nokia and SK Broadband have deployed a leased line network for Korea Hydro and Nuclear Power (KHNP) to enhance data security. Completed in August 2024, this deployment enables KHNP to protect its network against existing and emerging cyber threats, including quantum computing-based cyberattacks.

Nokia's Quantum-Safe Network solution, which uses a defense-in-depth approach with advanced network cryptography for protection against sophisticated cyber threats. The key technologies used in this project include Nokia's transmission equipment, interconnect routers, and service access systems. Nokia's Network Services Platform (NSP) also helped in simplifying network operations and management.

Kim Gooyoung, Head of Enterprise Sales Division at SK Broadband, said: "The integration of Nokia Quantum-Safe MACsec cryptographic technologies with KHNP's network will significantly enhance the security and reliability of South Korea's critical energy infrastructure. Advanced technologies, like quantum-safe networks, are becoming pivotal in safeguarding essential systems today and in the forthcoming quantum era. Collaborating with Nokia allows us to stay ahead of the constantly shifting cybersecurity environment and help our customers access the latest quantum-safe technology advancements for secure growth."

Jay Han, Head of Network Infrastructure business at Nokia Korea, said: "Protecting critical infrastructure is a hallmark of quantum-safe technology, and an area we understand well at Nokia. Our industry-leading quantum-safe network solutions and proven expertise in delivering high-performance, secure technologies for critical infrastructure operators are helping companies like KHNP safeguard their essential systems to protect against disruptions and attacks caused by cyber threats. We look forward to

working with SK Broadband to expand the use of our quantum-safe MACsec cryptographic technology throughout Korea."

20. The new math: Solving cryptography in an age of quantum

by Kelly Raskovich, Bill Briggs, Mike Bechtel, and Ed Burns
https://www2.deloitte.com/us/en/insights/focus/tech-trends/2025/tech-trends-quantum-computing-and-cybersecurity.html

Cybersecurity professionals already have a lot on their minds. From run-of-the-mill social engineering hacks to emerging threats from AI-generated content, there's no shortage of immediate concerns. But while focusing on the urgent, they could be overlooking an important threat vector: the potential risk that a cryptographically relevant quantum computer (CRQC) will someday be able to break much of the current public-key cryptography that businesses rely upon. Once that cryptography is broken, it will undermine the processes that establish online sessions, verify transactions, and assure user identity.

Let's contrast this risk with the historical response to Y2K, where businesses saw a looming risk and addressed it over time, working backward from a specific time to avert a more significant impact. The potential risk of a CRQC is essentially the inverse case: The effect is expected to be even more sweeping, but the date at which such a cryptographically relevant quantum computer will become available is unknown. Preparing for CRQCs is generally acknowledged to be highly important but is often low on the urgency scale because of the unknown timescale. This has created a tendency for organizations to defer the activities necessary to prepare their cybersecurity posture for the arrival of quantum computers.

"Unless it's here, people are saying, 'Yeah, we'll get to it, or the vendors will do it for me. I have too many things to do and too little budget,'" says Mike Redding, chief technology officer at cybersecurity company Quantropi. "Quantum may be the most important thing ever, but it doesn't feel urgent to most people. They're just kicking the can down the road."

This complacent mindset could breed disaster because the question isn't *if* quantum computers are coming—it's *when*. Most experts consider the exact time horizon for the advent of a CRQC to be irrelevant when it comes to encryption. The consensus is that one will likely emerge in the next five to 10 years, but how long will it take organizations to update their infrastructures and third-party dependencies? Eight years? Ten years? Twelve? Given how long it took to complete prior cryptographic upgrades, such as migrating from cryptographic hashing algorithms SHA1 to SHA2, it is prudent to start now.

In a recent report, the US Office of Management and Budget said, "It is likely that a CRQC will be able to break some forms of cryptography that are now commonly used throughout government and the private sector. A CRQC is not yet known to exist; however, steady advancements in the quantum computing field may yield a CRQC in the coming decade. Accordingly … federal agencies must bolster the defense of their

existing information systems by migrating to the use of quantum-resistant public-key cryptographic systems."

The scale of the problem is potentially massive, but fortunately, tools and expertise exist today to help enterprises address it. Recently released postquantum cryptography (PQC) algorithm standards from the US National Institute of Standards and Technology (NIST) could help to neutralize the problem before it becomes costly, and many other governments around the world are also working on this issue. Furthermore, a reinvigorated cyber mindset could set enterprises on the road to better security.

Now: Cryptography everywhere

Two of the primary concerns for cybersecurity teams are technology integrity and operational disruption. Undermining digital signatures and cryptographic key exchanges that enable data encryption are at the heart of those fears. Losing the type of cryptography that can guarantee digital signatures are authentic and unaltered would likely deal a major blow to the integrity of communications and transactions. Additionally, losing the ability to transmit information securely could potentially upend most organizational processes.

Enterprises are starting to become aware of the risks posed by quantum computing to their cybersecurity. According to Deloitte's Global Future of Cyber survey, 52% of organizations are currently assessing their exposure and developing quantum-related risk strategies. Another 30% say they are currently taking decisive action to implement solutions to these risks.

"The scale of this problem is sizeable, and its impact in the future is imminent. There may still be time when it hits us, but proactive measures now will help avoid a crisis later. That is the direction we need to take," says Gomeet Pant, group vice president of security technologies for the India-based division of a large industrial products firm.

Cryptography is now so pervasive that many organizations may need help identifying all the places it appears. It's in applications they own and manage, and in their partner and vendor systems. Understanding the full scope of the organizational risk that a CRQC would pose to cryptography requires action across a wide range of infrastructures, supply chains, and applications. Cryptography used for data confidentiality and digital signatures to maintain the integrity of emails, macros, electronic documents, and user authentication would all be threatened, undermining the integrity and authenticity of digital communications.

To make matters worse, enterprises' data may already be at risk, even though there is no CRQC yet. There's some indication that bad actors are engaging in what's known as "harvest now, decrypt later" attacks—stealing encrypted data with the notion of unlocking it whenever more mature quantum computers arrive. Organizations' data will likely continue to be under threat until they upgrade to quantum-resistant cryptographic systems.

"We identified the potential threat to customer data and the financial sector early on, which has driven our groundbreaking work toward quantum-readiness," said Yassir Nawaz, director of the emerging technology security organization at JP Morgan. "Our initiative began with a comprehensive cryptography inventory and extends to developing PQC solutions that modernize our security through crypto-agile processes."

Given the scale of the issues, upgrading to quantum-safe cryptography could take years, maybe even a decade or more, and we're likely to see cryptographically relevant quantum computers sometime within that range. The potential threat posed by quantum to cryptography may feel over the horizon, but the time to start addressing it is now.

"It is important that organizations start preparing now for the potential threat that quantum computing presents," said Matt Scholl, computer security division chief at NIST. "The journey to transition to the new postquantum-encryption standards will be long and will require global collaboration along the way. NIST will continue to develop new post-quantum cryptography standards and work with industry and government to encourage their adoption."

New: Upgrading to a quantum-safe future

There's good news, though. While upgrading cryptography to protect against the threat of quantum computers requires a comprehensive and widespread effort, given sufficient time, it should be a relatively straightforward operation.

Initial steps include establishing governance and policy, understanding current cryptographic exposure, assessing how best to prioritize remediation efforts across the infrastructure and supply chain, and building a comprehensive road map for internal updates and contractual mechanisms to ensure vendors meet the updated standards.

"The first step to reclaim control over decades of cryptographic sprawl across IT is to leverage modern cryptography management solutions, which empower organizations with critical observability and reporting capabilities," says Marc Manzano, general manager of cybersecurity group SandboxAQ.

Once these initial steps are completed, organizations can begin updating encryption algorithms. In August 2024, NIST released new standards containing encryption algorithms that organizations can implement. The agency says these encryption methods should withstand attacks from quantum computers by changing how data is encrypted and decrypted.

Current encryption practices encode data using complex math problems that outpace the computing power of even today's most powerful supercomputers. But quantum computers will likely be able to crack these problems quickly. The updated NIST standards move away from today's large-number-factoring math problems and leverage lattice and hash problems, which are sufficiently complex to bog down even quantum computers.

Large tech companies are already beginning their transition. Following the release of NIST's updated standards, Apple updated its iMessage application to use quantum-secure encryption methods. Google announced that it implemented the new standards in its cryptography library and will use them in its Chrome web browser. IBM, which has invested heavily in developing quantum computing technology, has integrated postquantum cryptography into several of its platforms, and Microsoft has announced that it will add quantum-secure algorithms to its cryptographic library.

In 2021, the National Cybersecurity Center of Excellence (NCCoE) at NIST started the Migration to PQC project. It has grown to over 40 collaborators, many of whom have cryptographic discovery and inventory tools with differing capabilities. The project demonstrates the use of these tools in a manner that will enable an organization to plan for their use. Other collaborators are focused on testing the PQC algorithms for use in protocols to understand their interoperability and performance as they prepare to implement PQC in their products.

"An organization needs to understand where and how it uses cryptographic products, algorithms, and protocols to begin moving towards quantum-readiness," says Bill Newhouse, co-lead for the Migration to PQC project at the NCCoE. "Our project will demonstrate use of the tools and how the output of the tools supports risk analysis that will enable organizations to prioritize what it will migrate to PQC first."

Next: Leveraging post-quantum cryptography to prepare for future threats

While enterprises upgrade their encryption practices, they should consider what else they might do. This can be likened to cleaning out the basement: What can be done to clean out the back corners no one has looked at in a decade? They will map out highly technical, low-level capabilities in core systems that haven't been assessed in years. Perhaps they will uncover other potential issues that can be addressed while upgrading cryptography, such as enhancing governance, improving key management processes, implementing a zero trust strategy, upgrading cryptography while modernizing legacy systems, or simply sunsetting tools that haven't been used in a while.

Organizations that engage in proper cyber hygiene are likely to strengthen their broader cyber and privacy practices. They will likely be more cautious about collecting and sharing anything other than strictly necessary data, establish more robust and accountable governance mechanisms, and continually assess trust between digital components. Beyond protecting against the far-off threat of quantum attacks, these practices harden an enterprise's defenses today by building secure habits into everyday activities.

Enterprises should consider how to create a reproducible set of activities to protect their cryptographic systems against various types of attacks and failures, a concept known as cryptographic resilience. Today, organizations need to prepare for the quantum threat vector, but tomorrow, the next new risk will require a different approach. Security teams shouldn't have to go through this entire exercise again when a new threat emerges—instead, they should develop the muscles necessary to add or swap out cryptographic capabilities quickly and seamlessly.

As our digital and physical lives become more closely linked, our friendships, reputations, and assets are undergoing a digital transformation. These areas are mediated digitally and secured cryptographically. Going forward, the privacy and integrity of messages, transactions, and an increasing share of the human condition will be built upon a foundation of digital trust. Protecting cryptography isn't only about protecting enterprise data stores—it's about shielding increasingly sensitive areas of our lives.

"As our reliance on cryptography intensifies in the digital economy, organizations must act swiftly to prepare for a controlled transition to maintain the trust they've built with customers and partners," says Michele Mosca, founder and CEO of evolutionQ. "It's crucial for organizations to develop a quantum-safe road map and partner with vendors to kick-start this vital shift. Prioritizing the security of your most sensitive information isn't just prudent—it's essential."

Quantum computers are likely to bring significant benefits to a range of areas, such as drug discovery, financial modeling, and other use cases, that improve people's lives. These potential benefits should not be overshadowed by the attendant security challenges. This is why enterprises should start hardening their defenses now so that they are prepared to reap the potential benefits of quantum computing without major disruption from its risks.

21. Enhancing network security with Accenture Federal Services using quantum optimization

by Rowen Wu
https://q-ctrl.com/blog/enhancing-network-security-with-accenture-federal-services-using-quantum-optimization

Federal agencies face a critical optimization challenge in today's cybersecurity landscape: effectively detecting security threats and inefficiencies in increasingly complex network activity. These challenges manifest as outlier "anomalies" that emerge from analyzing intricate device communication patterns across vast federal networks.

The federal sector is increasingly turning to advanced technologies like quantum computing and artificial intelligence to address these challenges. These tools offer new capabilities for processing complex network data and identifying subtle patterns that might indicate security threats or operational inefficiencies.

In a groundbreaking opportunity, we collaborated with Accenture Federal Services to explore innovative approaches to network security optimization. This partnership focused on leveraging quantum computing capabilities, applying our error suppression software, Fire Opal, to IonQ hardware through Amazon Braket, to enhance anomaly detection in complex network environments, where traditional methods face significant computational limitations.

Raising the security standard with quantum computing

Network anomaly detection is inherently difficult because it's rooted in solving a very challenging problem known as Max-Cut optimization. This problem requires splitting a network of connected "nodes" into two separate groups in a way that maximizes the communication—the "cut"—between them. It sounds simple, but as network size and complexity grow, the number of possible solutions increases exponentially. Classical solutions often rely on approximations that take shortcuts to save time.

The partnership exemplifies how combining domain expertise with cutting-edge quantum technology can create transformative solutions. By focusing on the Max-Cut optimization problem, the team developed an approach that maintains both organizations' strengths while pushing the boundaries of what's possible in network security.

Building high-performance quantum solutions with quantum infrastructure software

Working together, our teams leveraged Fire Opal's optimization solver while incorporating Accenture Federal Services' extensive experience in federal security requirements. This collaborative approach ensured that the solution met rigorous security standards while taking advantage of quantum computing's unique capabilities. Using the Fire Opal Optimization Solver, we simplified the process of implementing a hybrid quantum-classical algorithm to address the problem The Optimization Solver accepts a high-level problem definition and implements a hardware-efficient hybrid workflow that leverages the benefits of both quantum and classical computing.

In addition to problem abstraction, the Fire Opal Optimization Solver incorporates world-leading error suppression to push the quantum hardware to the limits whenever the QPU is called. This effective performance enhancement technology for quantum computers is delivered as a simple, fully automated solution suitable for end users of quantum computers. By suppressing errors automatically, Fire Opal enables application builders to run more complex use cases leveraging the full hardware potential.

The underlying technology is inherently hardware-agnostic, which enabled Accenture Federal Services to employ their approach on IonQ hardware accessed through the Amazon Braket quantum computing service.

Delivering world-class results

The success of this collaboration was demonstrated through comprehensive testing using the Westermo Network Traffic dataset. Accenture Federal Services tested over 1.8 million network packets recorded over 90 minutes. The joint solution achieved remarkable results, showcasing how strategic partnerships can drive innovation in quantum computing applications.

In performing the data analysis via quantum optimization, the Optimization Solver achieved an accurate solution and did so with a 3x higher success probability over a classical benchmark "local solver". This is a well-constructed but non-optimal classical benchmark, and outperforming it suggests that not only is the problem sufficiently hard to be considered for quantum solutions, but also that quantum optimization may form the basis for the detection of fraud and illicit behavior as quantum computers increase in size and capability over the coming years.

Preparing for quantum readiness through an ecosystem approach

By beginning to explore solutions on today's quantum hardware, Accenture Federal Services is positioning itself for a future where quantum technologies will be indispensable for tackling the most complex network security challenges. They are also learning to navigate the landscape of quantum hardware and software by leveraging flexible infrastructure software that works out-of-the-box with multiple cloud platforms and cloud-accessible hardware systems, such as Amazon Braket and IonQ.

This previews the availability of Fire Opal's error suppression technology on trapped ion devices. Users looking to achieve quality results across QPU modalities will soon be able to leverage IonQ's Forte and Aria devices with Fire Opalthrough an upcoming integration with Amazon Braket.

This integration demonstrates our commitment to making quantum technology useful through a focus on delivering hardware-agnostic, error-reducing, performance-management software to all quantum computing users through the breadth of the AWS network.

It takes an ecosystem working together to narrow the performance gap between the promise of quantum computers and the actual computational capabilities delivered to end users. This partnership has laid the groundwork for future collaborations in quantum computing, demonstrating the value of combining specialized expertise with innovative technology solutions. We're excited to be accelerating the entire industry and moving closer to unlocking new quantum-enabled applications across industries like logistics, finance, and chemistry.

We are presenting and exhibiting at Q2B Silicon Valley this week, an international conference uniting academics, end users, government officials and vendors to discuss the progress and future of the quantum industry. Please visit us at Hall A, Booth #G5!

22. Google's Willow chip to challenge cryptography, but Bitcoin will hold steady, players believe

by SANJANA B

https://www.thehindubusinessline.com/info-tech/googles-willow-chip-to-challenge-cryptography-but-bitcoin-will-hold-steady-players-believe/article68969159.ece

Google has unveiled its Willow quantum computing chip, which some speculate could "crack" Bitcoin. However, cryptocurrency experts argue that decrypting a Bitcoin typically requires around 13 million qubits, far exceeding Willow's 105 qubits.

On Monday,Alphabet and Google CEO Sundar Pichai announced the development of Willow on social media platform X. He stated that the quantum computing chip can reduce errors exponentially as Google scales up using more qubits, cracking a 30-year challenge in the field. In benchmark tests, Willow solved a standard computation in less than five minutes, unlike a supercomputer that would require indefinite time.

A qubit, or a quantum bit, is the basic unit of quantum information in quantum computing. Unlike a classical bit or a binary of 0 or 1, a qubit can represent both 0 and 1, allowing quantum computers to process many combinations simultaneously.

Existential risk?

Twitter user Monetary Commentary pointed out that this development is potentially alarming for Bitcoin and other cryptos that rely on public-key cryptography.

The user explained that Bitcoin's security is supported by elliptic curve cryptography (ECC), a system designed to be computationally impossible for traditional computers to break within a reasonable timeframe. However, quantum computers like Willow, with exponentially reduced error rates and vast computational power, pose a direct threat to ECC.

Quantum algorithms can factorise large integers and compute discrete logarithms – either of which can break ECC. A machine like Willow that can perform computations in minutes that would take other supercomputers infinitely longer, represents an existential risk to Bitcoin's security model.

"The idea of quantum computers cracking Bitcoin is still far off. Google's Willow chip, with 105 qubits, is impressive, but lightyears away from the millions needed to challenge Bitcoin's security. Think of qubits as the 'power cores' – the more you have, the more powerful the computer. Even if Willow's qubits are ground-breaking and hold promise for addressing challenges like climate modelling and drug discovery, it's not enough to break Bitcoin's encryption," observed Himanshu Maradiya, Chairman and Founder of CIFDAQ.

Obstacles like scaling and error correction remain. However, while the crypto world is building quantum-resistant solutions with the evolution of quantum technology, industries from finance to cybersecurity will need to adapt, ensuring that they are future-ready, he said.

Utkarsh Tiwari, the chief strategy office of KoinBX, resounded this, saying that while some discussions link quantum advancements to the potential for "cracking" it, Bitcoin is based on cryptographic algorithms like SHA-256, which would require more than a million qubits to pose a genuine threat.

"Willow's capabilities, while impressive, do not yet pose an immediate risk to the cryptographic foundations. The estimated computational power required to compromise Bitcoin's encryption methods is still far beyond what Willow can achieve," said Balaji Srihari, Vice-President, CoinSwitch.

A call to action

Quantum computing could theoretically solve cryptographic puzzles faster than classical systems. However, the timeline to achieve such capabilities remains uncertain, says Sathvik Vishwanath, the co-founder and CEO of Unocoin. Willow's demonstration focuses on specific benchmarks rather than direct cryptographic attacks.

However, Mohammed Roshan Aslam, the co-founder & CEO of GoSats, feels that new cryptography practices and encryption methodology will have to be developed to address any potential challenge posed by Google's Willow.

Nearly 105 qubits fall short of the necessary 13 million qubits to complete Bitcoin's decryption, he pointed out. "If subsequent R&D in Google Willow manages to integrate such computational power in the future, cryptography and encryption developments may align with addressing this challenge. Additional software upgrades like hard fork in blockchain may be implemented to address this issue, but that may not be the ideal solution. For now, we have only limited understanding of Google Willow, and crypto and tech stakeholders will have to work in tandem to find an amicable solution for this."

The Willow development serves as both a breakthrough and a call to action, with quantum computing potentially reshaping financial systems, including Bitcoin, in the future. However, Unocoin's Vishwanath added, the Bitcoin community remains resilient, focusing on maintaining long-term security and technological advancements to counter potential quantum threats.

23. China Unveils Record-breaking 504-qubit Superconducting Quantum Computer

by CHEN Na
https://english.cas.cn/newsroom/cas_media/202412/t20241206_893281.shtml

China set a new domestic record on Thursday (05 Dec 2024) with the launch of the "**Tianyan-504**" superconducting quantum computer equipped with the 504-qubit "Xiaohong" chip, marking a significant milestone in the field of quantum computing.

The quantum computer was co-developed by the China Telecom Quantum Group (CTQG), the Center for Excellence in Quantum Information and Quantum Physics under the Chinese Academy of Sciences and QuantumCTek Co., Ltd., a leading quantum company based in east China's Anhui Province.

The "Tianyan-504" surpasses the 500-qubit chip threshold and also promises to match the performance of international quantum computing platforms like IBM in terms of qubit lifetime, readout fidelity and other key aspects, according to the CTQG.

This quantum computer will be integrated into the "Tianyan" quantum computing cloud platform, making it accessible to users worldwide.

"Tianyan," China Telecom's quantum computing cloud platform launched in November 2023, has received over 12 million visits from more than 50 countries, providing convenient and straightforward quantum computing services to global users.

Established in May 2023 in Hefei, capital of Anhui, the CTQG is a wholly-owned subsidiary of China Telecom, focusing on quantum technology research and development. (Xinhua)

24. The Road to Shor Era Quantum Computing – Executive Summary

by GQI

https://quantumcomputingreport.com/the-road-to-shor-era-quantum-computing-executive-summary/

Global Quantum Intelligence (*GQI*) *has just published a report titled The Road to Shor Era Quantum Computing in partnership with the NATO Innovation Fund (NIF). This report provides a comprehensive analysis of the current state of quantum computing and identifies the key factors that will determine the emergence of a dominant design able to break RSA 2048 encryption standards.*

An Executive Summary of the report is provided in the text below:

Quantum technology, and quantum computing in particular, promises to be a key driver of future economic opportunities and geopolitical advantage. A large number of quantum platforms are currently being pursued by developers around the globe, each with their own roadmap to scale-up their system and targeting a wide variety of high profile applications. However all current developers still face significant challenges and the race remains open. What can be said to inform investment decisions and priorities along this journey?

This report adopts the benchmark of a system capable of using Shor's algorithm to break RSA 2048 as the criteria against which to assess roadmap challenges. It argues that a system meeting this large scale test will be a strong contender to become the dominant quantum design, securing major economic advantages. We analyze the criteria required to assess roadmaps against this target, and develop a framework for how investments in this journey can be assessed.

To date, many quantum roadmaps have prioritized demonstrating short term incremental progress. We argue that long term investors should want to see the most difficult roadmap challenges targeted early, rather than left as issues for later stages of the journey. The inflection points this could unlock have the potential to accelerate the field.

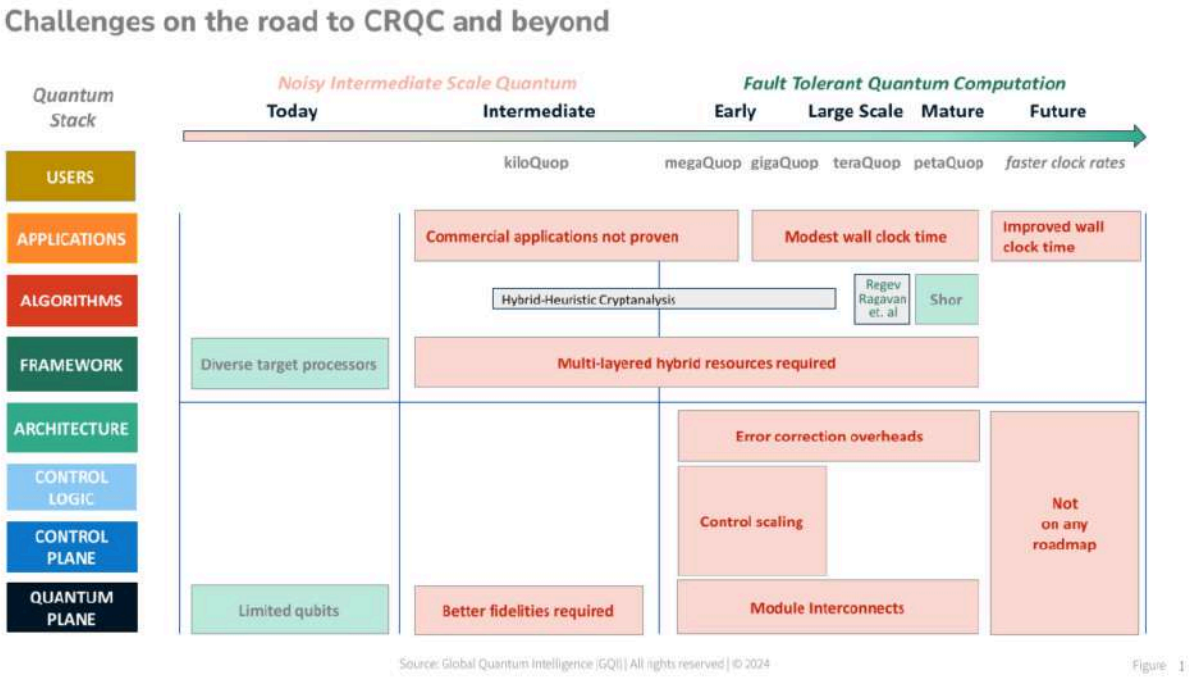
Quantum Technology is the largest paradigm shift in a generation. Our most fundamental description of nature, quantum mechanics, unlocks completely new resources not available via any other existing technology: true randomness, superposition and entanglement. Ultimately quantum tech, including computing, communications and sensing, will have a wide impact across all industry sectors. It will strengthen and accelerate other deep tech sectors, including biotech, AI & machine learning, robotics, crypto, blockchain and space.

Quantum computing (QC) is the most high profile sector of quantum technology. Quantum hardware itself is set to be comparatively slow compared to other modern computing hardware, but instead it gains its power from the unique algorithms it can implement. Benefiting from an exponentially expanded computational space and natively embodying the unique statistics of entanglement, it promises to perform certain computations beyond those practical on any Turing machine (i.e. any conceivable conventional computer). This is a new computing capability. The potential synergy it brings in simulating nature, quantum-simulating-quantum, is particularly compelling for many experts.

Many challenges remain. In particular, the power of intermediate scale quantum computers remains unproven. Some hope for significant commercial benefits with such systems. However, many believe that substantial benefits will require much larger systems. These will use quantum error correction (QEC) to deliver fault tolerant quantum computing (FTQC). Such devices will ultimately be capable of trillions of quantum operations (the teraQuop regime) and beyond.

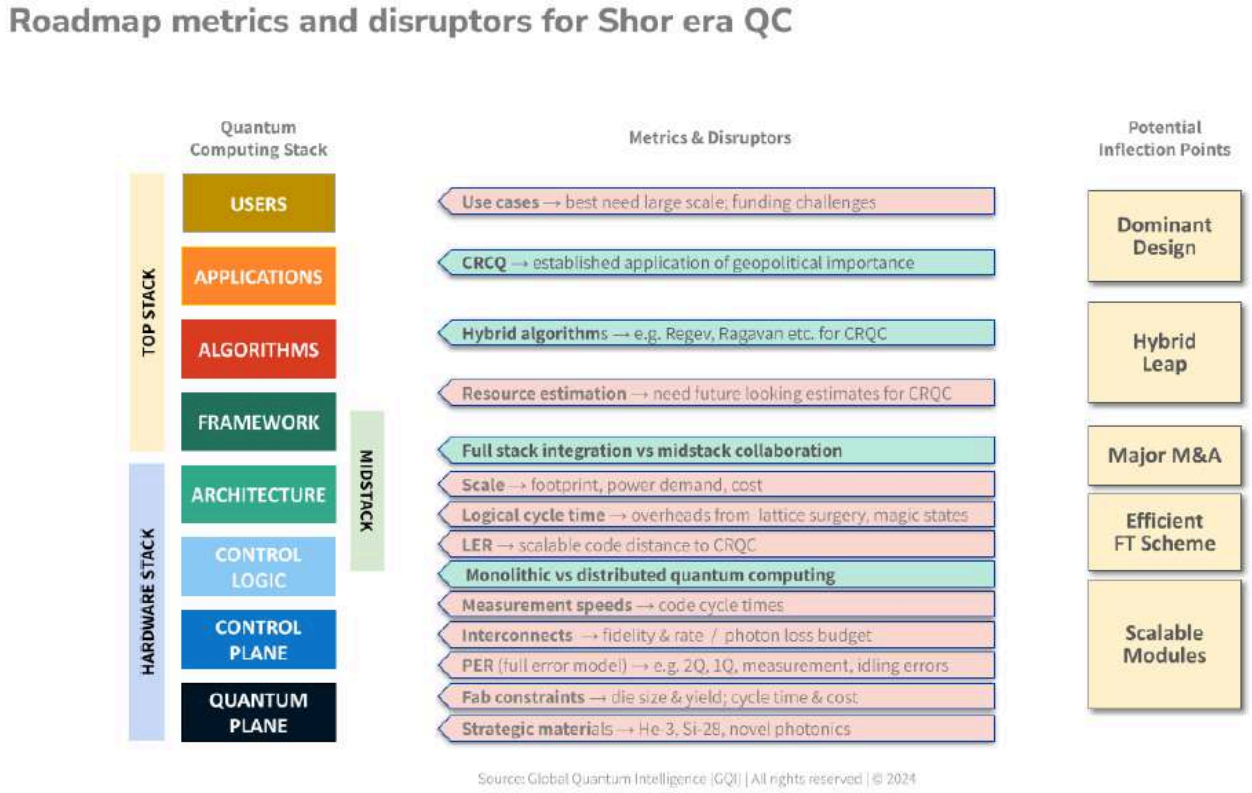
The NATO Innovation Fund (NIF) exists to help deep tech entrepreneurs in participating Allied Nations to tackle long term challenges such as this. It sees the quantum sector as a priority opportunity for such investment. In joint work, GQI and NIF have developed an approach to evaluate long-term quantum developer roadmaps.

Shor's algorithm for cryptanalysis provides a useful example of a well studied quantum algorithm with clear applications. Large scale quantum systems are expected to be able to break many of the public key cryptographic protocols in common use today in business and the Internet. We use the development of a cryptographically relevant quantum computer (CRQC), capable of breaking RSA 2048 encryption within a 1 day window, as a suitable benchmark against which to assess what it takes to create a truly large scale machine. Its significance however isn't just in its own utility, but also as a marker for other applications that machines of this scale are expected to be able to realize.



It is common to say that 'no one knows which platform will win this race. While GQI agrees with that overall assessment, we think that much can be said to inform the journey and at least rank the field. Particularly if we clearly identify that the goal is large scale computation. Against this background it is possible to identify the main challenges particular players face, and what are the time horizons within which their roadmaps seek to resolve them.

This report discusses the challenges at different layers of the tech stack in detail. We find that the baseline designs across all major qubit platform approaches still have many challenges to face (pink below). There are also potential disruptors, strategic questions or opportunities that could affect roadmaps across the sector (green below).



In particular we have identified potential inflection points, major advances that could significantly accelerate further progress.

- **Scalable Modules –** The sector needs to move beyond a selective focus on individual hero metrics, and isolated devices. We need to see this in robust multi-qubit devices with performance delivered across all required quantum operations within realistic speeds and a balanced and targeted error model. If these devices can also be provided with high quality couplers or interconnects; then that could open up dramatic progress via modular scaling. Conversely, without provision for the later, scaling potential is ultimately limited.

- **Efficient Fault Tolerance Schemes –** We don't dismiss the possibility that the well studied surface code may ultimately be the way we support QEC for large scale quantum computers. However we, and many in the field, are also excited about the disruptive potential of new novel QEC codes with dramatically higher encoding rates. More work is still required in fleshing out the practicality of the more demanding code cycles these require; enhanced connectivity (at reasonable rates and speeds) is probably key. Above all we need to see fault tolerant gate schemes defined and validated on top of these codes. Hidden in the detail are enticing opportunities to further reduce the overheads wired into other approaches (e.g. from lattice surgery and magic state production).

- **Major M&A –** Looking across the sector, it's easy to see that no individual player has all the best answers. There is a clear opportunity for value to be created by bringing together the best-of-breed technology and talent in new, and larger combinations. The pathway, vehicle and timing by which this will happen is less certain. Both industry and capital leadership are required. Unlocking substantial pools of capital to fund midscale growth to complete the quantum journey is a major upcoming challenge. Geopolitics is also set to shape this process.

- **Hybrid Leap –** It is already a tech industry trend to mobilize an hybrid mix of computing resources optimized to the problem at hand. The quantum computing sector has also realized for some time that a lot of classical computing power is going to be required just to make a quantum computer work. However we believe the opportunity runs deeper. In its early years, quantum computing has been dominated by a monolithic view of the available qubits. However, some of the most exciting recent quantum algorithmic progress (e.g. Lin-Tong in quantum simulation or Regev and Ragavan et. al. for cryptanalysis) has been explicitly built around breaking out large single quantum circuits into smaller pieces and moving parts of the algorithms onto classical resources. We believe that the provision of platforms able to support hybrid quantum/classical algorithm design, together with the opportunity presented by AI-assist, could unlock a new wave of algorithmic progress. Just as quantum hardware is expected to improve, quantum software improvements can play their part in closing the gap to quantum utility.

- **Dominant Design –** At the moment a plethora of different qubit technologies, and differing quantum platform designs are competing in the marketplace for attention and resources. We see the relative merits of these designs waxing and waning at different stages of scaling. Just as in the history of conventional semiconductors, we eventually expect a dominant design to emerge. We see building a CRQC as potentially the decisive battleground in establishing such a design. Once a clear forerunner and pathway is established, we expect investment and resources will drain away from the ecosystems surrounding other qubit platform technologies. Conversely the focus of resources will propel further a strong trajectory of continuing development.

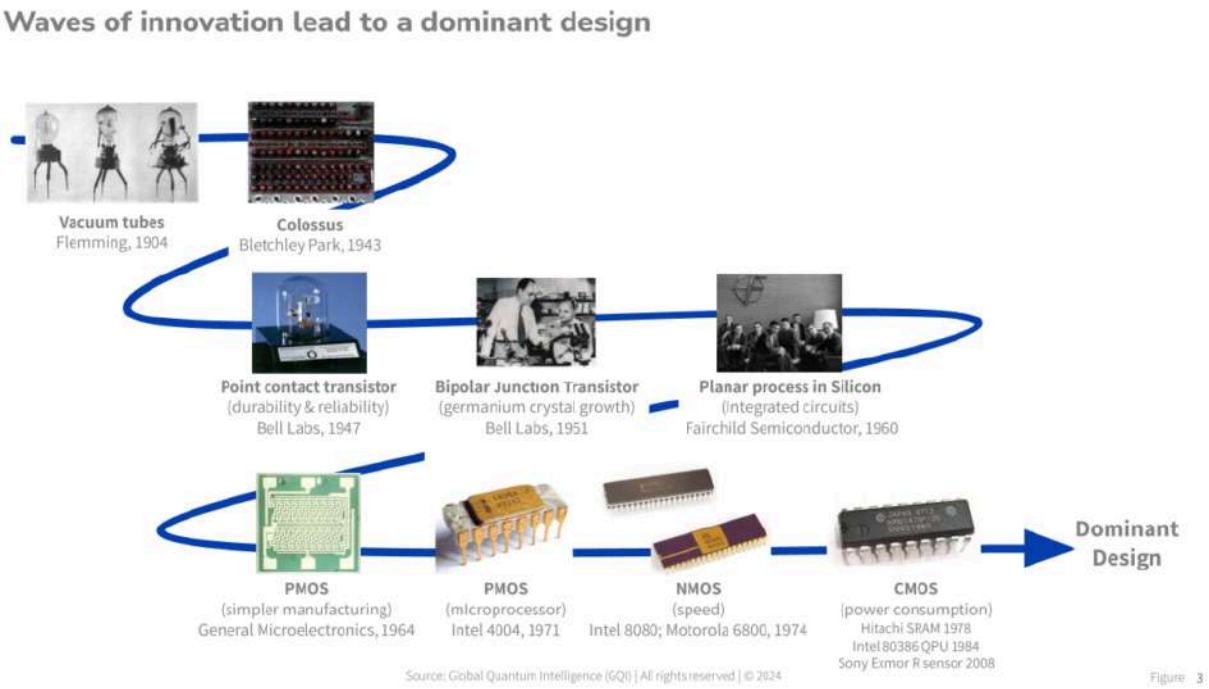


Figure 3

It is important to realize that different ecosystem participants have different objectives. Entrepreneurs naturally believe in their own technology, though they must ultimately also have a realistic assessment of when it is necessary to partner and seek integration via acquisition. Governments may be more interested in encouraging the development and relevance of their own quantum ecosystem rather than directly picking winners. Investors however have to make more specific choices, and also need the evidence base to support that.

This report introduces the challenge pathway framework to allow different roadmaps to be compared. These face different scaling challenges and address them at different scales and time horizons of system development.

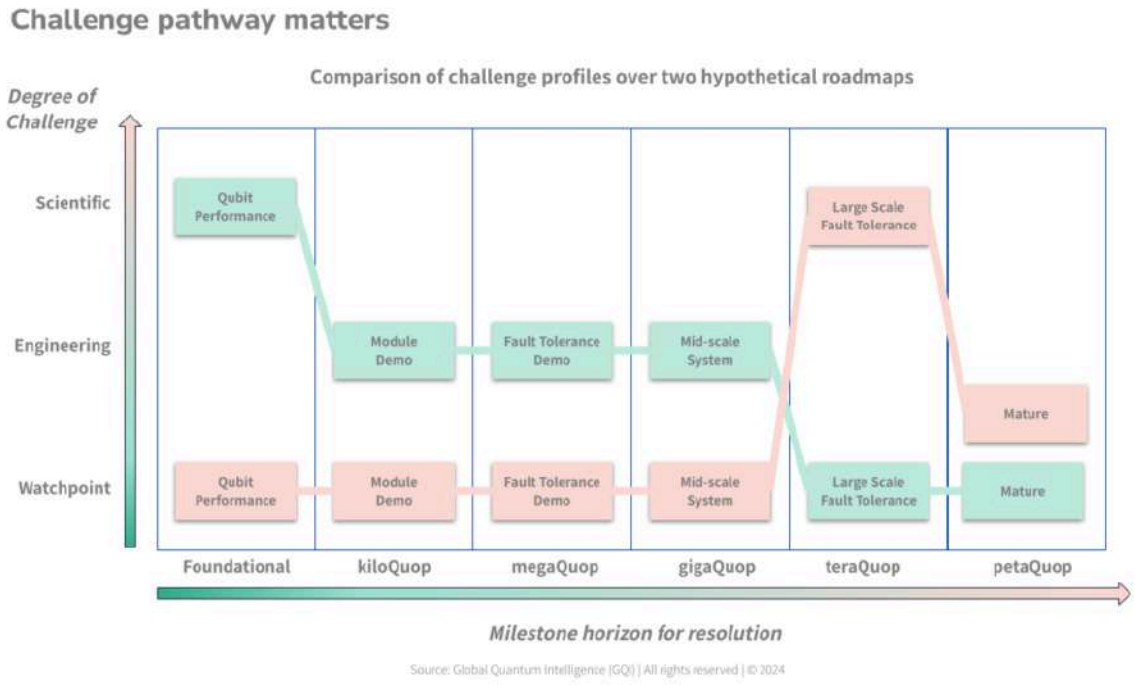


Figure 4

We find that this approach does provide useful calibration and differentiation of player approaches. We don't claim that one challenge pathway profile is appropriate for all ecosystem participants or will meet the investment thesis of all investors. However, for those investors focussed particularly on the long-term, large scale opportunity we argue that addressing the main challenges as early as possible in the roadmap should be preferable (the green pathway in the diagram). This is in sharp contrast to many early roadmaps examples. These have often favored early demonstrations of progress, promising some early commercial return and so supporting the next funding round.

Quantum technology is set to continue its exciting journey to deliver our 21st century future.

25. Where Cryptography Is Headed

by ADAM KOVAC
https://semiengineering.com/where-cryptography-is-headed/

Reports began surfacing in October that Chinese researchers used a quantum computer to crack military-grade AES 256-bit encryption. Those reports turned out to be wrong, but that did little to dampen concerns about what would happen if it was true.

The looming threat of quantum computers breaking today's encryption, and the stockpiling of encrypted data in preparation for a time when it can be decrypted, continue to haunt the security industry. The misinformation that was repeated by multiple news outlets was merely a precursor to the real thing.

"Work on that type of data structure has been going on in the higher-level crypto analysis communities for a very long time, and this particular paper completely overstated that this new technique was a quantum-based technique, so the headlines just ran with it," explained Scott Best, senior technical director, product management of Silicon IP at Rambus. "There's the expression that a lie makes its way around the world 10 times before the truth has time to put its pants on in the morning. Eventually the cryptographic community said, 'Everybody settle down.'"

The decryption did not break military-grade AES. "It was talking about this very esoteric structure that the community knows about," Best said. "They ran some simulations on the D-Wave quantum annealing cryptographic computer and had some interesting results, but it's nothing that we didn't know about. And it doesn't overachieve what we already can do with classical computers."

For the moment, at least, quantum-resistant cryptography appears to be secure. But the tech world isn't just sitting around waiting for the next attack. According to experts, quantum-resistant technology has been the most urgently worked on aspect of cryptography in recent years, despite quantum computers remaining enormously expensive and relatively rare. This is likely to remain the case for years, if not decades to come. While large-scale quantum computing has been on the receiving end of tens of billions of dollars in research, its widescale deployment does not seem to be imminent.

A McKinsey report estimates that quantum computers won't be able to function at scale until at least 2040.
But as the saying goes, it's wise to hope for the best and prepare for the worst.

"In terms of generalized cryptography, post-quantum cryptography is the biggest thing that has happened," said Mike Borza, a Synopsys scientist. "It's the idea of being prepared now for something that may happen in the future, and it's important. If you have a secret that you want to protect now, and you want to protect it for the next 50 years, then you should be using something that's quantum computer-resistant, because sometime in the next 50 years it's likely that a quantum computer at sufficient scale to crack conventional cryptography will be available."

Different solutions are being deployed, many of them resting on new algorithms that have been deemed quantum-secure by NIST. Some experts recommend focusing on larger key sizes. However, both of those developments come with complications, the latter requiring increasing amounts of compute, and the former having some mathematical vulnerabilities. The push to have more security on the edge and in IoT devices requires a shift left in implementing modern cryptography.

Key size a partial solution

When it comes to symmetric cryptography, Borza said making the key size bigger has been the most common approach for a post-quantum world. "If you want something that's 128 bits secure in a post-quantum-computing world, that means you need a key of 256 bits in size," he said. "That's pretty well understood for the conventional symmetric cryptography that we use today, and people are making that

change fairly easily because they're already accustomed to having keys of that size to protect top secret things."

But whether that's the best way forward is open to debate. "All AES encryption, all our banking, is secure because of 128-bit keys," said Prakash Madhvapathy, product marketing director at Cadence. "It's not factorable and it's secure. The design of these algorithms is not that easy to do and to make secure. It takes an army of cryptographers and analysts to design them. There are things called differential key attacks, where if you have four related keys that differ by only a few bits with each other – such as AES 256 bit, which has been hacked to the point where they say there is some weakness in the design of the substitution boxes – there is some residual linearity. If you give an analyst four keys that are 256 bits long, but they are very close to each other in terms of the number of the bit, they can crack the whole thing. The compute requirements to hack it now is not in the order of 2^56, but is now 2^96, which is worse than the 128 bits. The question is why should they use the 256-bit version when the 128-bit version, in the worst case, is more secure?"

Growing the key size requires additional computation, as well. Rambus' Best observed that the sheer scale of millions upon millions of secure data connections has necessitated the fine tuning of protocols of cryptographic strength.

"A lot of the work for getting these protocols right was, 'Exactly what does the key size have to be, and what is the cryptographic strength?'" Best said. "Sometimes cryptographic strength is as it was with RSA. RSA has a 2k bit size key that is less secure than the 4k bit size key, which is less secure than the 8k bit size key. AES 256 is a 32-byte key, which is more secure than AES 128. Sometimes security has that tradeoff of more and more data plus more and more processing power. A lot of the standardization effort over the last couple of years has been the fine tuning of the specification to ensure an effective tradeoff between key size, computation efficiency, and security."

Finding those optimal tradeoffs has been the result of tweaking relatively minor things, such as byte ordering. As Best explained, "When you deliver a piece of key material, when you deliver the construct of a key, and determine exactly what form public key is encoded in when it's delivered – and when there are different numbers of cycles, or when there is a different number of strength of algorithm – what type of initial initializations need to occur inside of the memory that is holding onto some of these pieces, such that the actual computation will remain secure?".

Borza said the trend of ballooning key sizes will continue when it comes to the levels above commercial-grade cryptography, with the same principle likely leading to the development of stateless hash-based solutions, which are the basis of NIST's FIPS 205, released in August 2024. For him, the real concern is asymmetric public key cryptography. "All of those algorithms do fall to a quantum computer of sufficiently large scale. If you have a secret that you want to protect for 50 years, you already need to be using something other than asymmetric cryptography, or using newer algorithms that stand up to the existence of a quantum computer, which allows you to solve the problem in parallel and effectively really reduce the key strength of a large asymmetric key. That's the whole focus of these NIST algorithms. You've got FIPS standards 203, 204, and 205, and there's also 206. 205 and 206 are the symmetric-based,

resilient algorithms, stateless hatch-based schemes, and the limitation of those is that you can use the keys once for different cipher texts. If you re-use the key across different cipher texts, then you produce what's essentially a mathematical exposure that allows the solution to be obtained, yet multiple texts that are encrypted with the same thing are no longer secure."

More compute resources needed

The introduction of these new algorithms creates its own set of issues. Lee Harrison, director of automotive IC solutions for Tessent at Siemens EDA, noted that the NIST algorithms are a lot more processor-intensive than their conventional counterparts. "They're a lot more involved than the lightweight algorithms that we had before, because they were kind of in the background and they just worked. These new algorithms take quite a presence."

That has particularly severe ramifications in areas where DFT is important, such as automotive. That issue is at the heart of a paper published by Harrison's colleague at Siemens, Janusz Rajski, which details an efficient, scalable cryptographic hash function.

"We did the research in that area because with design for testing, the logic and the technology that we add to customers' designs can't be too intrusive," said Harrison. "They don't want us to go and add a huge cryptography engine just for test access. Janusz did quite a bit of research in that area to really understand how he could minimize the footprint yet still provide a post-quantum type of algorithm."

The new FIPS standard comes as more processing is being done at the edge, which is necessitating some tough choices due to the impact on PPA. Because of the extra power requirements, Madhvapathy observed that how modern encryption is deployed needs to be considered early in the design process.

"The only reason to move such complex standards to the edge, in terms of implementation, would be if you have assets that you want to protect against such attacks," Madhvapathy said. "If such attacks are going to be more expensive than the assets themselves, which you can purchase directly, then the reasons for the attack goes away."

While beefed up security does necessitate tradeoffs, Harrison urged designers not to think of it as an additional cost, but part of the overall design cost. "The only time it really comes across as being an additional cost is if you add security at the end of the project," he said. "If security is integrated into your design process, then it's not costing you anything."

Crypto at the edge

That shift to the edge also comes as more and more computing is localized for performance and security reasons. While quantum-resistant crypto until now has been mostly reserved for sectors such as automotive and data centers, where cybersecurity is considered paramount, there are indicators that an increasing number of IoT/edge-based devices could soon receive the same consideration.

"When you think about what IoT devices typically are, you may wonder why security is needed for them," Harrison said. "But looking at what IoT devices are used for, a lot of them safety-critical and different types of applications. So having security within IoT is becoming quite common, and you'll see this kind of requirement grow over time."

In Europe, more stringent cybersecurity requirements are being mandated at the government level. This has ramifications for cryptography that go beyond the PQC realm and into key management, key rotation, management of certificates over time, and the ability to update keys. "No longer can you have a device with a key injected at fab and that is not managed afterwards," said Sylvain Guilley, co-founder and CTO of Secure-IC.

Effects on design

The need to adjust compute for more intensive algorithms already has begun to have real-world effects on design.

While cryptography is a complex issue for SoCs, Harrison said it presents a new set of problems at the chiplet level, where engineers must figure out how to provide security for a heterogeneous system. "Does it make sense to overload that kind of algorithm processing on every single chiplet, or would it make sense to have a single common cryptography engine on the device somewhere that all of the chiplets could access? The challenge is there's no universal standard around chiplet interconnect. So as much as it's a good idea at the moment, if you bundle a load of chiplets together, the chances of them all talking the same language is very remote."

The complexity of cryptography also has led to workflow adjustments. Guilley said it has become imperative to include an architecture team that will consider certification and security requirements early in the process. Adding on a security team with subject matter experts is also integral for turning requirements into functional feature.

Conclusion

The looming post-quantum era has led to new algorithms that are very compute-intensive. In turn, this has led to new ways of thinking about the tradeoffs involved in incorporating security into designs. This is especially important when it comes to applications like automotive, where DFT is critical.

While some experts have seen larger keys as part of the solution, others point out that turning to bigger keys can lead to other vulnerabilities. On top of that, advanced cryptographic techniques present unique challenges for chiplets, where the lack of a universal interconnect has made a common cryptographic engine an impossibility at present.

26. ALICE & BOB 2030 ROADMAP TO USEFUL QUANTUM COMPUTERS

by Dr. Raphaël Lescanne
https://alice-bob.com/blog/alice-bob-2030-roadmap-to-useful-quantum-computers/

Our Bet in Quantum Computing

Quantum computing is one of the most ambitious challenges in science and engineering today. Achieving "useful" quantum computers, ones that solve real-world problems, requires years of innovation, problem-solving, and relentless work.

When Théau and I started Alice & Bob in 2020, quantum computing was already progressing rapidly. Big players like Google and IBM were making headlines with their advances. But we made, or some might say, we had to make, a different choice.

We placed our bet on cat qubits, an emerging technology at the time, but one that promised to provide the strong foundation needed for practical, fault-tolerant quantum computing in a more efficient way.

Of course, this depended on one thing: being able to control the cat.

Why Cat Qubits?

Cat qubits are complex, not only a technological challenge, but also a deep physics problem. The principles behind them are intricate, even by quantum standards. But the payoff is worth it: with the right control, cat qubits provide a pathway to efficient error correction at scale. By focusing on quality over quantity, we can avoid massive hardware setups.

A single, well-controlled cat qubit is a strong building block for fault-tolerant quantum computers that are both powerful and efficient.

This was our bet: if we could demonstrate that cats are indeed protected from a whole class of quantum errors, as theory predicts, we could use a shortcut to the finish line to win the race, despite starting later and smaller than other players.

The Journey So Far

Thanks to the collective efforts of the entire community, and especially our talented team at Alice & Bob and our close academic partners, cat qubits are no longer just a bet.

We've made tremendous progress, and much of it is now testable on the cloud. Our cat qubits can be reliably manufactured and controlled, and we are scaling up to 16 cat qubits now. On Boson 4, our single-qubit device, we set a world record for bit-flip protection, 7 minutes, far beyond the tens of millisecond of other superconducting quantum systems. Boson 4 was launched on Google Cloud for everyone to access and test earlier this year, marking an important product milestone.

Theoretical breakthroughs are equally exciting. For example, we've shown that a quantum computer using cat qubits could run Shor's algorithm with up to 60 times fewer qubits than other approaches, and 200 times fewer when employing advanced error correction schemes. A few hundred thousand cat qubits could crack RSA encryption methods, whereas 20 million would be needed for competing architectures.

Looking back, our bet feels a bit less risky now.

Our Roadmap

With this solid foundation, the strategy gets clearer and we are able to share our roadmap to build a useful quantum computer by 2030. This roadmap outlines five key milestones that will bring us closer to achieving the first fault-tolerant quantum computer capable of solving real-world problems.

The Five Key Milestones

1. Master the Cat Qubit
2. Build a Logical Qubit
3. Fault-Tolerant Quantum Computing
4. Universal Quantum Computing
5. Useful Quantum Computing

Looking Ahead: Toward Practical Quantum Computing

As we continue to develop a useful quantum computer, our primary focus is on practicality. While the promise of quantum computing is widely recognized, the real challenge is making it achievable, in terms of cost, energy efficiency, footprint, and timelines, a problem that is not always talked enough about.

In this short blog post, I have mentioned several key concepts of quantum computing: qubits, quantum error correction, universality... However, for accurately understanding our strategy and, more broadly, for appreciating the real challenges facing the field, getting familiar with these concepts is essential.

This is why our roadmap was not published alone. It is the fourth and last section of our whitepaper, "*THINK INSIDE THE BOX: QUANTUM COMPUTING WITH CAT QUBITS*."The whitepaper is designed to help anyone, regardless of their background, grasp the most crucial aspects of quantum computing, as well as understand the cat qubit and why hardware efficiency is so critical.

27. The FBI now says encryption is good for you

by Jonny Evans
https://www.computerworld.com/article/3617118/the-fbi-now-says-encryption-is-good-for-you.html

Apple has been battling to maintain encryption for a decade. Two federal agencies now see it as a way to fend off foreign hackers.

Apple has faced an unequal battle in recent years as some lawmakers, the FBI, and regulators insist that the company create backdoors through which to access messages and other parts of its platform.

Apple and others have always insisted that there is no such thing as a safe backdoor, and that if one person has access, then it's only a matter of time until others gain access, too.

Use encryption for all your communications

Now, the FBI seems to agree.

In a recent security warning, the FBI and the US Infrastructure Security Agency have warned people to use encrypted apps such as iMessage and FaceTime for communication in order to retain security resilience against foreign hackers.

They also warn people to avoid using Rich Communication Services (RCS) when sharing messages between iPhones and Android devices, as RCS does not yet provide end-to-end encryption. (It is allegedly coming eventually, according to the RCS standards body, the GSMA). What this means is that Android and iPhone users should probably consider installing Signal for cross platform communications, which does provide cross-platform encryption.

Apple also continues to invest in encryption technologies to protect its customers, and recently introduced upgraded protection against future high-level attacks that use quantum computers to break into your communications.

An about face?

What's noteworthy about the FBI warning is that the agency has been battling Apple for years to convince it to put backdoors into its encryption – ostensibly to enable law enforcement. Apple has resisted so far, arguing that once you leave any form of vulnerability in any platform you are automatically placing customers at risk.

Knowledge of these back doors will inevitably slip outside the control of law enforcement into the hands of nation state attackers and – eventually – criminal groups, making everybody far less secure and placing

personal, commercial, and national interest at risk. Not only does such weakened encryption directly threaten personal privacy, it also undermines national security.

A former head of UK national security agency MI5 warned of this almost a decade ago, while Apple software Vice President Craig Federighi has similarly warned: "Weakening security makes no sense when you consider that customers rely on our products to keep their personal information safe, run their businesses or even manage vital infrastructure like power grids and transportation systems."

All the same, demands that Apple weaken platform security by diluting device encryption have remained. But with the attack environment now in a red zone, the FBI issued its warning about encryption.

It comes after a CISA warning concerning ongoing attacks by China-based hackers.

So, what is the FBI saying?

"Our suggestion, what we have told folks internally, is not new here: Encryption is your friend, whether it's on text messaging or if you have the capacity to use encrypted voice communication," said Jeff Greene, executive assistant director for cybersecurity at the CISA. "Even if the adversary is able to intercept the data, if it is encrypted, it will make it impossible [to use]."

The FBI also shared a recipe for security that should be on the desk of every IT purchaser. It recommends you use mobile devices that automatically receive timely OS updates, have encryption built in, and use multi-factor authentication for most collaboration tools. In other words, use a higher-end smartphone in preference to a low-end land-fill wannabe. Or, given that the best way to ensure security in your tech is to invest in secure products, use an iPhone, which has built-in encryption and is designed with a security-first agenda.

That focus on security likely reflects how Apple approaches the topic.

The next big war

After all, it was almost a decade ago that Apple CEO Tim Cook warned: "I think some of the top people predict that the next big war will be fought on cybersecurity. With hacking getting more and more sophisticated, the hacking community has gone from the hobbyist in the basement to huge, sophisticated companies that are essentially doing this, or groups of people or foreign agents inside and outside the United States. People are running huge enterprises off of hacking and stealing data.

"So yes, every software release we do, we get more and more secure," he said at the time.

Now, at last, the FBI seems to agree that encryption makes us safer. We really should keep using it, and reject arguments against doing so.

28. NVIDIA Launches cuPQC for Enhanced GPU-Accelerated Post-Quantum Cryptography

by Iris Coleman
https://blockchain.news/news/nvidia-launches-cupqc-gpu-accelerated-post-quantum-cryptography#google_vignette

NVIDIA introduces cuPQC, a GPU-accelerated software development kit, aimed at bolstering post-quantum cryptography for higher security against potential quantum computer threats.

NVIDIA has unveiled its latest innovation, the cuPQC software development kit (SDK), designed to enhance post-quantum cryptography (PQC) through GPU acceleration. This move aims to address the impending threat posed by quantum computers to current cryptographic systems, according to NVIDIA.

Addressing Quantum Threats

Quantum computing has advanced significantly over the past decade, raising concerns over its potential to compromise existing cybersecurity protocols. Algorithms such as those developed by Peter Shor could potentially crack widely-used encryption methods like RSA. In response, PQC has emerged as a crucial defense, utilizing cryptographic algorithms that resist both traditional and quantum attacks.

The urgency of adopting PQC is accentuated by "harvest now, decrypt later" strategies, where adversaries collect encrypted data today with the intent of decrypting it in the future as quantum capabilities evolve. This has led to new standards from the National Institute of Standards and Technology (NIST) and other global agencies mandating the use of PQC algorithms.

GPU-Accelerated Solutions

The cuPQC SDK offers developers a flexible, GPU-accelerated platform to transition from conventional cryptosystems to PQC protocols. By leveraging GPU hardware, the SDK can handle the larger key sizes and complex mathematical structures required by PQC algorithms, ensuring they are efficient and scalable.

In practical terms, applications in sectors like telecommunications, financial services, and cloud infrastructure stand to benefit from the high throughput cryptographic operations enabled by GPUs. These operations can be parallelized, enhancing both speed and performance, which is critical for research and the development of new PQC use cases.

Enhancing Transport Layer Security

Transport Layer Security (TLS), a fundamental internet security protocol, often faces computational challenges, especially when incorporating complex PQC calculations. cuPQC addresses these challenges by supporting high-throughput TLS applications. Utilizing NVIDIA's H100 SXM5 GPU, cuPQC achieves remarkable performance metrics, significantly outpacing current CPU capabilities.

For instance, with the NIST-approved PQC algorithm ML-KEM-768, cuPQC can perform up to 13.3 million key generations per second, showcasing a substantial improvement over traditional CPU-based solutions. This capability is vital in removing barriers to adopting PQC across industries.

Security and Integration

To further fortify security, cuPQC minimizes the need for data transfers between host and device by performing cryptographic processing directly on the GPU. This reduces latency and enhances efficiency, while also being robust against side-channel attacks.

cuPQC's integration with other cybersecurity frameworks, such as LibOQS, supports research into new cryptographic applications. According to Douglas Stebila from the University of Waterloo, this integration aids researchers in exploring new frontiers in cryptographic applications enabled by cuPQC's speed and functionality.

29.E.ON and IBM Quantum: Energizing the Future with Quantum Computing

by GQI

https://quantumcomputingreport.com/e-on-and-ibm-quantum-energizing-the-future-with-quantum-computing/

E.ON, one of Europe's largest energy companies, is leveraging quantum computing to address the growing complexity of energy distribution in a renewable-focused world. Partnering with IBM, E.ON is developing quantum algorithms to optimize energy pricing and hedge against risks such as weather volatility, shifting consumption patterns, and supply dynamics. This initiative aligns with E.ON's mission to maintain reliable and affordable energy supplies for its 47 million customers across 17 countries.

The partnership centers on creating algorithms that can outperform traditional Monte Carlo simulations in modeling energy risks. By integrating IBM's Qiskit and quantum hardware, E.ON is preparing for a future where quantum computing delivers significant efficiencies over classical methods. IBM projects that error-corrected quantum computers capable of such advancements will be operational by 2029.

E.ON's efforts underline the importance of investing in quantum expertise early. Dr. Giorgio Cortiana, E.ON's Head of Data & AI, emphasizes the need for industry collaboration and building internal quantum talent to stay competitive as quantum technologies evolve. The collaboration represents a step toward "quantum utility," with potential to revolutionize energy planning and pricing in the coming years.

30. AIVD, CWI, and TNO publish renewed handbook for quantum-safe cryptography

https://www.cwi.nl/en/news/aivd-cwi-and-tno-publish-renewed-handbook-for-quantum-safe-cryptography/

To prepare organizations for Q-Day, the day when quantum computers will be able to break certain widely used cryptography, the General Intelligence and Security Service (AIVD), Centrum Wiskunde & Informatica (CWI), and TNO are publishing a renewed handbook for quantum-safe cryptography. This extended second edition contains the latest developments and advice for transitioning to a quantum-safe environment, including more concrete advice on finding cryptographic assets, assessing quantum risks, and setting up cryptographic agility. It was presented on 3 December 2024 to the State Secretary for Digital Affairs and Kingdom Relations, Zsolt Szabó, during the 'Post-Quantum Cryptography' Symposium in The Hague.

Q-Day

Cryptography is used to protect data that should not be accessible by others. However, not every form of cryptography is safe against attacks by quantum computers. This Q-Day could occur within the next five to fifteen years, according to some experts. Malicious actors, such as hostile state actors, could then largely bypass certain contemporary cryptography. However, the risks to certain currently used cryptography begin today. This includes RSA and ECC (elliptic curve cryptography), which are used for encryption and digital signatures. Secured data can be intercepted today and then deciphered with a quantum computer from Q-Day onwards.

Additionally, transitioning to new cryptography might take ten years or longer. Therefore, organizations that work with important encrypted information – such as state or corporate secrets – must already be working on transitioning to a quantum-safe environment. This handbook helps organizations identify risks and provides concrete steps to work on a migration strategy.

Second Edition and PQChoiceAssistant

Since the publication of the first edition, more knowledge has been gained in the field of post-quantum cryptography (PQC). PQC is a collection of encryption methods that, unlike certain current methods, should be safe against attacks with quantum computers. This revised and extended second edition includes the latest developments and advice in the field of PQC. Additionally, several essential actions for

companies and organizations in the PQC migration have been examined in more detail. Furthermore, more concrete advice is included for inventorying cryptographic components in software used by organizations, assessing quantum risks, and cryptographic agility. It also provides a list of steps that are useful for any organization, regardless of the quantum threat ("no-regret moves"), and a detailed overview of PQC methods and international legislation. Practical experiences around the migration are also shared, and it includes the new advisory tool PQChoiceAssistant, which helps companies choose a PQC method.

European Cooperation

Since 2021, the CWI Cryptology research group and TNO have been organizing a series of symposia on post-quantum cryptography with the theme 'Act now, not later.' The aim is to bring government, business, and science together. The event on December 3 in The Hague, the 7th episode of this series, focused on internationalization and was organized with the help of the Ministry of the Interior and Kingdom Relations. One of the main topics was the development of the European Roadmap to make the European digital infrastructure quantum-safe. This roadmap should lead to a coordinated transition, with attention to interoperability, standards, and knowledge sharing within Europe. The Netherlands plays a leading role in this, together with Germany and France. These three countries jointly coordinate the EU working group.

31. Optalysys collaborates with Zama to supercharge Fully Homomorphic Encryption (FHE) development

https://optalysys.com/optalysys-and-zama-partnership/

Zama's software solutions provide powerful tools that enable a wide range of cutting edge applications for FHE, including encrypted machine learning and advanced confidentiality in blockchain smart contracts. As sectors worldwide, such as financial services, healthcare and defence, adopt and integrate more digital technologies, the risks associated with cyber threats grow significantly. Current cybersecurity solutions have significant limitations in protecting data in use, which is why the adoption of privacy-enhancing technologies (PETs) such as FHE, are fundamental for companies in protecting sensitive data. FHE is an advanced, quantum-resilient cryptography method that allows encrypted data to be processed without ever needing to be decrypted. It allows organisations to process data whilst maintaining privacy, opening up opportunities for safe collaboration across industries, even in untrusted environments.

The partnership aims to bridge the gap in FHE adoption by addressing its historically high computational demands. Integrating Zama's software solutions with Optalysys' Enable technology will maintain the ease of use of Zama products for developers while providing access to faster and more scalable FHE application deployments. It will allow the use of encrypted data for high-security applications across various sectors.

cDr Nick New, CEO of Optalysys, said, "Our partnership with Zama is a significant step for us as we continue to accelerate the development of FHE. Historically, scaling FHE applications has been a challenge due to its demand for specialist infrastructure and computing power. Our work with Zama aims to overcome this barrier and enable us to develop this revolutionary technology at a rapid pace."

Rand Hindi, CEO, Zama, said, "At Zama, our mission is to equip developers with the best FHE tools – tools that are easy to use, practical, and fast. Our collaboration with Optalysys is an exciting step toward making FHE faster, a crucial milestone in our journey to make this technology ubiquitous.

"We believe that this acceleration benefits machine learning applications and is equally transformative in the blockchain space, a key focus for us, where FHE has the unique ability to resolve the long-standing tension between transparency and confidentiality, unlocking new possibilities for privacy-preserving innovation onchain."

32. How MSSPs Can Prepare Clients for Post-Quantum Computing Threats

by Karthik Kannan
https://www.msspalert.com/perspective/how-mssps-can-prepare-clients-for-post-quantum-computing-threats

Around the world, the quantum community is making huge progress in creating stable, commercially viable quantum computers. As the idea of quantum technology becoming a part of everyday applications becomes more realistic, there's a growing sense of uncertainty.

Recently, NIST released an Initial Public Draft (IPD) report outlining a roadmap for transitioning from traditional public-key cryptographic algorithms to standardized post-quantum cryptography (PQC). This includes a transition plan, including timelines and key considerations for migration, aimed at helping federal agencies, industries, and standards organizations transition their Infrastructure, products, and services to PQC-ready by 2035. The report also includes a list of current and widely-used key establishment and digital signature algorithms that will soon be deprecated.

NIST also points out that transitioning from algorithm standardization to full integration into information systems can take anywhere between 10 to 20 years. Given the time it takes and the rise of "harvest now, decrypt later" attacks, it's more important than ever for organizations to start preparing for post-quantum cryptography (PQC) now. NIST's report serves as a vital resource, offering clarity and direction to help begin and speed up the PQC adoption journey.

Quantum machines could potentially break traditional encryption methods, putting sensitive information at risk. For businesses, getting ready for these threats is no longer optional—it's a necessity. This is where

Managed Security Service Providers (MSSPs) can aid in, offering valuable consultation service, support and Implementation plan.

Why Post-Quantum Security Matters

Current encryption methods, like RSA and ECC, rely on complex math problems that are hard for regular computers to solve. However, quantum computers, using algorithms like Shor's, can break these encryptions much faster. Knowing that a large-scale quantum computer could effortlessly break today's cryptographic algorithms like RSA, DSA, ECDH, ECDSA, and EdDSA and expose sensitive, confidential data means businesses' financial data, intellectual property, and customer information could be at risk; and a major concern for many CISOs.

Migration to PQC is a much more complex undertaking when compared to other cryptographic migrations from the past. The new PQC algorithms have significantly different properties from the current algorithms in terms of key sizes, signature sizes, key exchange, computational requirements, entropy, and others. Naturally, the challenges in migration are multifaceted, involving changes to infrastructure, algorithms, applications, and compliance frameworks. MSSPs must help organizations plan extensively, ensuring that their systems are robust enough to handle the demands of PQC while maintaining seamless operations.

History and Background of PQC Algorithms

Before we dwell on the role of MSSPs, let us understand a bit about the NIST's finalized PQC encryption algorithm standards and the key factors to consider for the PQC migration.

2016

In 2016, NIST kicked off the Post-Quantum Cryptography (PQC) Standardization Project aimed at developing trusted and tested PQC encryption algorithms that are secure against attacks by both classical and quantum computers.

2022

In July 2022, after the third round of the standardization process, NIST made a preliminary announcement, unveiling the first four selected algorithms:

- **CRYSTALS-Kyber** for KEM (Key Establishment Mechanism) for general encryption
- **CRYSTALS-Dilithium, Falcon,** and **SPHINCS+** for digital signature schemes

2023

In August 2023, NIST released the Initial Public Drafts (IPD) of three of the above algorithms to get industry feedback and make appropriate revisions.

2024

A year later, after completing the fourth round of standardization, on August 13, 2024, NIST released the finalized PQC encryption algorithm standards with name changes:

- **FIPS 203:** Referred to as ML-KEM, based on the CRYSTALS-KYBER algorithm for general encryption
- **FIPS 204:** Referred to as ML-DSA, based on the CRYSTALS-Dilithium algorithm for digital signatures
- **FIPS 205:** Referred to as SLH-DSA, based on the SPHINCS+ algorithm for digital signatures

The Critical Role of MSSPs in Achieving Crypto-Agility

Rising cyber threats mean more chances for managed security service providers. The world of PKI is transforming rapidly, driven by an unprecedented growth of machine (non-human) identities and disruptions like the shift towards shorter TLS certificate validity, Certificate Authority Browser (CA/B) Forum rulings, post-quantum cryptography, and new compliance mandates. As disruptions intensify and become more common, crypto-agility has become critical to adapt, stay the course, ensure security, and preserve digital trust.

Gartner forecasts global spending on security and risk management to reach $215 billion in 2024, up 14.3% from 2023's $188 billion.

Gartner forecasts that spending on security services including consulting, IT outsourcing, implementation and hardware support will total $90 billion in 2024, an 11 percent increase from 2023. Security services are expected to represent 42 percent of total security and risk management end-user spending.

With the complexities of the PQC transition, MSSPs can play a crucial role in helping organizations strengthen their security against quantum threats through a strong Crypto-Agile framework. Achieving crypto-agility is a journey, but with the right solutions, this transition becomes seamless and sustainable, ensuring robust mitigation ahead of emerging threats.

Here's how MSSPs can help:

1. PQC Risk Assessment and Readiness

MSSPs can partner with key cybersecurity vendors to create awareness across CISOs and Security architects. A consultative security service to their customers through a phased approach and a comprehensive assessment of an organization's cryptographic infrastructure would be key. Identifying vulnerable systems and educating clients about the implications of quantum computing can be a critical first step toward preparedness.

2. Implementing Quantum-Resilient Algorithms

MSSPs can stay ahead by using quantum-safe algorithms recommended by organizations like NIST. They can help clients gradually switch to these algorithms as part of a broader plan to prepare for post-quantum security.

3. Crypto Agility

MSSPs can collaborate with OEMs to help organizations build a comprehensive crypto-agile framework, enabling critical systems to quickly adapt to evolving cryptographic standards. With shorter TLS validity, certificate compromises, and post-quantum threats on the horizon, MSSPs need to ensure that organizations can be crypto-agile to ensure security and compliance. This flexibility is key to minimizing disruption during the transition to post-quantum solutions across their customers.

4. Cost-Effective Transition

For many enterprises, the cost of transitioning to post-quantum security can be daunting. MSSPs offer scalable, cost-effective solutions tailored to their clients' needs, eliminating the need for significant in-house expertise or resources.

Preparing Today for Tomorrow's Threats

Cryptography is foundational to internet security, and crypto-agility is crucial to staying ahead of evolving threats and preserving digital trust. Quantum computing may still be years away from mainstream adoption, but the risks it presents demand action now. MSSPs provide the expertise, tools, and proactive strategies to help businesses secure their digital assets in a post-quantum world.

33. The Origins of Lattice Cryptosystem

by Gokul B Alex
https://medium.com/akkadia/the-origins-of-lattice-cryptosystem-46428c9d1fae

Lattice cryptography is in vogue in recent times. This is a brief note on the historic origins of hard problems related to lattices. It was Miklos Ajtai, a Hungarian mathematician working in IBM who popularized the hard problems related to lattices. He published the seminal work on lattices titled as 'Generating Hard Instances of Lattice Problems' in 1996. He had landed in the world of lattices in search of a technique beyond the world of factorization problems.

He was working on Pigeonhole Principle and propositional logic which was published in the late 1980s and early 1990s. His influential paper, "The Complexity of the Pigeonhole Principle," was presented at the 29th Annual Symposium on Foundations of Computer Science (FOCS) in 1988. He demonstrated that the Pigeonhole Principle cannot be proved with polynomial-size, constant-depth Boolean formulas, highlighting the inherent complexity of this principle in propositional proof systems

It is interesting to see that the insights from the work on Pigeonhole Principle are found in his work on lattice cryptosystem. In the foundation work on lattices mentioned earlier, Ajtai goes into the historic roots of lattice problems. According to Ajtai, the question of finding a short vector in a lattice was already formulated by Dirichlet in 1842, in the form of Diophantine approximation problems.

Diophantine approximation often involves counting lattice points within certain geometric shapes, such as spheres or ellipsoids. The distribution of these points can provide insights into how well real numbers can be approximated by rationals. It is worth mentioning the contributions of Hermann Minkowski at this juncture. Minkowski studies the relationships between convex bodies and lattice points. His framework has provided tools for solving Diophantine approximation problems by analyzing the geometry of lattices.