Crypto News

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

March 03, 2025

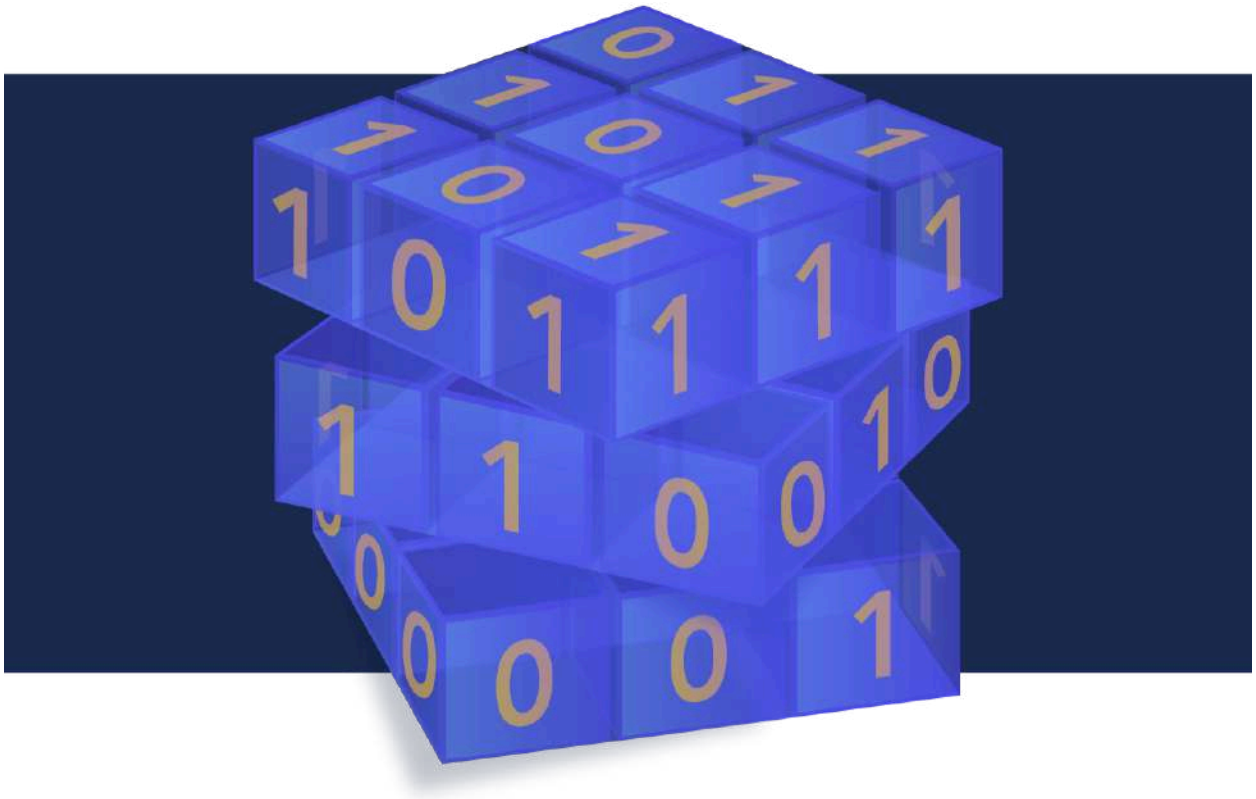


Table of Contents

Editorial

Happy Spring Readers! Let's start with the exciting news that you may have already heard of – Microsoft's Majorana 1. Microsoft isn't the first company to release a quantum circuit that claims to be fault-tolerant. That would go to Google's Willow back in December and since Microsoft's announcement, also to Amazon's Ocelot which came a mere week after Microsoft's announcement. What's exciting about Microsoft's announcement is the type of technology used. The 3 largest Cloud providers in the world are using 3 different methods to create a fault-tolerant quantum circuit. When it comes to Microsoft, they took the extra step of claiming to create the world's first topconductor. A true scientific breakthrough in itself as it utilizes a new state of matter previously only theorized – Majorana quasiparticles. It is theorized, that it would have the ability to scale up to 1 million qubits on a single circuit if they are able to create Majorana Zero Modes (MZM). With DARPAs stamp of approval and the scientific communities rallying around the topconductor technology as being more stable, it seems Microsoft may win the fault-tolerant quantum circuit race that may lead to the first quantum computer showing an advantage. I wouldn't count Google and Amazon out just yet though. Only time will tell which of these 3 tech giants will win in the end since some of the technology still needs to get past proof of concept, including the technology at Microsoft. Make your way to article 7 and 9 to learn more about the science and facts behind Microsoft's Majorana 1.

We've talked so much about Majorana 1 but in the International Year of Quantum, there's so many other topics we need to get updated on. The world's first hybrid quantum supercomputer has gone online in Japan. Reimei is a 20-qubit quantum computer which is now integrated with Fugaku which is "the world's sixth fastest supercomputer". A hybrid quantum-classical computer is the natural interim step needed to eventually reach a quantum advantage. Read article 14 for more. The USG has also not pulled back on PQC adoption and the use of cryptography. Read more in article 15 from one our own veteran working group members Jaime Gómez García. In line with this push for quantum-safe encryption, read article 20 and 22 for your call to action to secure your data before you become obsolete. With so many other interesting articles, I'll leave it up to you to peruse the newsletter and tell me which one struck your fancy. Happy reading!

The Crypto News editorial is authored by the co-Chair of the Quantum-Safe SecurityWorking Group (QSS WG) of the Cloud Security Alliance (CSA), Mehak Kalsi, MS, CISSP, CISA, CMMC-CCP and it is compiled by Dhananjoy Dey.

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

1. EU project recommends QR cryptography protocols

by Evie Kim Sing
https://identityweek.net/eu-project-recommends-qr-cryptography-protocols/

The European Commission signposted quantum resistant cryptography as the future for electronic machine-readable travel documents (eMRTDs). The threats from quantum have changed the mindset of stakeholders in a two-year project, funded by the Commission, to move towards the post era of quantum computing and standardise resistant cryptographic protocols.

Despite quantum rapidly accelerating, with substantial investments from both public and private sectors, it presents complex security challenges to "classical cryptography" as the capacity of quantum computers expands. The stance of the EU Commission encourages collaborative efforts from member states to "harmonise" safe cryptography to ensure the EU's digital infrastructures are secure in the next digital era.

Quantum was considered the new technological advancement of encrypting data, provisioning many social and economic benefits. However, understanding that quantum cryptography could be more secure than traditional cryptography has been dismantled, with the security of the system being flawed.

The digital security industry is saying that QR standards and infrastructures need to be developed to protect classical cryptography which is under threat from the continued advancements of quantum.

The European Commission states *"It is vital that communications remain protected in the future for the security of our citizens, societies, economies and the EU's digital single market"*. The recommendation published in April 2024 has been followed by the European initiative, the PQC4eMRTD (Post-Quantum Cryptography for electronic Machine-Readable Travel Documents) project.

The project is coordinated by key vendors, Infineon Technologies AG in partnership with Thales and CryptoNext Security, the Barcelona Supercomputing Center from Spain, and the Institute for Comparative Law at the Faculty of Law in Ljubljana, Slovenia. Standardising global QR protocols is high on the agenda and the project will promote synergy between different sectors to create a "detailed blueprint for Europe's transition to PQC".

2. How to Overcome the Quantum Threat

by Lisa Morgan
https://www.informationweek.com/cyber-resilience/how-to-overcome-the-quantum-threat

Quantum computing is expected to solve complex problems, but the technology has a dark underbelly, which is its ability to render classical encryption obsolete. That means every file at rest and in motion is at risk without limitation.

"[T]he advent of quantum computing is a game-changer -- a double-edged sword that demands both urgency and precision in response," says Timothy Bates, AI, cybersecurity, blockchain and XR professor of practice at University of Michigan and former Lenovo CTO, in an email interview. "Quantum computing has the potential to render our current encryption methods, like RSA and ECC, obsolete almost overnight. It's not a question of if but when. That 'when' could be sooner than we think given the accelerating pace of quantum advancements. The implications for secure communications, financial systems and even national security are staggering."

As Always, Bad Actors Have an Edge

The potential "winners" of the cryptography threat are countries unbound by strict ethical or regulatory frameworks. Bates says they will leverage quantum to breach security protocols without hesitation. Quantum-as-a-service (QaaS) platforms lower the bar for malicious actors, and the asymmetry between regulatory-constrained organizations and rogue entities gives the latter a significant edge.

"Quantum-safe encryption must be prioritized. The industry needs to fast-track the development of post-quantum cryptographic standards and embed them into critical systems now, not later. Collaboration between quantum computing pioneers, cybersecurity leaders and regulators will be crucial to staying ahead," says Bates. "Governments must adopt policies that encourage responsible quantum development while creating international standards to deter misuse."

He also believes that CIOs, CTOs, and CISOs must band together to share intelligence, pool resources, and test emerging quantum technologies in controlled environments because no one can tackle the problem alone.

3. Fortanix Expands Encryption Platform with NIST's Post-Quantum Cryptography Standards

by HPC
https://www.hpcwire.com/off-the-wire/fortanix-expands-encryption-platform-with-nists-post-quantum-cryptography-standards/

Fortanix, a leader in data-first cybersecurity and a Confidential Computing pioneer, today announced new capabilities to its data encryption and key management platform. Even as organizations struggle to manage the rising costs and complexity of data security, advances in AI and quantum computing will render current protections obsolete.

Quantum computers will be able to break most widely used public key cryptographic algorithms, putting long-term sensitive data at risk, and recent innovations in the field signal it could happen sooner than expected—customer information, PII, employee records, and proprietary company and product details are vulnerable. For example, encrypted data is being stolen today with the intent to decrypt it in the future, once quantum computing becomes available.

In response to rapidly escalating risks, the NSA and NIST introduced new quantum-resistant cryptographic algorithms last quarter. Fortanix has incorporated the full suite of CNSA 2.0 algorithms into its data encryption and key management platform, and now supports:

- Leighton-Micali Signature (LMS)
- Xtended Merkle Signature Scheme (XMSS)
- Advanced Encryption Standard (AES)
- Secure Hash Algorithm (SHA)
- CRYSTALS-Kyber (ML-KEM)
- CRYSTALS-Dilithium (ML-DSA)

Companies that use the Fortanix platform for their data encryption and key management will benefit immediately:

- Mitigates the risk—and associated costs—of exposing companies' most valuable data to advanced AI and quantum computing threats.
- Accelerates regulatory compliance: the U.S. government's NSM-10 requires agencies to develop a plan to transition to new algorithms within one year of updated standards, with full migration by 2035. Additionally, regulations such as PCI DSS 4.0, effective April 2025, already mandate strict adherence to secure cryptographic protocols.
- Meets the growing demand from both the market and consumers for robust data security when engaging with or transacting through a company's technology.

"The start of a PQC readiness journey is far from trivial—understanding where and how cryptography is applied is extremely complex," said Anuj Jaiswal, Chief Product Officer at Fortanix. "Most enterprises lack full, immediate visibility into their cryptographic footprint. With Fortanix, enterprises can not only discover and assess the risk of cryptographic assets that are not quantum resistant, but they can also achieve needed crypto agility to do PQC transition at scale."

"With NIST setting firm deadlines—2030 for initial adoption of post-quantum cryptography and 2035 for full phase-out of legacy algorithms—organizations can't afford to delay their PQC transition journeys," said Tomas Gustavsson, chief public key infrastructure officer at Keyfactor. "These deadlines are designed to drive a proactive shift towards ensuring all organizations are prepared before quantum-enabled breaches are a reality. All organizations have a leg in the race against quantum threats, meaning all must act now to ensure a smooth transition. Keyfactor is proud to partner with Fortanix to give organizations the tools they need to stay ahead of this critical shift."

4. Google Announces Quantum-Safe Digital Signatures in Cloud KMS, Takes "Post-Quantum Computing Risks Seriously"

by Esther Shein
https://www.techrepublic.com/article/google-cloud-kms-quantum-safe-digital-signatures/

Google announced on Thursday (20 Feb 2025) the development of quantum-safe digital signatures (FIPS 204/FIPS 205) in Google Cloud Key Management Service (Cloud KMS) for software-based keys. This is available in preview.

The search giant also provided a high-level view into its post-quantum strategy for Google Cloud encryption products, including Cloud KMS and the Cloud Hardware Security Module (Cloud HSM).

Mounting concern over public-key cryptography systems

This is significant, the company said, because the security of many of the world's most widely used public-key cryptography systems has increasingly become a concern as experimental quantum computing continues to advance. Large, cryptographically-relevant quantum computers have the potential to break these algorithms.

However, post-quantum cryptography (PQC) can use existing hardware and software to mitigate these risks. New PQC standards from the National Institute of Standards and Technology (NIST) became available in August 2024, enabling tech vendors around the world to begin PQC migrations.

"At Google, we take post-quantum computing risks seriously," wrote Jennifer Fernick, a senior staff security engineer, and Andrew Foster, engineering manager of Cloud KMS, in a Google Cloud blog post. "We began testing PQC in Chrome in 2016, we've been using PQC to protect internal communications since 2022, and we've taken additional quantum-computing protective measures in Google Chrome, Google's data center servers, and in experiments for connections between Chrome Desktop and Google products (such as Gmail and Cloud Console)."

Google's approach to quantum-safe Cloud KMS

Google detailed steps the company is taking to make Google Cloud KMS quantum-safe, which include:

- Offering software and hardware support for standardized quantum-safe algorithms.
- Supporting migration paths for existing keys, protocols, and customer workloads to adopt PQC.
- Quantum-proofing Google's underlying core infrastructure.
- Analyzing the security and performance of PQC algorithms and implementations.

- Contributing technical comments to PQC advocacy efforts in standards bodies and government organizations.

Pledging open-source availability

Google's Cloud KMS PQC roadmap supports the NIST post-quantum cryptography standards (FIPS 203, FIPS 204, FIPS 205, and future standards), which can help customers perform quantum-safe key import and key exchange, encryption and decryption operations, and digital signature creation, according to the company.

The software implementations of these standards will be available to Cloud KMS clients as open-source software and maintained as part of the Google-authored, open-source cryptographic libraries BoringCrypto and Tink, Fernick and Foster wrote.

Quantum-safe digital signatures are now available in Cloud KMS, so customers can use Google's existing API to cryptographically sign data and validate signatures using NIST-standardized quantum-safe cryptography with key pairs stored in Cloud KMS.

"This unblocks the essential work of testing and integrating these signing schemes into existing workflows ahead of wider adoption,'' Fernick and Foster explained. "It also can help ensure that newly-generated digital signatures are resistant to attacks by future adversaries who may have access to cryptographically-relevant quantum computers."

5. SEALSQ highlights need for post-quantum security

https://www.investing.com/news/company-news/sealsq-highlights-need-for-postquantum-security-93CH-3880685

TSEALSQ Corp, a subsidiary of WISeKey specializing in advanced cybersecurity technologies and currently generating $20.14 million in trailing twelve-month revenue, today emphasized the importance of post-quantum cryptography (PQC) in light of recent quantum computing developments by Microsoft. The tech giant's progress in creating a Majorana-based quantum chip underscores the urgency for quantum-resistant security measures as traditional encryption methods become increasingly vulnerable.

SEALSQ's suite of post-quantum security solutions includes PQC embedded within a robust Quantum-Resistant Public Key Infrastructure (PKI) and Post-Quantum Secure Elements designed for IoT, automotive, and critical embedded systems. The company's Quantum Lab provides best practices and guidance for organizations preparing to upgrade their systems to be quantum-ready. According to InvestingPro data, the company's stock has shown remarkable momentum with a 502% return over the past six months, though analysts anticipate sales decline in the current year.

The company's focus on integrated solutions based on semiconductors, PKI, and provisioning services, along with the development of post-quantum technology hardware and software products, positions SEALSQ as a key player in the transition to quantum-resistant encryption. This transition is crucial for sectors like banking, healthcare, and critical infrastructure, which rely heavily on digital communications and are at risk of being compromised by quantum computing capabilities. InvestingPro subscribers can access 12 additional investment tips and comprehensive financial metrics to evaluate SEALSQ's market position and growth potential.

SEALSQ's long-standing collaboration with Microsoft, including joint efforts within the Tech Accord and the integration of WISeKey's cybersecurity solutions into Microsoft platforms, demonstrates a shared commitment to enhancing digital security in the face of evolving threats. While the company maintains a strong current ratio of 3.58 and operates with moderate debt levels, InvestingPro analysis indicates the stock is currently trading above its Fair Value.

The information for this article is based on a press release statement from SEALSQ, and it reflects the company's current views regarding future events and financial performance. These forward-looking statements are subject to risks, uncertainties, and assumptions, and actual results could differ materially from those projected. SEALSQ has not committed to updating any forward-looking statements as new information becomes available.

In other recent news, SEALSQ Corp has made significant advancements in the field of cybersecurity and quantum-resistant technology. The company announced the development of a new cryptographic solution, Quantum RootCA, in collaboration with the OISTE.ORG Foundation, expected to launch in early 2025. This solution aims to safeguard digital identities and communications against the potential threats posed by quantum computing. SEALSQ is also set to unveil its QS7001 secure hardware platform at the NY Quantum Day, designed to handle post-quantum cryptographic algorithms and withstand potential quantum computer attacks. In addition, the company has launched a line of post-quantum semiconductors aimed at decentralizing AI development, promoting a sustainable AI future. SEALSQ's MS600X Secure Hardware Platform has received the Common Criteria EAL5+ Certification, and its VaultIC 408 microcontroller is on track for FIPS 140-3 Certification. These certifications underscore SEALSQ's commitment to maintaining high security standards. Furthermore, SEALSQ's secure microcontrollers are being integrated into drones for enhanced security, with notable partnerships in the defense sector. These developments position SEALSQ as a key player in the transition towards quantum-resistant encryption and secure technology solutions.

6. Will quantum computers disrupt critical infrastructure?

by Joe Fay
https://www.bbc.com/news/articles/cpq9zxxn72qo

Twenty five years ago computer programmers were racing to fix the millennium bug amidst fears that it would cause banking systems to crash and planes to fall out of the sky.

Much to everyone's relief the impact turned out to be minimal.

Today, some fear there is a new critical threat to the world's digital infrastructure. But this time, we cannot predict exactly when it will move from theory to reality, while the ubiquity of digital technology means fixing the problem is even more complicated.

That's because the arrival of quantum computing means that many of the encryption algorithms that underpin and secure our hyperconnected world will be trivially easy to crack.

Quantum computing is radically different to the "classical" computing used today. Instead of processing binary bits which exist in one of two states – one or zero, on or off – quantum computing uses qubits, which can exist in multiple states, or superpositions.

"The reason why it's so powerful is because you're doing all those possible computations simultaneously," Prof Nishanth Sastry, director of research for computer science at the University of Surrey, explains. This means it's "much, much more efficient, much, much more powerful."

This means quantum systems offer the possibility of solving key problems that are beyond classical computers, in areas such as medical research and materials science, or cracking particularly complex mathematical problems.

The problem is some of those same mathematical problems underpin the encryption algorithms that help to ensure trust, confidentiality and privacy across today's computer networks.

Today's computers would take thousands, even millions of years, to crack current encryption standards, such as RSA. A suitably powerful quantum computer could, theoretically, do the job in minutes.

This has implications for everything from electronic payments and ecommerce to satellite communications. "Anything that's protected by something that's vulnerable becomes fair game for people that have access to quantum relevant computers," says Jon France, chief information security officer at non-profit cybersecurity organization ISC2.

Quantum computers capable of breaking asymmetric encryption are thought to be years away.

But progress is being made.

In December, Google said its new quantum chip incorporates key "breakthroughs" and "paves the way to a useful, large-scale quantum computer".

Some estimates say a quantum device capable of breaking current encryption would require 10,000 qubits, while others say millions would be needed. Today's systems have a few hundred at most.

But businesses and governments face a problem right now, as attackers could harvest encrypted information and decrypt it later when they do gain access to suitably powerful devices.

Greg Wetmore, vice president for software development at security firm Entrust, says if such devices could emerge in the next decade, technology leaders need to ask, "What data in your organization is valuable for that period of time?"

That could be national security information, personal data, strategic plans, and intellectual property and secrets - think of a soft drink company's "secret" formula or the precise balance of herbs and spices in a fast food recipe.

Mr France adds, if quantum computing becomes widespread, the threat becomes more immediate with the encryption that protects our daily banking transactions, for example, potentially trivial to break.

The good news is that researchers and the technology industry have been working on solutions to the problem. In August, the National Institute of Standards and Technology in the US released three post quantum encryption standards.

The agency said these would "secure a wide range of electronic information, from confidential email messages to e-commerce transactions that propel the modern economy." It is encouraging computer system administrators to transition to the new standards as soon as possible, and said a further 18 algorithms are being evaluated as backup standards.

The problem is this means a massive upgrade process touching virtually all our technology infrastructure.

"If you think about the number of things out there with asymmetric encryption in them, it's billions of things. We're facing a really big change problem," says Mr France.

Some digital infrastructure will be relatively easy to upgrade. Your browser, for example, will simply receive an update from the vendor, says Mr France. "The challenge really comes in discrete devices and the internet of things (IOT)," he continues.

These might be hard to track down, and geographically inaccessible. Some equipment – legacy devices in critical national infrastructure such as water systems, for example – might not be powerful enough to handle the new encryption standards.

Mr Wetmore says the industry has managed encryption transitions in the past, but "It's the sharper discontinuity that makes this threat more serious."

So, it is trying to help customers build "crypto agility" by setting out policies now and using automation to identify and manage their cryptographic assets. "That's the secret to making this transition an orderly one and not a chaotic one."

And the challenge extends into space. Prof Sastry says many satellites – such as the Starlink network – should be relatively straightforward to upgrade, even if it means briefly taking an individual device offline temporarily.

"At any given point in time, especially with the LEO (low earth orbit) satellites, you've got 10 to 20 satellites above your head," Prof Sastry says. "So, if one can't serve you, well so what? There are nine others that can serve you."

More challenging, he says, are "remote sensing" satellites, which include those used for geographical or intelligence purposes. These carry a lot more compute power on board and typically include some sort of secure computing module. A hardware upgrade effectively means replacing the whole device. However, says Prof Sastry, this is now less of a problem thanks to more frequent and lower cost satellite launches.

While the impact of the millennium bug might have been minimal in the first days of 2000, that's because an immense amount of work had gone into fixing it ahead of a known deadline, says François Dupressoir, associate professor in cryptography at the University of Bristol.

By contrast, he adds, that it is not possible to predict when current encryption will become vulnerable.

"With cryptography," says Mr Dupressoir "If somebody breaks your system, you will only know once they've got your data."

7. Microsoft unveils Majorana 1, the world's first quantum processor powered by topological qubits

by Chetan Nayak
https://azure.microsoft.com/en-us/blog/quantum/2025/02/19/microsoft-unveils-majorana-1-the-worlds-first-quantum-processor-powered-by-topological-qubits/

Quantum computers promise to transform science and society—but only after they achieve the scale that once seemed distant and elusive, and their reliability is ensured by quantum error correction. Today, we're announcing rapid advancements on the path to useful quantum computing:

- **Majorana 1:** the world's first Quantum Processing Unit (QPU) powered by a Topological Core, designed to scale to a million qubits on a single chip.

- **A hardware-protected topological qubit:** research published today in *Nature*, along with data shared at the Station Q meeting, demonstrate our ability to harness a new type of material and engineer a radically different type of qubit that is small, fast, and digitally controlled.
- **A device roadmap to reliable quantum computation:** our path from single-qubit devices to arrays that enable quantum error correction.
- **Building the world's first fault-tolerant prototype (FTP) based on topological qubits:** Microsoft is on track to build an FTP of a scalable quantum computer—in years, not decades—as part of the final phase of the Defense Advanced Research Projects Agency (DARPA) Underexplored Systems for Utility-Scale Quantum Computing (US2QC) program.

Together, these milestones mark a pivotal moment in quantum computing as we advance from scientific exploration to technological innovation.

Harnessing a new type of material

All of today's announcements build on our team's recent breakthrough: the world's first *topoconductor*. This revolutionary class of materials enables us to create *topological superconductivity,* a new state of matter that previously existed only in theory. The advance stems from Microsoft's innovations in the design and fabrication of gate-defined devices that combine indium arsenide (a semiconductor) and aluminum (a superconductor). When cooled to near absolute zero and tuned with magnetic fields, these devices form topological superconducting nanowires with Majorana Zero Modes (MZMs) at the wires' ends.

For nearly a century, these quasiparticles existed only in textbooks. Now, we can create and control them on demand in our topoconductors. MZMs are the building blocks of our qubits, storing quantum information through 'parity'—whether the wire contains an even or odd number of electrons. In conventional superconductors, electrons bind into Cooper pairs and move without resistance. Any unpaired electron can be detected because its presence requires extra energy. Our topoconductors are different: here, an unpaired electron is shared between a pair of MZMs, making it invisible to the environment. This unique property protects the quantum information.

While this makes our topoconductors ideal candidates for qubits, it also presents a challenge: How do we read quantum information that is so well hidden? How can we distinguish between, say, 1,000,000,000 and 1,000,000,001 electrons?

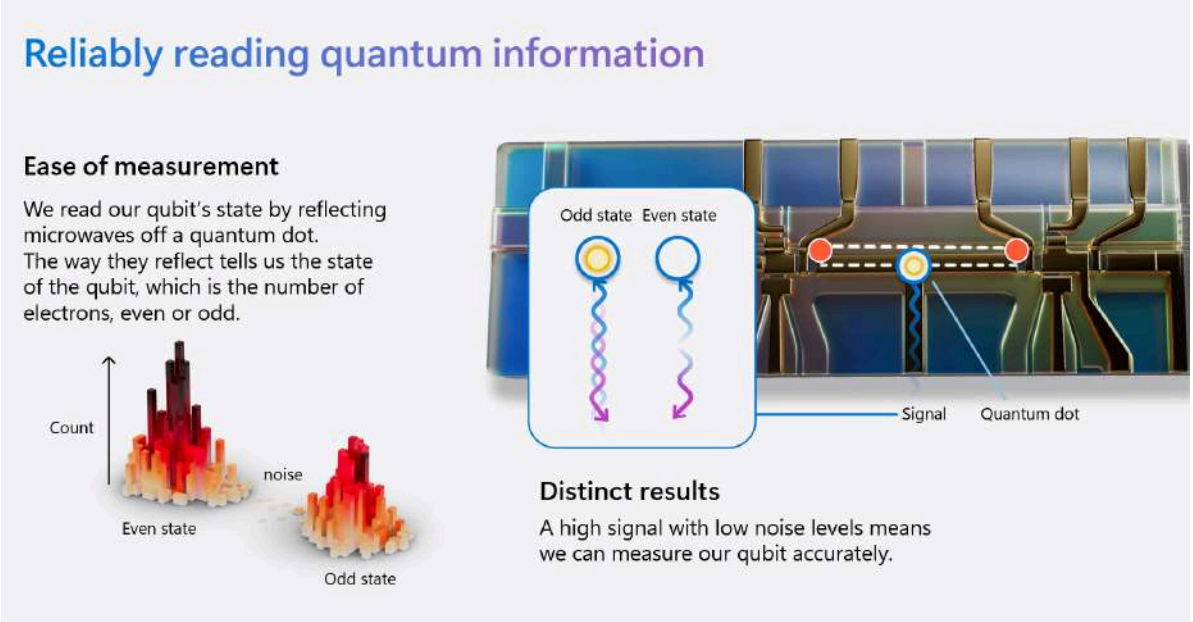


Figure 1: Reading the state of our topological qubit.

Our solution to this measurement challenge works as follows (also see Figure 1):

- We use digital switches to couple both ends of the nanowire to a quantum dot, which is a tiny semiconductor device that can store electrical charge.
- This connection increases the dot's ability to hold charge. Crucially, the exact increase depends on the parity of the nanowire.
- We measure this change using microwaves. The dot's ability to hold charge determines how the microwaves reflect off the quantum dot. As a result, they return carrying an imprint of the nanowire's quantum state.

We designed our devices so these changes are large enough to measure reliably in a single shot. Our initial measurements had an error probability of 1%, and we've identified clear paths to significantly reduce this.

Our system shows impressive stability. External energy—such as electromagnetic radiation—can break Cooper pairs, creating unpaired electrons that can flip the qubit's state from even to odd parity. However, our results show that this is rare, occurring only once per millisecond on average. This indicates that the shielding that envelops our processor is effective at keeping such radiation out. We are exploring ways to reduce this even further.

It's perhaps not surprising that quantum computation would require us to engineer a new state of matter specifically designed to enable it. What's remarkable is how accurate our readout technique already is, demonstrating that we are harnessing this exotic state of matter for quantum computation.

Revolutionizing quantum control through digital precision

This readout technique enables a fundamentally different approach to quantum computing in which measurements are used to perform calculations.

Traditional quantum computing rotates quantum states through precise angles, requiring complex analog control signals customized for each qubit. This complicates quantum error correction (QEC), which must rely on these same sensitive operations to detect and correct errors.

Our measurement-based approach simplifies QEC dramatically. We perform error correction entirely through measurements activated by simple digital pulses that connect and disconnect quantum dots from nanowires. This digital control makes it practical to manage the large numbers of qubits needed for real-world applications.

From physics to engineering

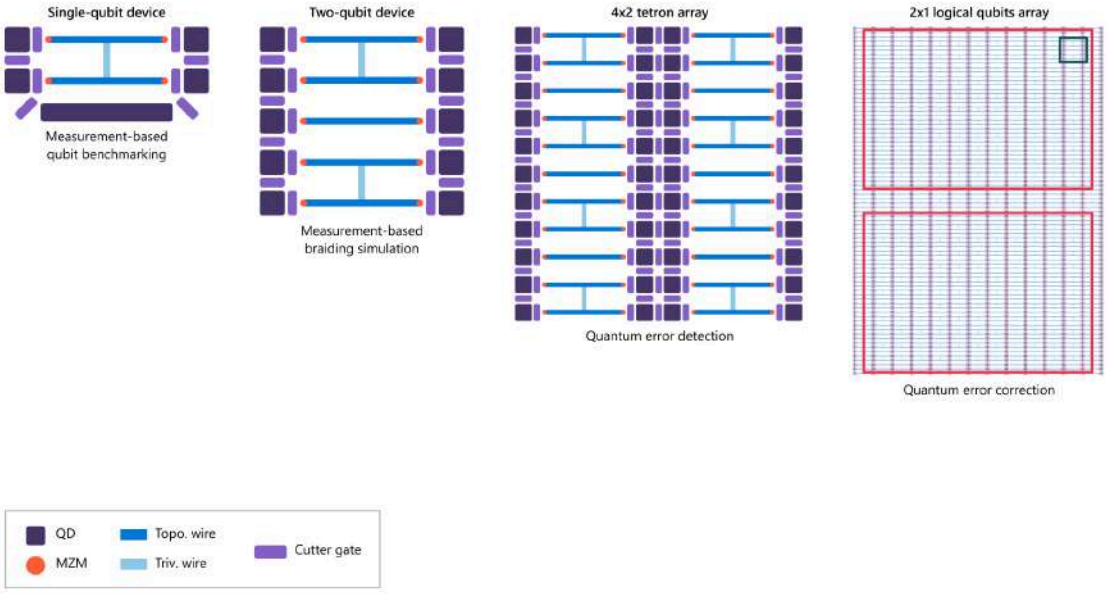


Figure 2: Roadmap to fault-tolerant quantum computation with tetrons. The first panel shows a single-qubit device. The tetron is formed through two parallel topological wires (blue) with an MZM at each end (orange dot) connected by a perpendicular trivial superconducting wire (light blue). The next panel shows a two-qubit device that supports measurement-based braiding transformations. The third panel shows a 4×2 array of tetrons supporting a quantum error detection demonstration on two logical qubits. These demonstrations build toward quantum error correction, such as on the device shown in the right panel (a 27×13 tetron array).

With the core building blocks now demonstrated—quantum information encoded in MZMs, protected by topology, and processed through measurements—we're ready to move from physics breakthrough to practical implementation.

The next step is a scalable architecture built around a single-qubit device called a tetron (see Figure 2). At the Station Q meeting, we shared data demonstrating the basic operation of this qubit. One fundamental operation—measuring the parity of one of the topological nanowires in a tetron—uses the same technique described in our *Nature* paper.

Another key operation puts the qubit in a superposition of parity states. This, too, is performed by a microwave reflectometry measurement of a quantum dot, but in a different measurement configuration in which we decouple the first quantum dot from the nanowire and connect a different dot to both nanowires at one end of the device. By performing these two orthogonal Pauli measurements, Z and X, we've demonstrated measurement-based control—a crucial milestone that unlocks the next steps on our roadmap.

Our roadmap now leads systematically toward scalable QEC. The next steps will involve a 4×2 tetron array. We will first use a two-qubit subset to demonstrate entanglement and measurement-based braiding transformations. Using the entire eight-qubit array, we will then implement quantum error detection on two logical qubits.

The built-in error protection of topological qubits simplifies QEC. Moreover, our custom QEC codes reduce overhead roughly tenfold compared to the previous state-of-the-art approach. This dramatic reduction means that our scalable system can be built from fewer physical qubits and has the potential to run at a faster clock speed.

DARPA's recognition of our approach

The Defense Advanced Research Projects Agency (DARPA) has selected Microsoft as one of two companies to advance to the final phase of their rigorous benchmarking program known as Underexplored Systems for Utility-Scale Quantum Computing (US2QC)—one of the programs that makes up DARPA's larger Quantum Benchmarking Initiative (QBI). Microsoft views this recognition as validation of our roadmap for building a fault-tolerant quantum computer with topological qubits.

DARPA's US2QC program and its broader Quantum Benchmarking Initiative represent a rigorous approach to evaluating quantum systems that could solve problems that are beyond the capabilities of classical computers. To date, the US2QC program has brought together experts from DARPA, Air Force Research Laboratory, Johns Hopkins University Applied Physics Laboratory, Los Alamos National Laboratory, Oak Ridge National Laboratory, and NASA Ames Research Center to verify quantum hardware, software, and applications. Going forward, the larger Quantum Benchmarking Initiative is expected to engage with even more experts in the testing and evaluation of quantum computers.

Previously, DARPA selected Microsoft for an earlier phase upon an assessment that we could plausibly build a utility-scale quantum computer in a reasonable timeframe. DARPA then evaluated the Microsoft quantum team's architectural designs and engineering plan for a fault-tolerant quantum computer. As a result of this careful analysis, DARPA and Microsoft have executed an agreement to begin the final phase of the

program. During this phase, Microsoft intends to build a fault-tolerant prototype based on topological qubits in years, not decades—a crucial acceleration step toward utility-scale quantum computing.

Unlocking quantum's promise

Eighteen months ago, we laid out our roadmap to a quantum supercomputer. Today we hit our second milestone, demonstrating the world's first topological qubit. And we've already placed eight topological qubits on a chip designed to house one million.

A million-qubit quantum computer isn't just a milestone—it's a gateway to solving some of the world's most difficult problems. Even today's most powerful supercomputers cannot accurately predict the quantum processes that determine the properties of the materials essential to our future. But quantum computing at this scale could lead to innovations like self-healing materials that repair cracks in bridges, sustainable agriculture, and safer chemical discovery. What today requires billions of dollars in exhaustive experimental searches and wet-lab experiments could be found, instead, through calculation on a quantum computer.

Our path to useful quantum computing is clear. The foundational technology is proven, and we believe our architecture is scalable. Our new agreement with DARPA shows a commitment to relentless progress toward our goal: building a machine that can drive scientific discovery and solve problems that matter. Stay tuned for more updates on our journey.

8. IDEMIA's Amaanie Hakim on Quantum-Safe Security and Future Challenges

by Kajal Mehra
https://timestech.in/idemias-amaanie-hakim-on-quantum-safe-security-and-future-challenges/

In an interview with TimesTech, Amaanie Hakim, VP Innovation at IDEMIA Secure Transactions, discusses the imminent threat of quantum computing to cryptography. She highlights IDEMIA's pioneering efforts in post-quantum security, including quantum-safe smart cards and SIMs, and the need for crypto-agility. Amaanie emphasizes global collaborations and India's role in advancing cryptographic research to secure financial transactions, IoT devices, and critical infrastructures.

TimesTech: Quantum computing is expected to disrupt traditional cryptographic security. How imminent is this threat, and what steps should organizations take now to prepare for the post-quantum era?

Amaanie: If we only look at what Quantum Computers can do today, we may think we still have time. But the truth is that even though Quantum Computers cannot break traditional cryptography yet, the threat is already here. The first and most urgent threat relates to the "harvest now, decrypt later" type of attacks.

Just imagine that an attacker steals a database containing medical records or personal data, encrypted with traditional cryptography. You may think it is safe, but actually your medical records do not expire, and are still of value 10 years from now. When the Quantum Computers are ready, the attackers can decrypt that data harvested today and exploit these medical records. In India alone, we had more than 6000 cyberattacks per week in the health sector in the first semester of 2024, which can give you an idea of the size of the threat.

There is another aspect which is very important for us at IDEMIA Secure Transactions: the security of chips in the field. Today when a car or a smart meter is equipped with a chip to secure its connectivity, that chip is likely to last for at least 10 years, and we cannot imagine recalling or replacing the billions connected devices when Quantum Computers are ready to break current cryptography. Knowing that most experts estimate that they will be ready in less than 10 years, we should already be deploying Quantum-ready chips.

TimesTech: IDEMIA Secure Transactions has proactively developed quantum-resistant solutions, such as the first quantum-safe smart card in 2019 and the quantum-safe 5G SIM in 2021. Can you share insights into the technology behind these innovations and their real-world impact?

Amaanie: Cryptography relies on using very complex maths problems which are very hard to solve. With Quantum Computing, some of our current complex maths problems will become easy to solve.

So what the Crypto researchers are doing is to imagine new complex maths problems that are not easy to solve even for Quantum Computers, that we call Post Quantum Cryptography or PQC. This is what we do when we participate in the NIST standardization efforts for example.

The thing is that our chips are designed to provide cryptographic functions and these maths computations in the most efficient manner, both in terms of processing memory required and in terms of performance. When moving to Post Quantum cryptography, as the underlying math problems are totally rethought, we also need to rethink our hardware, introducing accelerators designed for this new type of crypto, but also our software, to optimize computations. This was our first priority in 2019: implementing these new types of algorithms on our chips to ensure they could run in an acceptable time for end users.

But since then, we have been working on supporting customers and partners in preparing for post-quantum migration at the ecosystem level. We are for instance leading a consortium alongside other French cybersecurity leaders, focused on Post Quantum readiness of end-to-end use cases.

TimesTech: With decades of expertise in cryptography (AES, RSA, ECC) and embedded security software (EAL6), how is IDEMIA Secure Transactions leveraging its experience to future-proof financial transactions and secure communications?

Amaanie: Our cryptography experts actively work on adapting embedded security for the post quantum era, as demonstrated by their multiple research papers published over the past few years, for instance at the Cryptographic Hardware and Embedded Systems conference.

Beyond embedded security, we are putting our expertise and knowledge at the service of our customers and of the ecosystem to anticipate as much as possible, working on clients' end-to-end implementations.

In the payment ecosystem, we have built in 2022 a proposition to integrate post-quantum cryptography into card payment protocols. In 2024, we demonstrated the first post-quantum resistant offline transaction for CBDC.

Back to the connected devices I was mentioning earlier, we are also actively involved in the migration of these connected edge devices, implementing not only PQ-ready protocols but also embedding crypto-agility. Remember that we have years of hindsight on "traditional" cryptography, which is not the case on PQC. So we do know that the PQC algorithms being standardized will evolve, and we need to have a solution to update cryptography without shutting down systems or replacing the devices. This is what we call crypto-agility.

For our clients to be ready, we need to start working now on real-life implementations and use cases, and we already are!

TimesTech: Governments and enterprises are increasingly concerned about quantum threats. What collaborations or initiatives is IDEMIA Secure Transactions undertaking to help them implement quantum-safe security solutions?

Amaanie: First, we participate in global research and standardization efforts. Beyond the NIST I already mentioned earlier, we contribute for example to GSMA, ETSI, GlobalPlatform and FIDO Alliance working groups, as well as several standardization bodies and organizations in the telecoms and IoT fields in India.

Second, we work hand in hand with our customers and with partners to test the solutions we propose on end-to-end use cases.

For instance, in 2024, we have announced with Telefonica and Quside the launch of our Quantum-Safe Connectivity for IoT devices project.

We have also launched a strategic research partnership with Indian Institute of Technology, Hyderabad (IIT Hyderabad) on Post Quantum Cryptography, sponsoring PHD scholars. We actively contribute to standardization bodies and organizations in India, including TSDSI, TEC, and CDOT, showcasing our commitment to advancing cryptographic research in the region.

TimesTech: What new quantum-safe technologies is IDEMIA Secure Transactions working on, and how do you see the cybersecurity landscape evolving over the next decade?

Amaanie: I have been working in this industry for more than 20 years, and what I can testify is that cybersecurity needs are constantly accelerating, with attackers that are more and more organized.

This migration is going to take years, with "traditional" and post-quantum cryptography co-existing and even combined with what we call hybrid cryptography.

Our duty as a leader in cybersecurity and cryptography technologies is to stay at the forefront of anticipation and innovation in this field, to ensure we build the foundation of crypto-agile systems that we can adapt constantly to security threats arising as mentioned earlier.

9. FAQ on Microsoft's topological qubit thing

by Scott Aaronson
https://scottaaronson.blog/?p=8669

Did you see Microsoft's announcement?

Yes, thanks, you can stop emailing to ask! Microsoft's Chetan Nayak was even kind enough to give me a personal briefing a few weeks ago. Yesterday I did a brief interview on this for the BBC's World Business Report, and I also commented for the MIT Technology Review.

What is a topological qubit?

It's a special kind of qubit built using nonabelian anyons, which are excitations that can exist in a two-dimensional medium, behaving neither as fermions nor as bosons. The idea grew out of seminal work by Alexei Kitaev, Michael Freedman, and others starting in the late 1990s. Topological qubits have proved harder to create and control than ordinary qubits.

Then why do people care about topological qubits?

The dream is that they could *eventually* be more resilient to decoherence than regular qubits, since an error, in order to matter, needs to change the *topology* of how the nonabelian anyons are braided around each other. So you'd have some robustness built into the physics of your system, rather than having to engineer it laboriously at the software level (via quantum fault-tolerance).

Did Microsoft create the first topological qubit?

Well, they say they did! [**Update:** Commenters point out to me that buried in *Nature*'s review materials is the following striking passage: "The editorial team wishes to point out that the results in this manuscript do not represent evidence for the presence of Majorana zero modes in the reported devices. The work is published for introducing a device architecture that might enable fusion experiments using future Majorana zero modes." So, the situation is that Microsoft is unambiguously claiming to have created a topological qubit, *and* they just published a relevant paper in *Nature*, but their claim to have created a topological qubit has not yet been accepted by peer review.]

Didn't Microsoft claim the experimental creation of Majorana zero modes—a building block of topological qubits—back in 2018, and didn't they then need to retract their claim?

Yep. Certainly that history is making some experts cautious about the new claim. When I asked Chetan Nayak how confident I should be, his response was basically "look, we now have a topological qubit that's behaving fully as a qubit; how much more do people want?"

Is this a big deal?

If the claim stands, I'd say it would be a scientific milestone for the field of topological quantum computing and physics beyond. The number of topological qubits manipulated in a single experiment would then have finally increased from 0 to 1, and depending on how you define things, arguably a "new state of matter" would even have been created, one that doesn't appear in nature (but only in *Nature*).

Is this useful?

Not yet! If anyone claims that a single qubit, or even 30 qubits, are already *useful* for speeding up computation, you can ignore anything else that person says. (Certainly Microsoft makes no such claim.) On the question of what we believe quantum computers will or won't *eventually* be useful for, see like half the archives of this blog over the past twenty years.

Does this announcement vindicate topological qubits as the way forward for quantum computing?

Think of it this way. *If* Microsoft's claim stands, then topological qubits have finally reached some sort of parity with where more traditional qubits were 20-30 years ago. I.e., the non-topological approaches like superconducting, trapped-ion, and neutral-atom have an absolutely *massive* head start: there, Google, IBM, Quantinuum, QuEra, and other companies now routinely do experiments with dozens or even hundreds of entangled qubits, and thousands of two-qubit gates. Topological qubits can win if, and only if, they turn out to be *so much* more reliable that they leapfrog the earlier approaches—sort of like the transistor did to the vacuum tube and electromechanical relay. Whether that will happen is still an open question, to put it extremely mildly.

Are there other major commercial efforts to build topological qubits?

No, it's pretty much just Microsoft [**update:** apparently Nokia Bell Labs also has a smaller, quieter effort, and Delft University in the Netherlands also continues work in the area, having ended an earlier collaboration with Microsoft]. Purely as a scientist who likes to see things tried, I'm grateful that at least one player stuck with the topological approach even when it ended up being a long, painful slog.

Is Microsoft now on track to scale to a million topological qubits in the next few years?

In the world of corporate PR and pop-science headlines, sure, why not? As Bender from *Futurama* says, "I can guarantee anything you want!" In the world of reality, a "few years" certainly feels overly aggressive to me, but good luck to Microsoft and good luck to its competitors! I foresee exciting times ahead, provided we still have a functioning civilization in which to enjoy them.

10. American Binary Launches First Fully CNSA 2.0 Quantum-Resistant VPN, Protecting Against "Harvest Now, Decrypt Later" Attacks

by Kevin Kane
https://www.prnewswire.com/news-releases/american-binary-launches-first-fully-cnsa-2-0-quantum-resistant-vpn-protecting-against-harvest-now-decrypt-later-attacks-302378506.html

American Binary today (18 Feb 2025) announced a breakthrough in cybersecurity with the launch of Ambit Client, the first and only enterprise VPN solution to achieve full compliance with the NSA's CNSA 2.0 standard for quantum resistance. This milestone arrives as organizations face an immediate threat from "Harvest Now, Decrypt Later" (HNDL) attacks, where cybercriminals are already collecting encrypted data to decrypt it once quantum computers become available.

"The quantum threat isn't a future problem—it's happening now," said Kevin Kane, CEO and Founder at American Binary. "While other VPN providers claim quantum resistance, Ambit Client is the only solution that delivers complete protection across all four critical cryptographic components required by CNSA 2.0."

The Quantum Security Gap

Current VPN solutions leave organizations vulnerable by implementing quantum-resistant algorithms in only some of their cryptographic components. For true quantum resistance, all four key components must meet CNSA 2.0 standards:

- Digital Signature
- Key Exchange
- Bulk Encryption (AEAD)
- Hashing

Ambit Client stands alone in achieving CNSA 2.0 compliance across all four components, including the implementation of ML-KEM 1024 cryptography—mathematically proven to resist both conventional and quantum computer attacks.

Organizations using traditional VPNs that rely on Diffie-Hellman Key Exchange, hybrid cryptography, or elliptic-curve cryptography remain exposed to HNDL attacks. These vulnerabilities could allow adversaries to decrypt sensitive data once quantum computers become capable enough—a milestone expected as early as 2030.

"As I revealed in my Bloomberg documentary, The Massive Cyberattack You Never Heard About, the greatest cyber threats aren't just coming—they're already here. Quantum computing will soon shatter traditional encryption, leaving our most sensitive data exposed. That's why investing in post-quantum solutions isn't optional; it's urgent. American Binary's post-quantum VPN embodies the resilience, security, and innovation that define American Binary values—ensuring that our critical infrastructure remains protected against the next frontier of cyber warfare. The future belongs to those who secure it now." — Jose Arrieta, former CIO of U.S. Department of Health & Human Services (HHS) and CEO of Imagineer LLC.

11. China Launches Its Own Quantum-Resistant Encryption Standards, Bypassing US Efforts

by Matt Swayne
https://thequantuminsider.com/2025/02/18/china-launches-its-own-quantum-resistant-encryption-standard-bypassing-us-efforts/

China has announced a global call for new cryptographic algorithms to counter the security threats posed by quantum computing, signaling a move away from US-led efforts in the field.

The Institute of Commercial Cryptography Standards (ICCS), which operates under the Chinese Cryptography Standardization Technical Committee, is soliciting proposals for post-quantum cryptographic (PQC) algorithms. The initiative aims to establish national standards for encryption that can withstand quantum attacks, covering public-key cryptography, cryptographic hash functions and block ciphers. According to ICCS, the effort encourages international participation, with algorithms being evaluated for security, performance, and implementation feasibility.

That, in itself, might not be seen as an unusual initiative, but experts see China's decision to pursue an independent cryptographic standard as a strategic move. As reported by New Scientist, China may be avoiding US-led encryption initiatives due to concerns over potential "back doors" that could allow US intelligence agencies to access encrypted communications. There is also speculation that China may seek to integrate its own covert access points into its encryption protocols.

The urgency of developing quantum-resistant encryption stems from the growing capabilities of quantum computers. These machines, which leverage quantum mechanics to perform certain calculations exponentially faster than classical computers, pose a direct threat to current encryption methods.

TO ADOPT NIST STANDARDS, OR NOT

The National Institute of Standards and Technology (NIST) has been leading efforts to develop encryption standards resistant to quantum attacks since 2012. The agency launched a multi-phase initiative to evaluate and standardize post-quantum cryptographic (PQC) algorithms, aiming to replace public-key encryption methods vulnerable to quantum decryption.

In 2022, NIST selected four candidate algorithms—CRYSTALS-Kyber for public-key encryption and CRYSTALS-Dilithium, FALCON, and SPHINCS+ for digital signatures—marking a major step toward formalizing new global encryption standards. The selection process, which involves collaboration with academic and industry cryptographers, is ongoing, with additional algorithms under review for broader cryptographic functions. While NIST's standards primarily serve US organizations, they are widely adopted worldwide, influencing cybersecurity policies across industries.

Dustin Moody, a mathematician at NIST, told New Scientist that China has previously selected PQC algorithms similar to those chosen by NIST, but its approach to standardization is more opaque.

"In the larger picture, it's not surprising to us that they are doing their own standards," Moody told New Scientist. "Historically, China hasn't trusted the cryptography standards the US puts out and have developed their own. I think this is also true with regards to Russia."

While NIST's standards are primarily intended for US organizations, they are widely adopted internationally. Moody said NIST will monitor China's efforts and would not rule out incorporating strong Chinese-developed algorithms into its own framework.

"If it offers enough of an improvement, we could potentially do something about it," Moody said.

ICCS's initiative invites researchers worldwide to submit candidate algorithms, and the institute has released draft guidelines for cryptographic hash function proposals, with public comments open until March 15, 2025. This aligns with China's broader strategy of exerting more control over its technology infrastructure.

12. The International Year Of Quantum: Igniting Possibility, Accelerating The Future

by Cierra Choucair

https://thequantuminsider.com/2025/02/14/the-international-year-of-quantum-igniting-possibility-accelerating-the-future/?utm_source=resonance-newsletters.beehiiv.com&utm_medium=newsletter&utm_campaign=the-quantum-insider-weekly-quera-s-230-million-round-quantum-supercomputer-connection&_bhlid=06a653fea70b552298329c4da6506b02e7a71f9d

Quantum has always been a force of contradiction—both foundational and elusive, shaping the modern world while remaining an enigma to most. It exists in the devices we use, the systems we rely on, yet it is spoken of in paradoxes, understood by few.

The opening ceremony of the International Year of Quantum was an acknowledgment of this duality—not just a reflection on a century of discovery, but a call to shape what comes next. It was a gathering of scientists, policymakers, and industry leaders, aligned not only in their ambition but in their responsibility to make quantum's future more tangible, more accessible, and more inclusive.

UNESCO, the American Physical Society, and organizations like The Quantum Insider are championing this year-long initiative to bring quantum into public consciousness—not as a distant theoretical field, but as a potential tool to impact society at every level. The mission is not just to celebrate progress but to ensure that the next era of quantum is one that belongs to all.

A Convergence of Purpose

The ceremony was not just a stage for reflection—it was a stage for alignment. On stage, we confirmed as a community that we are on the right page, with common themes of accessibility, education, responsible development, and tools to work towards the Sustainable Development Goals. Off stage, conversations deepened, partnerships formed, and the work of the future was not just imagined but actively set in motion.

Building something new requires an ability to see beyond what exists and take the next best step forward. The International Year of Quantum is not just about celebrating achievements; it is about pushing past barriers—technical, conceptual, institutional—to ensure that quantum's promise is realized for all.

Celia Merzbacher, Executive Director of QED-C, captured this vision: "The International Year of Quantum, I believe, is an opportunity—because it's broad, it's inclusive, and it's raising awareness. While QED-C is very much focused on advancing the commercial industry, that industry depends on the entire innovation ecosystem—from research to product development. I always say: quantum is global. Innovation is global. Talent is globally distributed, and the markets are global. The International Year of Quantum is about bringing together as many stakeholders as possible."

And true inclusion is an active process—one that goes beyond awareness and requires sustained engagement across disciplines, industries, and communities. As the conversation deepened, a common thread emerged: progress in quantum will come not just from visionaries but from those who refine, challenge, and evolve ideas in real time. Allison Schwartz, Vice President of Global Government Relations & Public Affairs at D-Wave, reinforced this reality: "Being at the center of this industry—building applications today and providing real-time cloud access across 42 countries—gives us a unique opportunity to tap into new generations of innovators. We're especially focused on those who aren't just thinking theoretically but are asking, 'What can I do today?'"

Quantum is not a solitary endeavor. It thrives on collaboration, on the merging of disciplines, on ideas that challenge conventional wisdom. Krysta Svore, Technical Fellow and Vice President of Advanced Quantum

Development for Microsoft, emphasized this dynamic: "In computing, you always compare—you run it, measure against a baseline, and if it's better, you use it. But in quantum computing, we haven't been able to do that. The power today is that we are producing reliable quantum machines that can be integrated and layered onto existing workflows."

The future of quantum cannot be built in isolation. It is not a closed-loop system, self-contained and exclusive to a handful of experts. It must be expansive, integrative, and, above all, inclusive.

The Question of Understanding

Education stood as one of the ceremony's most urgent themes. Digital literacy is foundational in today's world, yet classical computer science remains absent from many K-12 curriculums. Mathematics and physics—essential to quantum computing—are often overlooked. If we do not prioritize these subjects early, we risk creating a future where only a select few have the knowledge and opportunity to engage with this technology in meaningful ways.

But waiting for the next generation to come of age is not an option. The urgency of quantum's development requires a workforce that draws from all disciplines and industries. We need physicists, yes—but also electrical engineers, software developers, policymakers, and advocates. The success of quantum technology will not rest on scientists alone; it will require the efforts of an entire ecosystem.

Rajeeb Hazra, CEO of Quantinuum, put it bluntly: "A big part of the access challenge is workforce. For quantum to realize its full potential, it must evolve from a small set of people who have to labor inordinately hard against the systems of the world to do it right."

Mitra Azizirad, President & COO of Strategic Missions & Technologies at Microsoft, expanded on this idea: "The first step for us—and what I'm most focused on—is identifying those initial hybrid applications. How do we work with our partners and customers to determine what they will be? Because when you think about the marriage of AI and quantum, there's an incredible opportunity ahead."

Jonathan Felbinger, Deputy Director of the QED-C, drew a parallel to AI: "I think this is a great opportunity to capture the public imagination—much like AI has. Every day, there's something in the news about AI, and I'm sure kids today are thinking, 'I want to work in AI. I want to learn AI.' In a way, they've become AI-native, interacting with it, shaping it, and building awareness around it. I want that same level of public engagement for quantum—both in terms of understanding use cases and building the future workforce."

Ethics, Sustainability, and the Responsibility of Knowledge

Science does not exist in a vacuum, nor should it. The pursuit of knowledge is deeply human, driven by curiosity, by wonder, by the desire to push beyond the known. But awe alone is not enough. If we possess a technology, even in its early stages, that has the potential to address the world's most profound challenges,

then the responsibility to pursue it extends beyond personal ambition—it becomes an obligation to humanity.

Professor Yasser Omar, President of the Portuguese Quantum Institute, reminded attendees in his opening remarks on the second day of the event that "Basic science is a societal benefit." But its impact depends on how we choose to apply it. The responsibility of scientific discovery does not lie solely with researchers in the lab—it extends to educators, policymakers, businesses, and individuals who seek to integrate and apply these discoveries for the benefit of society.

Hazra emphasized this dual responsibility: "Our job is to accelerate useful quantum computing for good—and each word in that is meaningful. Our role is to ensure we are accelerating both the rate of technology creation and its adoption. It does no good to develop technology and leave it in the lab. And it does no good to stop innovating just because democratizing that technology beyond the lab is getting harder."

As with any powerful technology, ethical considerations and security risks must also be addressed. Merzbacher urged a balanced approach: "In the context of the International Year of Quantum, I think we should focus on the beneficial applications—whether it's point-of-care diagnostics, improving weather forecasting to help farmers, or other positive impacts. As we develop these beneficial uses, national security controls will need to be targeted. Protections will still be necessary, but they should be narrowly focused to ensure that quantum's positive applications can be widely shared and used."

The Work That Lies Ahead

One of the most striking takeaways was the acknowledgment that progress is not always comfortable and quantum cannot afford to be an exclusive field. The future belongs to those willing to integrate it across industries, disciplines, and communities. The ceremony was a beginning, not an endpoint.

As Hazra observed, "The last three or four years—and even the last decade, before Quantinuum was formed—have been years of discovery. We've learned what works, and we've learned what doesn't. Now, 2025 is the year of acceleration. I'm not saying we've solved all the problems, but we have a path—we have a map. And now, we're moving faster along that map. The International Year of Quantum marks the year of accelerating useful quantum computing for good."

The urgency is not just in the technology itself but in the decisions we make around it. The International Year of Quantum is not just a celebration; it is a challenge. A call to ensure that the foundations we build now will last. Science, after all, is not just about what we can do—it is about what we should do.

Azizirad, with passion and intention, captured the essence of this moment: "But right now—this moment—is the most exciting. Because we're on the cusp of something where everything feels possible. We're in the 'art of the possible' phase, where we're truly ideating and layering quantum into what comes next."

13. The UK's war on encryption affects all of us

by Gaby Del Valle
https://www.theverge.com/policy/612136/uk-icloud-investigatory-powers-act-war-on-encryption

The encryption wars have reached a fever pitch, and the most contentious battle is not happening in the United States, where much of the action has been in the past — like the government's efforts to restrict exports of encryption software until the 1990s and the FBI's standoff with Apple in 2016. It's in the United Kingdom, where the government has reportedly ordered Apple to give officials blanket access to iCloud users' encrypted backups. And the order allegedly didn't just apply to UK users — it demanded backdoor access for users *worldwide*.

The secret order, first reported by *The Washington Post*, was issued in January under the auspices of the UK's Investigatory Powers Act of 2016. Apple's compliance or refusal will have ramifications far beyond the UK, potentially making users less safe and signaling to other governments that they, too, can seek backdoor access — a way of bypassing encryption — to users' information via legislation.

"Simply put, the message the UK government is sending is that its own citizens cannot expect its government to respect their privacy, and that it is willing to put their security at risk from all manner of bad actors like hackers and thieves because it cannot tolerate the ability to have a private conversation online," Andrew Crocker, surveillance litigation director at the Electronic Frontier Foundation, told *The Verge*.

Apple can appeal the ruling to a secret panel, but per the *Post*'s reporting, it can't delay complying with the order during an appeal. And the UK's Home Office would prohibit Apple from telling users that the government can now access their encrypted backups. This obviously creates a huge problem for Apple, which has built its reputation on safeguarding user privacy.

"Apple should be transparent with its users about how it's responding to this threat to their privacy and security," Greg Nojeim, the director of the Center for Democracy and Technology's Security and Surveillance Project, told *The Verge*. "It remains to be seen whether this move to weaken global cybersecurity around the world will hold, or whether the UK will back off."

Apple did not respond to *The Verge*'s request for comment.

For now, bystanders are left guessing. "If Apple does not appeal — if we don't see or hear about an appeal — does that mean they have complied?" Joe Jones, the director of research and insights at the International Association of Privacy Professionals, told *The Verge*. "If they complied, that creates a precedent not just for the UK, but for many other law enforcement authorities around the world."

It's Apple's policy to respond to law enforcement requests for data. Until 2022, iMessage might have been end-to-end encrypted, but iCloud backups were not, so a warrant would typically result in the police getting access to your phone. But that year, Apple implemented end-to-end encryption for iCloud backups under a

feature it called "Advanced Data Protection." Though users have to opt in to Advanced Data Protection, this feature rendered Apple's compliance with governments much less useful for law enforcement than before.

Security experts say, however, that the company's resistance to backdooring has less to do with taking a stand against governments and more to do with baseline cybersecurity.

Governments are locked out of encrypted iCloud backups "because everybody is locked out of it, so that hackers can't get in," Ciaran Martin, the former head of cybersecurity at the UK's Government Communications Headquarters — their equivalent to the NSA — said in a recent interview with the BBC. The issue with backdoors, Martin continued, is that there's no way to build one that lets law enforcement in and keeps everyone else out. "If you build a door, other people will try to get in," he said.

But according to Martin, the fact that the order is no longer secret could prevent it from being effective. "For the order to work, it has to not be known about by the criminals and the offenders," he said.

Previous matchups between tech companies and governments over backdooring have had decidedly mixed results. In 2016, Apple and the FBI were involved in a bitter legal battle over the tech company's refusal to unlock the iPhone of one of the San Bernardino shooters, which Tim Cook described as a fight to "help you protect your data and your privacy." The feds needed the password because, a few days after the shooting, someone with access to the phone triggered a password reset of the shooter's iCloud account, effectively locking law enforcement out.

Microsoft's refusal to give federal law enforcement access to emails stored at a data center in Dublin, Ireland, almost led to a US Supreme Court case — which was dropped after Microsoft and other tech giants, including Apple, Amazon, and Google, threw their support behind the CLOUD Act.

Given Apple's public comments, the company is unlikely to comply with the UK order. "There is no reason why the UK [government] should have the authority to decide for citizens of the world whether they can avail themselves of the proven security benefits that flow from end-to-end encryption," Apple told Parliament in March.
Rather than comply, people familiar with the matter told the *Post*, Apple may stop offering encrypted storage to UK-based users — but that still wouldn't address the Home Office's demand that Apple let its officials access the encrypted backups of users around the world.

"The challenge for that approach is that the UK's Investigatory Powers Act is extraterritorial," Jones said, which could lead to a "lengthy, protracted legal process. And these lengthy and protracted legal processes often spill out into diplomatic and political issues as well."

14. World's 1st hybrid quantum supercomputer goes online in Japan

by Keumars Afifi-Sabet
https://www.livescience.com/technology/computing/worlds-1st-hybrid-quantum-supercomputer-goes-online-in-japan?utm_source=substack&utm_medium=email

Engineers in Japan have switched on the world's first hybrid quantum supercomputer.

The 20-qubit quantum computer, called **Reimei**, has been integrated into Fugaku — the world's sixth-fastest supercomputer. The hybrid platform will work to tackle calculations that can take classical supercomputers much longer to process.

The machine, which is housed at the Riken scientific institute in Saitama, near Tokyo, will be used primarily for physics and chemistry research, representatives from Quantinuum, the makers of Reimei, and Riken said in a joint statement

Quantum computers could one day overtake classical computers, with the potential to complete calculations in minutes or seconds that would otherwise take today's most powerful machines millions of years. However, until quantum computers are large and reliable enough, scientists say that integrating their capabilities into supercomputers can be a stopgap.

Unlike most quantum computers that use superconducting qubits, Reimei uses trapped-ion qubits. This involves isolating charged atoms, or ions, in an electromagnetic field — known as an ion trap — and using lasers to precisely control their quantum state.

This enables the scientists to manipulate the ions so they can be used as qubits that store and process quantum information. Trapped ion qubits encourage more connections between qubits and longer coherence times, whereas superconducting qubits have faster gate connections and are easier to fabricate on chips.

Riken representatives said they chose Quintinuum's quantum computer for the integration because it has a unique architecture that physically moves qubits.This process of "ion shuttling" allows qubits to be moved around a circuit as required, allowing for more complex algorithms.

Error-correcting system

Qubits are inherently "noisy," so to effectively scale up quantum computers, scientists are developing error-correction techniques to increase the fidelity of qubits.

In Reimei, the physical ion qubits have been grouped to create "logical qubits" — meaning a set of physical qubits that store the same information in several places. Logical qubits are a key route to achieving a desired reduction in qubit errors, because distributing the information in different places spreads out the points of failure, meaning a qubit failure does not disrupt an ongoing calculation.

Quaintinuum previously achieved a breakthrough in creating a logical qubit with an error rate 800 times lower than physical qubits, which it integrated into its quantum computing processors.

While Reimei-Fugaku is the first fully operational, integrated hybrid system, other companies have previously tested such systems. In June 2024, IQM integrated a 20-qubit quantum processor into the SuperMUC-NG supercomputer in Garching, Germany.

That system, however, is still in the testing phase, with no confirmed public date when it becomes fully operational. In October, IQM representatives announced the company would integrate a 54-qubit system into the supercomputer in the latter half of 2025 followed by a 150-qubit chip in 2026.

15. The US government pushes for PQC adoption and extensive use of cryptography

by Jaime Gómez García
https://www.linkedin.com/posts/jaime-gomez-garcia_pqc-cryptography-cybersecurity-activity-7293276862250729472-GNq6/?utm_source=share&utm_medium=member_ios&rcm=ACoAAAOkuF0BDyzIhAX77o1KAPeEAsOkGdeoUxg

On Jan. 16th, 2025, the Biden administration published the "Executive Order on Strengthening and Promoting Innovation in the Nation's Cybersecurity" (EO 14144). The Trump administration revoked several Biden Executive Orders on the inauguration day, but this EO was not one of them.

This EO shows near-future requirements by US agencies to their vendors. These requirements may permeate to the financial sector as requisites from US agencies to their providers or as features that will be more relevant in major technology products and offerings. It also shows interesting trends on actions that may need to be prioritized.

The EO focuses on making cybersecurity controls effective to avoid organizations and the supply chain to comply minimally with no impact in improving security. It seeks accountability of software and cloud services providers.

Highlights on cryptography

There are several requirements promoting the use of cryptography and accelerating the transition to PQC:

- Use of public-key cryptography to implement phising-resistant authentication.
- Implement Internet routing protections to defend against malicious traffic diversions.
- Implement cryptography-protected DNS, email, voice, videoconference and instant messaging.
- Implement PQC "as soon as practicable".
- Improve key management onprem and in the cloud.

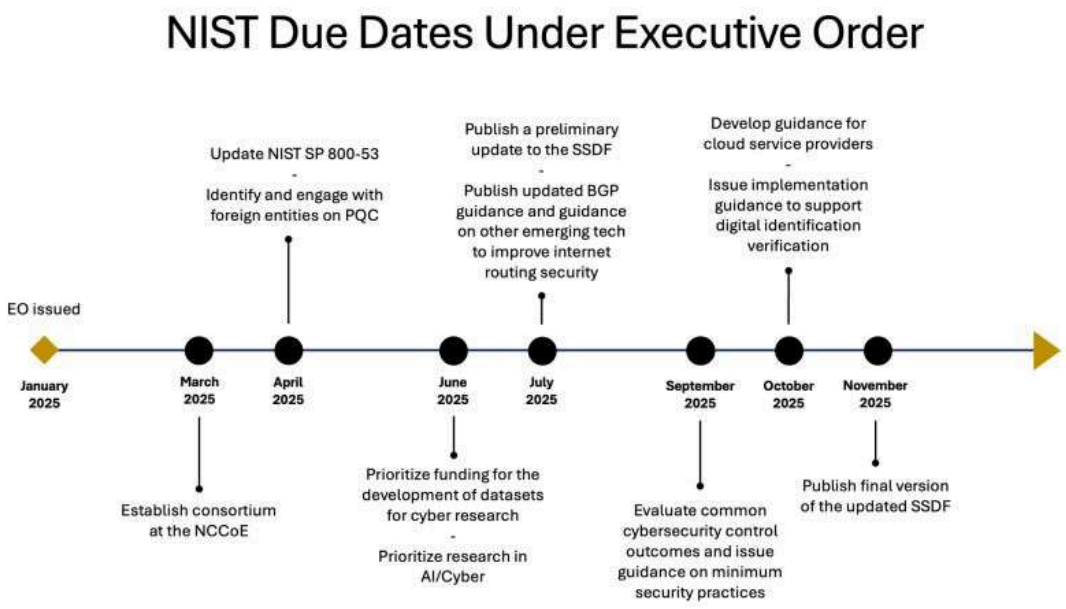
I appreciate the expanded focus on means to achieve data protection:

- Introducing or improving cryptography in various processes and protocols.
- Protecting Internet traffic routing, as it is a first step for HNDL attacks.

More details:

- The order highlights "the People's Republic of China presenting the most active and persistent cyber threat" to the US.
- Use of Route Origin Authorizations and performing Route Origin Validation filtering.
- NIST to publish updated guidance on BGP security methods, route leak mitigation and source address validation.
- Encrypted DNS must be deployed wherever supported.
- Email messages must be encrypted in transport and, where practical, use end-to-end encryption.
- Expand the use of authenticated transport-layer encryption between email servers and with clients.
- Voice, VCand IM must enable transport encryption and use end-to-end encryption by default.
- Implement PQC key establishment or hybrid key establishment including a PQC algorithm as soon as practicable upon support from the vendors.
- Support TLSv1.3 ASAP but no later than 2029.
- Cryptographic keys with extended lifecycles should be protected with HSMs, TEEs, etc.

Executive order: https://lnkd.in/d-ifZtrf National Institute of Standards and Technology (NIST) responsibilities: https://lnkd.in/dnhUbrfH



16. Revolutionize Your Digital Safety: Discover Quantum RootCA's Defense Against Quantum Threats

by Kenan Voss
https://www.yanoticias.es/news-en/revolutionize-your-digital-safety-discover-quantum-rootcas-defense-against-quantum-threats/79389/

In a bold leap toward unparalleled digital protection, SEALSQ teams up with the OISTE.ORG Foundation to launch the innovative Quantum RootCA by early 2025. This pioneering initiative is a frontline defense against the daunting threats posed by the rise of quantum computing. By employing state-of-the-art Post-Quantum Cryptography algorithms such as CRYSTALS-Dilithium and FALCON, Quantum RootCA ensures your data and digital identity are robustly shielded.

As we approach a world where quantum technology can potentially unravel traditional encryption, Quantum RootCA emerges as a crucial safeguard. Key sectors, especially IoT security, healthcare, telecommunications, and financial services, stand to gain significantly, securing their communications and critical data against unprecedented quantum attacks.

Central to this venture is the creation of the Quantum Lab, where businesses and innovators are invited to engage directly with the quantum-safe PQC-PKI platform. This space offers the unique opportunity to partake in pilot projects, giving companies the chance to experience firsthand the power and necessity of quantum-resistant security frameworks.

The integration with tools like Hardware Security Modules (HSMs) and Trusted Platform Modules (TPMs) bolsters resilience in key generation and authentication, ensuring that organizations can seamlessly upgrade their security infrastructure to meet the challenges of a quantum-powered future.

As the quantum era dawns, the Quantum RootCA initiative marks a decisive step forward, bringing cutting-edge security solutions to the forefront. It invites you to embrace a future where your digital world is fortified and trusted, ready to withstand the tests of time and technology. With Quantum RootCA, secure your digital frontier and become part of the next great leap in cybersecurity evolution!

Is Your Data Ready for Quantum Threats? Discover How SEALSQ Brings Quantum-Resistant Security

Pros and Cons of Quantum RootCA

Pros:

1. **Enhanced Security:** Quantum RootCA offers advanced protection against the formidable threats posed by quantum computing, securing sensitive data across numerous sectors.

2. **Cutting-edge Technology:** Implements state-of-the-art Post-Quantum Cryptography (PQC) algorithms such as CRYSTALS-Dilithium and FALCON.

3. **Broad Industry Impact:** Provides security solutions for critical sectors like IoT, healthcare, telecommunications, and financial services.

Cons:

1. **Implementation Complexity:** Transitioning to quantum-resistant infrastructures may be complex and resource-intensive for some organizations.

2. **Initial Investment:** Initial costs associated with deploying quantum-resistant technologies and settings may be high.

3. **Adaptation Requirement:** Requires significant organizational change management and training.

What Are the Key Features and Innovations of Quantum RootCA?

Key features of Quantum RootCA include advanced PQC-PKI platforms and a collaborative Quantum Lab for pilot testing. Innovations such as the integration with Hardware Security Modules (HSMs) and Trusted

Platform Modules (TPMs) enhance the robustness of encryption key generation and authentication processes, equipping organizations with future-ready cybersecurity frameworks.

How Will Quantum RootCA Impact Security Across Industries?

Quantum RootCA is predicted to lead the charge in enhancing digital defenses against quantum threats, especially in sectors that handle sensitive data. By providing businesses, particularly in IoT, healthcare, telecommunications, and financial services, with robust quantum-resistant encryption, Quantum RootCA ensures that these industries can continue operating securely amidst the evolving technological landscape.

How Can Organizations Integrate Quantum RootCA into Their Security Infrastructure?

To integrate Quantum RootCA, organizations should initiate collaborations with SEALSQ via the Quantum Lab, which facilitates pilot projects to experience the technology firsthand. Leveraging built-in tools like HSMs and TPMs will aid in a seamless transition to quantum-safe security ecosystems. Training and involving key personnel in the transition phase ensures strategic integration tailored to individual organizational needs.

17. Is Quantum Computing a Threat? Experts Warn Urgent Action Needed

by Ben Kline
https://www.yanoticias.es/news-en/is-quantum-computing-a-threat-experts-warn-urgent-action-needed/79352/

In a gripping new report, MITRE unveils the long timeline before quantum computers could threaten high-security encryption, projecting a clear window until around 2055 to 2060 before these machines could crack RSA-2048 encryption, the safeguard for classified data. But don't be fooled; the clock is ticking, and the race is already on.

As quantum technology advances, especially in nations like China, the urgency for proactive measures in the U.S. could not be greater. While researchers anticipate that current quantum technology won't be able to handle sensitive decryption for decades, adversaries are laying the groundwork, enhancing their capabilities in quantum communication and cryptographic key distribution. This puts U.S. intelligence at a potential disadvantage, especially if breakthroughs in error correction allow quantum decryption as early as 2035.

MITRE's message is clear: preparation is essential. U.S. government agencies must transition to post-quantum cryptography immediately, investing in quantum research, supply chain security, and building

robust intelligence monitoring systems. The stakes are high, and a breach could mean catastrophic loss of sensitive information.

As experts warn, staying ahead of adversaries means not just watching them closely but also fostering technological advancement within our borders. With quantum threats on the horizon, delaying action is not an option. The future of national security could depend on the steps taken today.

Takeaway: Embrace the future of encryption now to protect vital data from quantum threats that, while years away, could arrive sooner than anticipated!

The Quantum Countdown: Are We Prepared for a Crypto Catastrophe?

In a new report, MITRE highlights the urgency surrounding the potential threat of quantum computers to high-security encryption systems, particularly RSA-2048, which currently safeguards classified data. While projections suggest that quantum computers capable of breaking RSA-2048 may not materialize until 2055 to 2060, the acceleration of quantum technology, especially in nations like China, is raising alarms.

Key Insights on Quantum Threats and Encryption

1. **Timeline for Quantum Threats:** Although experts believe that fully operational quantum computers are decades away, advancements in quantum communication and cryptography mean that preparations must begin now. Some forecasts anticipate breakthroughs in error correction that could lead to quantum decryption as early as 2035.

2. **Need for Post-Quantum Cryptography:** To safeguard sensitive information, U.S. government agencies are urged to transition to post-quantum cryptography. This includes investing in research and technologies capable of withstanding the future capabilities of quantum computers.

3. **International Concerns:** Adversaries are already investing in quantum technologies, which could give them a strategic advantage. Continuous monitoring of advancements abroad is essential to ensure national security.

Frequently Asked Questions

What is post-quantum cryptography and why is it important?

Post-quantum cryptography refers to cryptographic algorithms that are designed to be secure against the potential threats posed by quantum computers. It is crucial because traditional algorithms like RSA and ECC (Elliptic Curve Cryptography) could be rendered obsolete by quantum computing, making sensitive data vulnerable to exploitation.

How likely is it that quantum computers will be able to break current encryption methods by 2035?

While major breakthroughs are still being researched, experts warn that advancements in quantum algorithms and error correction techniques could make it feasible to perform specific decryption tasks on a smaller scale by 2035. This potential capability underscores the need for immediate action in adopting new cryptographic methods.

What steps should organizations take to prepare for quantum threats?

Organizations should start evaluating their current encryption methods and transition to post-quantum cryptographic algorithms. This process involves conducting risk assessments, upgrading infrastructure, and investing in quantum-safe technologies to protect sensitive data from emerging threats.

Relevant Trends and Innovations

- **Innovations in Quantum Key Distribution:** Technologies that enable the secure transfer of cryptographic keys using quantum mechanics are being developed and tested, providing a potential safeguard against quantum decryption.

- **Market Forecasts for Quantum Computing:** The quantum computing market is projected to grow significantly, indicating an increasing need for businesses to stay ahead of technological advancements to secure their data.

Conclusions

As the clock ticks towards a quantum future, the need for proactive measures in cryptography has never been more critical. The safe encryption of sensitive data directly impacts national and organizational security, urging immediate dialogue on advancing post-quantum solutions.

18. Sectigo Debuts Post-Quantum Cryptography Testing Platform with Crypto4A

by Kirsten Doyle
https://informationsecuritybuzz.com/sectigo-post-quantum-cryptography-test/

Sectigo has introduced Sectigo PQC Labs, a testing platform developed in collaboration with Crypto4A, a provider of quantum-safe Hardware Security Modules (HSMs).

The platform aims to help companies prepare for the transition to post-quantum cryptography (PQC) by offering a secure environment to test, validate, and implement quantum-resistant cryptographic certificates.

Start Planning for Post-quantum Cryptography

According to Gartner: "Security and risk management leaders need to begin planning for their move to post-quantum cryptography (PQC) now, due to the wide and deep impact of replacing cryptographically dependent systems."

Sectigo PQC Labs enables entities to safely explore, test, validate and create post-quantum cryptographic certificates now, for eventual use in their technology stacks. Doing so allows businesses to gather insights to come up with mitigation plans against PQC's two main threat scenarios of current concern, which are:

- **Harvest Now, Decrypt Later Attacks:** Malicious actors collect encrypted data today with the intent to decrypt it once quantum computers become capable of breaking current encryption methods.

- **Long-Lived Digital Signatures:** Critical digital signatures used in PKI, IoT devices, legal contracts, and medical records could be vulnerable over time as quantum computing advances.

Sectigo CEO Kevin Weiss stressed the importance of addressing quantum threats, stating that the platform provides a secure testing environment for firms to evaluate their systems and plan for a smooth transition to post-quantum security.

Crypto4A's quantum-safe HSM technology plays a key role in the platform's security framework. CEO Bruno Couillard noted that with NIST's plans to deprecate current cryptographic algorithms by 2030 and ban them entirely by 2035, the time for businesses to act is now, to future-proof their encryption strategies.

Sectigo PQC Labs offers:

- A sandbox environment for testing PQC assets, including post-quantum certificates.
- Educational tools to facilitate PQC integration into existing PKI.
- Security strategy enhancements for organizations adopting a quantum-readiness approach.

The launch aligns with Sectigo's broader QUANT (Quantum-resistant, Uncover, Assess, Navigate, Track) readiness strategy, aimed at guiding organizations through the transition to PQC.

A Very Real Threat

Quantum computers that can break modern cryptography should become a reality within the next decade, comments Dr Adam Everspaugh, Cryptography Expert at Keeper Security. "Though the date is uncertain,

the superiority of quantum computing capabilities poses a very real threat to nation-states, enterprises, and individuals."

Everspaugh says while quantum computing has the potential to revolutionize various fields, it also threatens current public key encryption methods. The primary attack of concern is store-and-crack (harvest now, decrypt later) where attackers may capture and store encrypted information and web traffic now, and then, when quantum computers are available, break the encryption to read the data that is stored.

"If this information is still valuable in the future, attackers can use it to exploit sensitive systems. At Keeper Security, we are actively tracking developments and updating our product roadmap to ensure we're ready to integrate the latest cryptographic standards as soon as production software libraries fully support them," Everspaugh adds.

Considerable Time and Effort

Philip George, Executive Technical Strategist at Merlin Cyber, says Post-Quantum Cryptography (PQC) presents an opportunity to introduce quantum-resistant cryptography and system-level agility into IAM and zero-trust protection strategies.

This, George adds, will ultimately grant the industry more time to explore QIST-based enhancements to the digital identity and access management ecosystem as well as a greater technology landscape. "Whether leveraging classical, PQC, or QIST based computing, data and human/machine based identities will remain high value targets, especially in a potentially quantum connected world."

Migrating to the new post-quantum algorithms will take considerable time and effort, says George. Aligning these activities with similar large-scale modernization efforts like zero-trust will be key. "As such, an alignment will ensure the significant effort to adopt ZTA principles won't be undone by continuing to rely on soon-to-be deprecated cryptography. Lastly, consider cryptographic agility as a mechanism to reduce the level of effort to adopt the next batch of standards. Such an approach may be necessary to offset more frequent changes to approved crypto standards. We may now be entering a time where long lived standards become a thing of the past as continued progress is made on viable quantum computers."

19. Barcelona Supercomputing Center Unveils Quantum System Developed with 100% European Technology

https://insidehpc.com/2025/02/barcelona-supercomputing-center-unveils-quantum-systen-developed-with-100-european-technology/?utm_source=substack&utm_medium=email

The Barcelona Supercomputing Center – Centro Nacional de Supercomputación (BSC-CNS) – has presented what it said is the first quantum computer developed with 100 percent European technology.

"This milestone consolidates BSC at the forefront of supercomputing in Europe and lays the foundations for a new era of hybrid computing, combining traditional and quantum computing," the center said in its announcement.

The new system is part of Quantum Spain, an initiative coordinated by BSC and promoted by the Ministry for Digital Transformation and Public Administration, through the State Secretariat for Digitalisation and Artificial Intelligence (SEDIA). Funded by the Recovery, Transformation and Resilience Plan, the initiative is part of the Digital Spain 2026 programme and the National Artificial Intelligence Strategy (ENIA).

Quantum Spain is a collaborative effort involving 27 leading research and supercomputing institutions in Spain, including the 14 nodes of the Spanish Supercomputing Network (RES) and other institutions such as CSIC, ICFO and universities such as the University of Barcelona, the Autonomous University of Madrid and the Polytechnic University of Valencia, among many others.

The new quantum computer was presented today, at an event held in the Torre Girona chapel, where the BSC installed the first four versions of the MareNostrum and now houses the new quantum infrastructure that will be integrated into MareNostrum 5, the most powerful supercomputer in Spain and one of the most advanced in the world.

The event was attended by the President of the Generalitat de Catalunya, Salvador Illa, the Minister of Science, Innovation and Universities, Diana Morant, the Minister for Digital Transformation and the Civil Service, Óscar López, the Catalan Minister of Research and Universities, Núria Montserrat, the Government Delegate in Catalonia, Carlos Prieto, the Secretary of State for Science, Juan Cruz Cigudosa, and the Secretary of State for Digitalisation and Artificial Intelligence, María González Veracruz.

The integration of this new digital quantum computer into the MareNostrum 5 supercomputer represents a significant advance in the country's computational capacity. This new system will be joined by one of the first European analogue quantum computers, awarded to BSC by the European Commission's High Performance Computing Joint Undertaking (EuroHPC JU). Both systems offer complementary technologies and make up the BSC's quantum infrastructure, reinforcing its role as a key player in the European advanced computing landscape and consolidating Spain as a leader in quantum research and supercomputing.

The combination of quantum and classical technologies will boost research and innovation, fostering industrial and technological progress in Spain and contributing to the creation of highly qualified jobs. The new system will be available to the scientific community, companies and public organisations through the access mechanisms of the Spanish Supercomputing Network (RES).

Quantum computing has the potential to transform diverse fields by enabling the study of phenomena at the atomic level. Its applications range from chemistry, where it could accelerate the development of new materials and medicines, to the resolution of complex problems in sectors such as logistics and finance.

Moreover, its ability to optimise processes makes it a key tool for these areas, especially when combined with artificial intelligence to develop more efficient machine learning algorithms. In the field of security, this technology could transform cryptography, presenting new challenges, but also offering more robust solutions.

The construction of Quantum Spain's new quantum computer has been led by the joint venture formed by the Spanish companies Qilimanjaro and GMV, which contributed their experience in cutting-edge technologies to develop a system based on superconducting qubits, the fundamental units of quantum computing. These cubits, unlike traditional bits, can represent multiple states simultaneously, allowing them to perform much more complex calculations.

This system, built with 100% European technology, represents a decisive step in Spain's strategy in quantum computing and reinforces European technological autonomy, aligning with the European Commission's strategy to reduce dependence on key infrastructures from third countries.

20. Call for action: urgent plan needed to transition to post-quantum cryptography together

https://www.europol.europa.eu/media-press/newsroom/news/call-for-action-urgent-plan-needed-to-transition-to-post-quantum-cryptography-together?utm_source=substack&utm_medium=email

On 7 February 2025, Europol hosted a Quantum Safe Financial Forum (QSFF) event, during which the QSFF has issued a call to action for financial institutions and policymakers, urging them to prioritise the transition to quantum-safe cryptography. With the rapid advancement of quantum computing, the financial sector faces an imminent threat to its cryptographic security. This transition presents both a challenge and an opportunity to enhance cryptographic management practices across the industry. During the event, representatives from leading organisations discussed the need to urgently address the transition and the challenges industry peers, vendors, policymakers, and society are facing.

A coordinated approach to the transition

A sufficiently advanced quantum computer has the potential to break widely used public-key cryptographic algorithms, endangering the confidentiality of financial transactions, authentication processes, and digital contracts. While estimates suggest that quantum computers capable of such threats could emerge within the next 10 to 15 years, the time required to transition away from vulnerable cryptographic methods is significant. A successful transition to post-quantum cryptography requires collaboration among financial institutions, technology providers, policymakers, and regulators.

The forum recommends the following key actions:

1. Financial institutions and policymakers should prioritise the transition to quantum-safe cryptography and actively support its implementation.

2. Coordination among different stakeholders will be key, ensuring alignment on their planning, roadmaps and the concrete implementation of the transition to PQC, establishing common goals and a shared view of the requirements to achieve them.

3. There is no need for additional legislation to be made, a voluntary framework established between regulators and the private sector would be sufficient, setting guidelines for quantum-safe cryptography and promoting standardisation across institutions.

4. This transition presents an opportunity to enhance cryptography management practices. A forward-looking framework to cryptography management is needed.

5. Promote collaboration, knowledge sharing and fostering a cohesive approach across jurisdictions at global scale. This means encouraging the industry, including private and public sector actors, to partner up in the context of quantum-safe experiments, projects, Points of Contact and other initiatives.

The threat of 'Store now, decrypt later' and the regulatory response to it

The QSFF warns of the increasing risk posed by 'Store now, decrypt later' (SNDL) attacks, where malicious actors collect encrypted data today with the intention of decrypting it in the future using quantum computing. Sensitive financial information, including long-term investment strategies and confidential agreements, could be compromised if urgent security measures are not taken.

These challenges have been identified by Europol and presented in the First Report on Encryption, published by the EU Innovation Hub, and The Second Quantum Revolution report, published by Europol's Innovation Lab. Although these reports focus on the law enforcement perspective, there are synergies that can also be applied to the financial industry.

Governments and regulatory bodies worldwide have begun addressing the quantum threat, with the introduction of major regulatory acts in Europe, the United Kingdom, the United States and Singapore. Despite these efforts, a 2023 survey of 200 financial sector leaders found that 86% of organisations feel unprepared for post-quantum cybersecurity. Additionally, 84% anticipate the need to adopt quantum-safe solutions within the next two to five years.

The QSFF urges financial institutions, vendors, and policymakers to take immediate steps towards a quantum-safe financial ecosystem. The QSFF emphasises that action should be taken promptly to protect the industry from significant risks, financial losses, and reputational damage.

21. QuSecure's Post-Quantum Cryptography Featured at Davos 2025

by Rashmi
https://www.bisinfotech.com/qusecures-post-quantum-cryptography-featured-at-davos-2025/

QuSecure™ has announced its inclusion in the inaugural World Economic Forum (WEF) Quantum Application Hub, which debuted at the WEF Annual Meeting in Davos, Switzerland, last month. The hub provided a platform for attendees to explore real-world quantum applications, including QuSecure's advanced post-quantum cryptography solutions. This milestone underscores QuSecure's leadership in quantum-resilient cybersecurity and its role in shaping the future of secure digital infrastructure.

The WEF Quantum Application Hub allows world leaders, policymakers, and industry executives to experience the revolutionary impact of quantum technologies firsthand. As quantum computing evolves, the urgency to implement quantum-safe encryption has become critical. QuSecure's inclusion highlights its commitment to securing global communications and data against emerging quantum threats.

"We were honored to be part of the inaugural WEF Quantum Application Hub and to have demonstrated crypto-agility to the global leaders at Davos," said Rebecca Krauthamer, CEO of QuSecure. "It's a privilege to collaborate with visionary leaders like Arunima Sarkar and Shreyash Ramesh on this impactful initiative, providing hands-on insight into the real-world possibilities of quantum technology and bringing its impact beyond theory and into reality for global leaders."

Through the QuSecure Experience Protection application, visitors can explore industry-specific scenarios demonstrating how quantum computing affects networks today, particularly encryption for data in transit. They can step into the role of a network administrator, executing cryptographic agility with a few clicks and experiencing next-generation cryptography in real time.

22. If you're not working on quantum-safe encryption now, it's already too late

by David Gewirtz
https://www.zdnet.com/article/if-youre-not-working-on-quantum-safe-encryption-now-its-already-too-late/

Remember Nokia? Back before smartphones, many of us carried Nokia's nearly indestructible cell phones. They no longer make phones, but don't count Nokia out. Ever since the company was founded in 1865, Nokia has successfully pivoted to industries showing promise.

Here's a fun trivia fact you can use at your next party: Nokia once made toilet paper. In fact, the company was initially founded as a pulp mill. Later, the Finnish company made rubber boots and respirators.

Here's another name you might be familiar with: Bell Labs. For years, Bell Labs was at the forefront of technology research. In fact, UNIX (which inspired Linux) was developed at Bell Labs, along with many other critical technologies like lasers, transistors, the C and C++ programming languages, and even optical fiber systems. In 2016, Nokia acquired Bell Labs.

Now, Nokia's portfolio of hardware and software solutions -- spanning mobile and fixed network infrastructure, cloud data center technologies, and beyond -- serves as a foundation for digitalization and the AI and quantum era across industries.

According to Martin Charbonneau, head of Quantum-Safe Networks at Nokia, "7 out of 10 fiber-connected homes in the US use Nokia technology, 15 out of 20 power utilities in the US, and more than 1,000 public sector organizations worldwide trust our technologies for their critical operations."

ZDNET had the opportunity to sit down with Martin to discuss another transformative technology on the cusp: quantum computing. Quantum computing is expected to be able to solve some problems a million times faster (yes, you read that right, a million) than conventional computing. Some of our most robust encryption algorithms could take tens or hundreds of thousands of years to crack using traditional computing. But with quantum computing, those problems could be solved in seconds.

Let's dive deep into what this all means for telecommunications, security, AI, and our future.

ZDNET: How does quantum computing differ from classical computing?

Martin Charbonneau: Conventional computers are based on the concept that electrical signals can be in only one of two states or binary bits to store and process data -- on or off, zeros and ones.

Quantum computers are based on the principles of quantum mechanics. Quantum computers can encode more data concurrently using quantum bits, or qubits, in superposition, which can scale exponentially. A qubit can behave like a bit and store either a zero or a one, but it can also be a weighted combination of zero and one at the same time.

Because they are not limited to only one state at a time, they can perform tasks exponentially faster than classical computers and can also carry out multiple processes at once, further increasing their capacity and speed.

ZDNET: Why does quantum computing pose such a significant threat to current encryption methods?

MC: Quantum computers can solve problems or compromise mathematical cryptography algorithms in mere minutes that would have taken even the biggest conventional supercomputers thousands of years to compromise.

The point when a quantum computer exists that can break common encryption in use today is called Q-Day, and the computer that could break it is referred to as a CRQC or Cryptographically Relevant Quantum Computer.

ZDNET: Could you provide an example of a critical industry particularly vulnerable to quantum-based attacks?

MC: Many of the particularly vulnerable industries are the organizations we think of as being targets of cyber threats today, like governments and defense organizations.

But in reality, with today's public key cryptography rendered useless, all networks -- across all industries -- will become vulnerable to attack. Threat actors could cripple critical infrastructure by attacking the networks that support them.

Quantum threats could impact power and water supplies, public transportation systems, telecommunications, public safety communications, financial market data and systems, healthcare research and hospital networks, and more -- with life-threatening and economy-impacting consequences.

Quantum attacks won't target only those companies or organizations that are using quantum computers themselves. A CRQC poses a threat to any industry, as well as the businesses and individuals they serve.

It is a matter of risk management for all.

ZDNET: What are the primary encryption methods at risk with the advent of quantum computing?

MC: As we move into the Quantum 2.0 age [actual use, rather than theoretical research -- DG], many of the standard cryptography algorithms and protocols in place today are at risk from a CRQC.

The Information Communications Technology (ICT) industry is realizing the seismic impact of this and is undergoing a significant migration of its cryptographic practices, with many organizations already in the planning stage, and some in a migration or execution phase.

To date, we have been 'lucky' that our existing mathematics cryptography algorithms have not been previously compromised. So, moving forward we must build a robust and resilient cryptography tool kit that addresses the potential of quantum computing.

This is essential to ensure we can support our continued digitalization and ensure a Quantum Secure Economy.

ZDNET: What role does artificial intelligence play in both enabling and mitigating risks related to quantum computing?

MC: AI can significantly enhance quantum computing by optimizing quantum algorithms and improving efficiency. This means quantum computers can solve complex problems faster and more effectively by using fewer quantum computer resources. AI also helps in developing new quantum algorithms and managing the vast amounts of data processed by quantum computers.

On the flip side, AI may also enable quantum threats. For example, AI may help quantum computers break current encryption methods much faster with new algorithms. Additionally, AI may automate and enhance attack strategies, creating new ways to exploit vulnerabilities.

AI may also play a crucial role in defending against quantum threats. It may help develop quantum-safe cryptographic algorithms that are resistant to quantum attacks. AI-driven risk assessment tools may continuously monitor systems for potential threats, detect anomalies, and provide real-time insights to mitigate risks. This may enrich the security and trust of our digital infrastructure.

ZDNET: How imminent is the threat of quantum computers breaking existing encryption standards?

MC: The arrival of a CRQC is not an "if," it's a "when." The timing of a CRQC is directly related to the advancement (and stability) of quantum computing. The faster a mature/stable quantum computer arrives, the sooner the threat arrives.

There are many organizations and governments around the world working on advancing quantum computing technologies so we can realize the vast benefits of the technologies. Concurrently, other organizations are looking at the innovation speed and advancements to measure how soon a threat could arise.

One report on the topic is the Quantum Threat Timeline report from the Global Risk Institute . Their latest analysis puts a 14% chance of a CRQC becoming available in the next 5 years.

This may sound like a small number, but it increases rapidly with time, where the risk is over 60% in 15 years based on the current status of quantum computing. The pace of innovation in quantum computing is not slowing either. Its acceleration could mean the timeline looks different next year. So, the idea is to be aware of the threat and take action now to protect critical infrastructure.

While the availability of the CRQC may not come in the near term, threat actors are already preparing for Q-Day. Many are collecting encrypted data from target organizations today and storing it so that it can be decrypted when the evolution of quantum computing delivers a CRQC capable of rendering some existing cryptographic algorithms obsolete. The industry refers to this ongoing activity as harvest now, decrypt later (HNDL).

These are severe risks, and the timeline to transition to a new quantum computer-secure future, with techniques such as post-quantum cryptography security models, is intricate. Our industry must take proactive measures now. We need to plan and deploy quantum-safe cryptography-based solutions in a defense-in-depth approach to provide secure and trusted connectivity, enable a quantum-safe global economy, and continue digital transformation.

Many global policy, regulatory, and government agencies (CISA, NSA, NIST in the US, for example) are urging critical infrastructure industries to make the move now to protect their data and critical communications.

ZDNET: What is post-quantum cryptography?

MC: Post-quantum cryptography (PQC) is one of the key methods to protect sensitive information as quantum computers evolve, posing risks to current encryption.

By developing quantum-resistant algorithms, PQC helps ensure long-term data security and maintain trust in digital economies. PQC will be used in applications such as banking transactions, secure communications, and protecting intellectual property, with organizations like NIST in the United States leading standardization efforts.

Today, many applications rely on public key infrastructure (PKI) for the generation and management of encryption keys. PQC seeks to improve upon today's cryptography by modifying the underlying mathematical methods used by these ciphers. PQC is only one of the required elements in creating quantum-safe networks.

ZDNET: What role does standardization play in preparing industries for a quantum-secure future?

MC: For main principles or technologies, quantum security encompasses more than just post-quantum cryptography (PQC). It involves building cryptographic resiliency through a defense-in-depth approach, which we believe is realized by utilizing multi-layer encryption and diverse cryptosystems, such as pre-shared keys and quantum key distribution.

Meanwhile, standardization plays a critical role in preparing industries for a quantum-secure future by ensuring interoperability, security, and compliance. In the US, NIST's post-quantum cryptography (PQC) standards provide robust encryption algorithms designed to withstand quantum attacks. The IETF is

integrating PQC algorithms into secure protocols, which are then adopted by 3GPP for telecommunications.

Globally, ETSI and ITU focus on Quantum Key Distribution (QKD) to secure communication networks. Additionally, cybersecurity recommendations from agencies such as the NSA, ANSSI, and BSI guide industries in adopting secure-by-design principles and quantum-resistant technologies.

These efforts collectively build a resilient and secure digital infrastructure, ready to face the challenges posed by quantum computing.

ZDNET: How are different industries preparing for quantum risks?

MC: Government and defense industries are on top of the risk and acting as leaders. We also see progressing adoption across other industries, like Banking Financial Services and Insurance (BFSI) and mission-critical networks.

Different industries move at different paces based on their risk profile and the complexity and criticality of their infrastructure. We see in virtually every industry we work with (which spans telecoms, the public sector, and enterprise) that some organizations are still in a learning phase, some are identifying their unique risks, and yet some are still in the assessment phase.

Some leading organizations (across different industries, interestingly) are engaging in partnerships to drive quantum-security. For many industries, movement will inevitably come as global policy, regulatory, and government agencies impose mandates to ensure quantum security.

ZDNET: How does Nokia's approach to quantum safety address the specific needs of these industries?

MC: As we continue on our digitalization journey, it's clear that the importance of having safe and trusted connections will only continue to grow. Our reliance on safe and trusted connectivity is increasing, and it's essential that we act now to shield our digital future from the quantum paradigm shift.

In addition to promoting the adoption of PQC for obtaining quantum-safe applications, we are also promoting quantum-safe networks. This focuses on agile solutions with a defense-in-depth approach, through multi-layered network cryptography technology options, that can adapt to unique business needs, deliver the confidence to scale network deployments, and evolve as the quantum threat evolves. This complementary approach is all about reducing risk and ensuring trust in our digital communication infrastructure.

We believe this outcome is not just a short-term solution, but a long-term strategy that will persist through time. It's a trust-enabling bridge between current networks and the future quantum economy. And it's not just about today -- it's about generations to come.

Consumers, enterprises, mission-critical infrastructure builders, and communication service providers are all seeking this outcome of having quantum-safe security. They want to ensure that their digital communication infrastructure and data remain secure, reliable, and trustworthy.

At Nokia, we're committed to delivering this outcome. We have quantum-safe solutions today -- proven and ready for immediate implementation. Concurrently, Nokia Bell Labs is at the forefront of leading-edge research in specific technological domains, driving innovation with key academic and technology partners and shaping the future of quantum computing and quantum-safe network solutions.

ZDNET: How does proactive quantum-safe planning compare in cost and effort to reactive measures taken after vulnerabilities are exploited?

MC: We've seen the effects and costs of significant cyber breaches. IBM has estimated in a report that the cost of the average cyber breach is over $4.8M USD. And even beyond the cost, the loss of public trust, and impact on a company's brand can be significant.

To assess an organization's risk factor, Dr. Michele Mosca of the University of Waterloo and EvolutionQ created a risk assessment theorem. This is where an organization needs to take into consideration the time it will take for a CRQC to become a reality, the time it will take the organization to migrate its cybersecurity systems, and the length of time its data needs to remain secure.

Our industry needs to reflect on the time required to migrate to quantum-safe cryptography through the lens of the Mosca Equation, which further reinforces that we already have a zero-day vulnerability.

Conducting a cryptography migration in a crisis is far from ideal. Haste could create new vulnerabilities or incremental vulnerabilities, costs will be increased, and so forth. There's an opportunity to plan for this now, conduct a thorough, thoughtful migration strategy, and roll it out in an effective, controlled, and properly managed way.

ZDNET: How far along is quantum-safe encryption?

MC: There is an awakening in the industry. While PQC is currently in the news, there are other forms of quantum-safe cryptography, like Pre-Shared Key technology (which is actively available and deployed). They're evolving.

These technologies are mature and can be utilized now in a multi-layered approach to protect critical systems. QKD technology is also emerging, evolving, and becoming available.

The announcement of NIST standardization of PQC algorithms was discussed in this recent article from Nokia and Nokia Bell Labs.

ZDNET: How does the concept of "crypto-agility" fit into long-term planning for quantum resilience?

MC: Crypto-agility is the ability to quickly adapt to new cryptographic algorithms and protocols as threats evolve. We believe that crypto-agility is one of the important components [of quantum resilience], but not the only one.

For enterprise applications, this means migrating over time from traditional Public Key Cryptography (PKC) methods such as RSA, which are vulnerable to quantum attacks, to Post-Quantum Cryptographic (PQC) algorithms.

However, crypto-agility is not just about migrating to new algorithms; it's also about the ability to adapt to new threats and vulnerabilities as they emerge. This flexibility ensures that our systems can seamlessly transition to stronger security measures without significant disruptions, maintaining robust protection against emerging vulnerabilities.

Crypto agility needs to be complemented with crypto-resiliency, which involves relying on a digital fabric of complementary quantum-safe cryptosystems. By integrating multiple cryptographic methods, including symmetric cryptography, we ensure continuous protection and adaptability, even in the face of advanced quantum threats.

This resilience is crucial for maintaining the integrity and security of our data over time. Should a PQC algorithm weaken or break over time, the other symmetric cryptosystem would still be offering protection.

Multi-layered quantum-safe cryptography adds additional layers of security by employing multiple quantum-resistant cryptographic techniques. For service providers and enterprises building network-layer connectivity, this means activating complementary quantum-safe network-level encryption using symmetric-based cryptography.

This approach complements the application layer, which uses PKC PQC-based cryptography, reducing the risk of a single point of failure and ensuring that if the application layer is compromised, others remain intact to provide ongoing protection.

Together, these strategies form a robust defense-in-depth framework. By combining crypto-agility, crypto-resiliency, and multi-layered quantum-safe encryption, we create a comprehensive and proactive security posture that can withstand current and future threats, ensuring the security and resilience of our digital infrastructure.

ZDNET: Are there challenges in integrating quantum-safe encryption into legacy systems, and how can they be overcome?

MC: The WEF has estimated that the quantum-safe cryptography migration could force the replacement of between 10 and 20 billion devices globally. Many of these devices are IoT devices and are not capable of migration to quantum-safe cryptography.

In terms of networks where Nokia is a key supplier, we've already embedded quantum-safe encryption engines into our product platforms and silicon.

The challenge for the networking industry is around the generation and automated generation, distribution, and deployment of quantum-safe cryptographic keys.

ZDNET: How does the transition to quantum-safe encryption impact data protection laws, such as GDPR or CCPA?

MC: Quantum-safe data protection complements these regulations. Whether data is in-flight, at rest, or during processing, ensuring data privacy and protection against emerging quantum threats is key to compliance.

ZDNET: Where will quantum-safe cryptography be used?

MC: Quantum-safe cryptography, in the context of our answers, mainly applies to the protection of data in flight.
It will also be applied to digital signatures, firmware, software downloads, etc., used in numerous use cases, from cloud access and data center interconnects, to the digital supply chain and more.

Quantum-safe measures will be integrated and aligned with broader cybersecurity, so at some point, we believe the aim is that everything will be quantum-safe.

ZDNET: What collaborative efforts between private companies and research institutions have been pivotal in advancing post-quantum cryptography?

MC: As we navigate the complex landscape of quantum-safe applications and networks, it's clear that our industry's response requires a collaborative approach. This is not a challenge that can be solved by one company or organization alone. It requires specialized expertise, innovation, agility, and a strong focus on customer intimacy.

Collaboration is vital -- working together to achieve a common goal. Nokia and our collaborators are engaging and bringing together the best minds and expertise from across the quantum and security industry to drive innovation and progress. We are engaged in partnerships with QKD experts, and Public Key Infrastructure with Post-Quantum Cryptography (PKI-PQC) specialists and more.

Using a unified language and framework can help raise awareness about the threat of quantum attacks and the solution of quantum-safe networks. But it's not just about language -- it's about action. We need

collaboration across various players, including application providers, technology vendors, system integrators, research institutions, connectivity providers, and quantum technology innovators.

By working together, we can drive progress, innovation, and adoption of quantum-safe networks. Ultimately, Nokia can ensure that our customers and industries are protected from the threats of the evolving quantum threat landscape.

ZDNET: What would you say to organizations that feel the quantum threat is too distant to warrant immediate action?

MC: While a CRQC may not exist yet, investment and technological evolution are continuing at an accelerating pace, with experts predicting that a CRQC will be available within the next 5 to 15 years. Transitioning systems takes time; therefore, it's crucial to act now to mitigate your future risks.

Furthermore, encrypted data can be harvested today and held to be decrypted later when CRQCs become accessible, a strategy known as "harvest now, decrypt later" (HNDL). By implementing quantum-safe measures now, customers can protect their data's integrity, confidentiality, and authenticity today and for the quantum future.

Lastly, everyone should understand that the whole ICT sector is migrating to new quantum-safe cryptography. Thus, immediate action should take place for an organization to plan, define, and execute an ordered and resilient migration. Such an approach will minimize risk and costs.

ZDNET: Could you share your vision of what a fully quantum-safe critical infrastructure might look like in the next 10–20 years?

MC: In the next 10 to 20 years, we foresee a fully quantum-safe digital world, where advanced quantum-safe technologies will protect sensitive data at both the application and network layers. Post-Quantum Cryptography (PQC), Pre-Shared Key (PSK) cryptography, and Quantum Key Distribution (QKD) will ensure secure, confidential, and tamper-proof communications.

We believe this world will be built on a robust defense-in-depth framework, ensuring that the entire communication fabric is quantum-secure against both current quantum threats and future advancements in code-breaking.

This will be realized by complementing quantum-safe applications with network-level quantum-safe cryptography, embracing a crypto-resilient approach that utilizes both asymmetric and symmetric cryptography.

In this future world, organizations will employ AI-driven risk assessment tools to continuously monitor and mitigate potential quantum threats. This will ensure that security, privacy, and trust -- essential elements for our digital economies -- create a robust, crypto-resilient world capable of withstanding the challenges posed by quantum computing.

That said, let's remember that this vision of a quantum-safe future begins now, today, safeguarding generations to come.

ZDNET: Lastly, how do you foresee quantum-safe encryption evolving as quantum computing technologies mature?

MC: Depending on the timeframe, as we advance with quantum communication, the pure act of connecting to one another will need to be quantum-safe. All communications will need to be quantum-safe.

As the world moves forward and technology evolves, the threats will similarly evolve. So, much like our world today, we will need to continue to stay on top of emerging threats. Unfortunately, no silver bullet will solve all of our cybersecurity challenges.

It's an arms race of sorts, but there are powerful tools that can be deployed in a proactive way to mitigate the risk to our economy and society.

23. Post-Quantum Cryptography—Securing Semiconductors in a Post-Quantum World

by Enrique Martinez, EnSilica
https://www.allaboutcircuits.com/industry-articles/post-quantum-cryptographysecuring-semiconductors-in-a-post-quantum-world/

Quantum computing advances are exciting, but they're also a looming threat to securing ICs, driving the need for Post-Quantum Cryptography (PQC). Learn about PQC, how it's being implemented, and the legislation involved.

Quantum computing isn't just a step forward. It's a leap. It has the potential to fundamentally upend computing and set an entirely new standard, allowing computers to solve complex problems and overcome optimization barriers that were previously thought impossible.

Google recently achieved "quantum supremacy"—a theoretical benchmark at which a quantum machine performs a task far beyond the capabilities of a non-quantum supercomputer. The experiment, which Google carried out to demonstrate the potential of quantum computing, would have taken a classic supercomputer almost 50 years to complete. Much is said of the AI revolution, but quantum computing will prove to be the big game changer.

However, while quantum computing promises to deliver extraordinary leaps forward in processing power, it also has the potential to render today's public key cryptography obsolete. As semiconductor technology advances, the role of cryptography in securing integrated circuits has become core to their development.

Application-Specific Integrated Circuits (ASICs), are custom-designed for specific tasks, often embedded in devices in environments where security is critical, such as in communications, financial systems, and defense applications. The cryptographic algorithms embedded in these chips are the first line of defense against unauthorized access and data breaches. However, as quantum computing rises to supremacy, the cryptographic methods that have long protected these systems are now under threat.

Quantum computers, unlike classical machines, can process complex calculations at unprecedented speeds, threatening to unravel the encryption that currently safeguards sensitive data. This looming challenge has spurred the development of Post-Quantum Cryptography (PQC), a new class of cryptographic algorithms specifically designed to resist quantum attacks. These algorithms are not just theoretical. They are rapidly being integrated into the next generation of ASICs, ensuring the products using these specialized chips remain secure against future quantum threats.

The Evolution of Cryptography in ASICs

Hardware accelerators are preferred over software implementations for cryptographic functions in ASICs due to several key advantages. Firstly, they offer significantly lower latency and higher throughput, meeting the stringent performance requirements of modern applications. Secondly, by offloading cryptographic tasks from the CPU, hardware accelerators reduce the overall load on the system's main processor, allowing it to handle other critical tasks more efficiently. Lastly, hardware accelerators enhance security by providing dedicated, tamper-resistant environments for cryptographic operations, which are less vulnerable to side-channel attacks.

Initially, classical cryptographic algorithms like AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman, named after the three inventors who pioneered it) provided robust enough security for data in sectors ranging from finance to telecommunications. These algorithms, based on the principles of symmetric and asymmetric encryption, were embedded into ASICs as hardware accelerators to ensure that sensitive data remained protected during transmission and storage. However, as conventional computational power increases and threats become more sophisticated, the limitations of these algorithms have begun to surface.

Both are vulnerable to brute force attacks, where hackers use trial and error to guess an encryption key. Until recently, brute force attacks on AES or RSA encrypted systems were virtually impossible or would take so long to achieve that it was barely worthwhile. While AES with 256 key size is still considered secure against quantum computers, in 2023, one researcher discovered a flaw in RSA that has existed for more than 25 years, but it's only as computing power has evolved that this flaw has begun to pose a real problem.

This has led to the development of advanced techniques such as Elliptic Curve Cryptography (ECC), Elliptic Curve Digital Signature Algorithm (ECDSA) which are higher performance, more secure, smaller key size, replacements of RSA. The ECC/ECDSA algorithm is computationally much more complex than RSA and in nearly all use cases require hardware acceleration.

These algorithms with relatively compact hardware accelerators can be used in resource-constrained environments like embedded systems. However, even these algorithms will eventually be thwarted by quantum computing as it becomes more readily available. A quantum computer has the potential to solve complex mathematical problems, like factoring large prime numbers, exponentially faster than classical computers, rendering current encryption methods like RSA, ECC, and ECDSA potentially vulnerable, while AES with 256 key size is still considered secure against quantum computers.

The Rise of Post-Quantum Cryptography (PQC)

This impending threat has accelerated the shift towards PQC, signalling a new phase in the evolution of cryptography hardware accelerators within ASICs.

PQC algorithms are specifically designed to be secure against the power of quantum computing. Among the most promising are CRYSTALS-Kyber, an asymmetric key encapsulation mechanism to replace the functionality of the ECC algorithm and CRYSTALS-Dilithium, a lattice-based digital signature scheme to replace the ECDSA.

Both have been now standardised by the National Institute of Standards and Technology (NIST) as part of their post-quantum cryptography standardization process. These PQC algorithms are an order of magnitude more complex than the classical algorithms generally requiring hardware acceleration for the majority of application use cases. For backward compatibility most systems will also be required to support classical cryptography as well.

The silicon resources of a cryptographic accelerator depend on the cryptographic operations to be supported, performance required (signing/key generation time or throughput) and the maximum bits in the key size you need to support for each type algorithm.

Cryptography algorithm	Typical gate count of hardware accelerator (NAND2)	Remark
RSA	40 k	2048-bit key size
ECC	150 k	384-bit key size
ECSA	180 k	384-bit key size
AES	60 k	256 bit-key size
SHA256 (SHA2)	15 k	
SHA512 (SHA2)	30 k	
SHA3	60 k	
CRYSTALS Kyber	250 k	ML-KEM-512/768/1024
CRYSTALS Dilithium	750 k	ML-DSA-44/65/87

Integrating these algorithms into ASICs is not just a theoretical exercise but a necessary step in future-proofing digital security. By adopting PQC, we can ensure that our critical infrastructure remains secure even as quantum computing becomes more widespread, marking a critical moment in the evolution of cybersecurity.

Implementation Timelines and Legislation

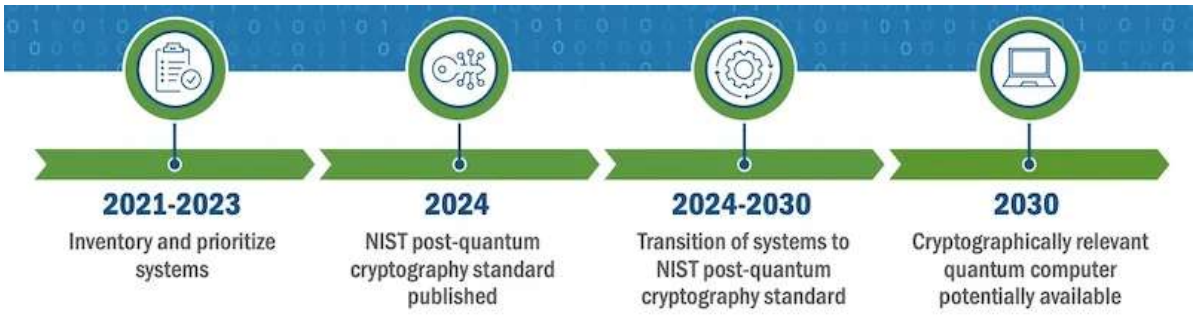
Implementing PQC now is crucial to proactively safeguard sensitive data against future quantum threats, preventing potential data harvesting attacks. A data harvesting attack, often referred to as a "harvest now, decrypt later" attack, involves adversaries stealing encrypted data today with the intention of decrypting it in the future once quantum computers become available. This type of attack poses a significant risk, as data harvested now could be vulnerable to decryption in the future, compromising its confidentiality and integrity.

The risks associated with quantum computing were once as ethereal and difficult to define as the technology itself—a problem that felt so distant it was hardly worth worrying about. Technology waits for no one, however, and as the risks associated with quantum computing become more apparent, governments and regulatory bodies are stepping up efforts to enforce stronger cybersecurity measures.

Recent legislation, such as the EU Cyber Resilience Act, mandates that devices, including ASICs, incorporate more advanced security features to protect against emerging threats, including quantum

threats. This legislation is driving a wave of redesigns and upgrades, as companies strive to ensure that their products meet these new standards and are resilient against both current and future vulnerabilities. This legislation is set to enter into force by the end of 2024, with manufacturers required to place compliant products on the market by 2027.

The United States Department of Homeland Security (DHS) has provided guidance on the timescales for the implementation of PQC. DHS has stated that each using organization should develop a plan for systems transitions upon publication of the new post-quantum cryptographic standard (August 2024) and be fully prepared by 2030 when they believe quantum computers are potentially available. They also state the transition plans should consider creating cryptographic agility to facilitate future adjustments and enable flexibility in case of unexpected changes. The full infographic is available on the DHS website.



The push for PQC is not just about staying ahead of technological advances; it's increasingly a matter of regulatory compliance. As these laws take effect, companies that fail to adopt PQC and other enhanced cryptographic measures risk not only data breaches but also legal and financial penalties. The integration of both classic cryptography and PQC algorithms in ASICs is therefore becoming a critical strategy for companies looking to secure their products in an era of heightened cybersecurity awareness.

What Does This Mean For The Product Landscape?

Classical and PQC cryptographic accelerators are becoming essential building blocks in any ASIC, to the extent that they are now likely to be as significant as the selection of a CPU. The first ASICs likely to incorporate these accelerators will be those used in network infrastructure, where high throughput requirements necessitate hardware accelerator support. For ASICs of 28 nm and below, the silicon overhead is manageable, making it a viable option to future-proof ASIC technology.

The adoption of these technologies is already in progress. PQC and classical hardware accelerator libraries are being developed and licensed. However, given the long development cycle (typically 2–3 years) of these complex ASICs, FPGA-based (Field-Programmable Gate Array) accelerators will serve as a bridging solution, quickly migrating to an ASIC if volumes and performance demand it.

Unlike traditional processors, which execute instructions in a predefined sequence, FPGAs can be programmed to implement custom hardware circuits tailored to particular workloads. A companion ASIC

would use classical encryption to secure the connection to the main system ASIC and add high-throughput PQC functionality via PCIe or similar low-latency, high-speed serial protocols.

In 2025 it's likely that "post-quantum readiness" will become a major selling point for many networking, communication and industrial products in the coming years, but whatever the product—PCQ support is no longer something that can be ignored.

24. Quantum Computing: Preparing for a Post-Quantum World in the Cybersecurity Domain

by Munish Gupta
https://timestech.in/quantum-computing-preparing-for-a-post-quantum-world-in-the-cybersecurity-domain/

Microsoft's announcement of 2025 as the year to become quantum-ready is certainly encouraging organizations to become well-prepared for a quantum future. Quantum Computing, which focuses on the development of computers on the principles of quantum theory and solves problems that cannot be cracked by classical computing, is a giant leap in computing capability. Unlike classical computers, quantum computing leverages quantum bits or qubits and has the potential to revolutionize several industrial sectors such as healthcare, cryptography, pharmaceutical, cybersecurity, manufacturing, financial services, and more. Governments and businesses across the globe are committing billions of dollars to this new technology.

Updated McKinsey analysis for the third annual Technology Monitor predicts sectors such as chemicals, life sciences, finance, and mobility which are likely to see the earliest impact from quantum computing could gain up to USD 2 trillion by 2035. Several industry leaders are expecting fault-tolerant quantum computers to be ready by 2030.

Advantages of Quantum Computing

Quantum computing offers transformative advantages by solving complex problems beyond the reach of classical systems. Recently Google announced that quantum computers could solve a problem or perform a mathematical calculation in 5 minutes that cannot be completed by the world's most powerful supercomputers in 10 septillion years (10×10^{24}). This technology has the potential to offer higher levels of sustainability across agriculture, energy, and other sectors. It can contribute to a more sustainable future by lowering energy consumption and optimizing resource usage, as well as enabling operational efficiency. With the capability to process humongous amounts of data sets and perform real-time computations, quantum computing can accelerate innovation and improve decision-making.

Quantum Computing Threats to Cybersecurity

Although the quantum computing industry is set to make immense progress, studies reveal businesses are skeptical about the technology as it has the potential to challenge data protection and cybersecurity. Organizations are perturbed over quantum computing's capability to decrypt and disrupt today's conventional cybersecurity protocols and widely used cryptographic methods, making digital communications vulnerable. Cryptographically relevant quantum computers (CRQCs) have the potential to decrypt today's encryption standards putting sensitive data with long-term value at risk. CRQCs can disrupt critical systems across healthcare and other industries if quantum-safe measures are not implemented in time. Furthermore, encrypted data intercepted today could be decrypted in the future by leveraging quantum computing, known as the 'harvest now, decrypt later' strategy, and has the potential to become a cybersecurity threat.

Post-Quantum Readiness

With McKinsey estimating that 5,000 quantum computers will be operational by 2030, post-quantum readiness is a top priority for organizations as a key part of their cybersecurity strategy. The drive to adopt post-quantum cryptography (PQC) will enable organizations to avoid threats from cybercriminals and risks associated with quantum computing. PQC includes building cryptographic protocols that can resist potential attacks from quantum computers. The development of post-quantum encryption standards such as Lattice-based Cryptography, Hash-based Cryptography, Code-based Cryptography, and Quantum-safe network design are key. Security teams should focus on post-quantum preparedness which is a multi-year effort.

- **Take inventory and understand risk exposure**

  It is crucial to identify and classify various types of data stored in the organization. Focus on cryptographic assets and algorithms and where they reside. Assets with long-term sensitivity and regulatory requirements should be prioritized. Organizations should also have a good understanding of the potential exposure to risks, cryptography standards embedded into systems, and how data is safeguarded. This knowledge can help in establishing the need and urgency of PQC and the relevant roadmap. Additionally, PQC migration efforts should consider both technical as well as business impact points of view.

- **Establish a transition strategy**

  After establishing data inventory and potential exposure, it is time to develop a mitigation strategy team and allocate roles to respective team members. Prioritize the migration of the most valuable data with the longest shelf-life to post-quantum cryptography. Build a roadmap to leverage quantum-safe algorithms.

- **Collaborate with trusted providers**

It is crucial to collaborate and work with trusted solution providers and cybersecurity experts experienced in quantum-safe technologies. The IT vendors of organizations should have a deep knowledge of post-quantum implementation.

- **Monitor technological developments**

  Staying well-informed about developments in quantum computing and PQC is important as it will support security teams to anticipate and mitigate potential risks.

- **Educate all stakeholders**

  All relevant teams and key stakeholders should be educated on the progress in quantum computing and associated security risks. They should also be trained in the adoption of new cryptographic standards.

The Post-Quantum era is definitely going to be a big shift for the IT ecosystem of organisations and requires heavy lifting. They should definitely start looking into existing architecture and identify ways to re-architect to minimize the impact and to have Architecture of the future to support business.

Governments and organizations have to invest in quantum research and developing a quantum-ready workforce, while establishing a quantum-resilient infrastructure to be well-prepared for a post-quantum world.

25.Seven Assertions about Quantum Computing

by Gil Kalai
https://gilkalai.wordpress.com/2025/02/05/seven-assertions-about-quantum-computing/

The purpose of this post is to present seven assertions about quantum computing that arose in my research. I welcome questions and remarks and will gladly clarify or elaborate on them.

Four Predictions About Quantum Computation in General

1. **Inherent Noise in Two-Qubit Gates**
   Two-qubit gates will inherently be noisy. Engineering efforts to reduce this noise will encounter a barrier that prevents achieving the quality required for quantum fault-tolerance.

2. **Correlated Errors in Cat States**

Cat states will inevitably experience substantially correlated errors. (A cat state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ represents entanglement between two qubits.)

3. **Limitations of NISQ Devices**
   Samples generated from boson sampling and quantum computers in the intermediate scale correspond to a primitive computational complexity class called **LDP (low degree polynomials)**. As a result, they are incapable of demonstrating quantum supremacy or achieving high-quality quantum error-correction. This argument imposes a computational-complexity-based limit on the engineering efforts to reduce errors in NISQ (Noisy Intermediate-Scale Quantum) devices.

4. **Noise Sensitivity in Small Quantum Circuits**
   The empirical distributions of samples obtained from 12-qubit random circuits inherently contain a significant noise-sensitive component. This means that the empirical distributions are necessarily non-stationary (changing over time), and are inherently unpredictable.

Three Assertions About Google's 2019 Quantum Supremacy Experiment

1. **Statistical Unreasonableness in Fidelity Predictions**
   Predictions based on the fidelities (error-rates) of individual components of Google's experiment were successful in a statistically unreasonable manner.

2. **Lack of Separation Between Calibration and Sampling Stages**
   Contrary to Google's description of their experiment, there was no strict separation between the calibration stage and the stage of generating samples from large quantum circuits.

3. **Lack of Transparency in Crucial Data**
   Google has not provided essential data required to rigorously scrutinize their experiment. Specifically:

   - Over five years after the experiment, the team has not shared the individual two-qubit gate fidelities. This lack of disclosure is unreasonable.
   - Details about the calibration stage remain concealed under commercial secrecy.

Assertions (1)-(4) form part of my broader *argument against quantum computers* (see this post for a brief description and this paper); Assertion (1)-(3) are part of *the case against the Google 2019 quantum supremacy experiment* (see this post for a summary and links to my relevant papers).

I believe all seven assertions are correct; however, they are not definitive. For the four assertions in the first part, the arguments are partially heuristic, and I do not anticipate stronger claims in the form of a mathematical theorem proving that quantum computers are impossible, nor a derivation of their impossibility from an agreed-upon physical principle. Additionally, in both parts, there are several counterarguments that warrant consideration.

26. Exploring the potential for quantum advantage in mathematical optimization

by IBM
https://www.ibm.com/quantum/blog/optimization-white-paper

Recent publications from members of the Quantum Optimization Working Group deliver a fresh perspective on the potential for quantum computers to demonstrate value for interesting combinatorial optimization problems.

Optimization problems touch every facet of your life. You decide the best order to run errands to save time, or use your maps app to find an optimal driving route that avoids traffic. Optimization problems also appear widely in the industries that touch our everyday lives. They are crucial in the operation of energy grids, supply chains, and more—helping to ensure stability, safety, and efficiency.

In some cases, we solve these optimization problems using our intuition, or by making common-sense judgments based on prior experience. However, when the considered tasks grow too complex, we need to represent them as optimization problems that we can tackle with mathematics. Over the years, computational methods for solving combinatorial optimization problems have come to play an important role in business and science, and help to solve many of these problems efficiently. Nevertheless, some combinatorial optimization problems remain extremely challenging, even for state-of-the-art methods run on the most powerful classical supercomputers.

Quantum computers have the potential to augment our ability to solve optimization problems. However, questions remain as to which quantum methods and optimization problem classes will enable us to achieve practical quantum advantage. So far, those questions have been difficult to answer because the field of quantum optimization has lacked systematic, reproducible benchmarks that allow us to make fair performance comparisons between quantum and purely classical optimization algorithms—especially given the limitations of what researchers can actually run on current quantum hardware. A white paper recently published in *Nature Reviews Physics* by representatives of the Quantum Optimization Working Group aims to address these challenges.

Co-authored by 46 members of the working group—including representatives from enterprise and academic research institutions like University of Amsterdam, MIT, Zuse Institute Berlin, IBM, Hartree Centre, E.ON, Wells Fargo, and more—the white paper provides a broad overview of optimization methods and explores the potential for quantum advantage in a variety of problem settings. Moreover, it explores potential strategies to improve existing quantum methods. A notable example of this which the white paper mentions comes from promising new collaborative research conducted by IBM, Los Alamos National Lab, and the University of Basel. That research details how applying something known as the Conditional Value at Risk (CVaR) to the samples returned from a quantum computer may be useful for various optimization tasks. More on that later.

The white paper also outlines the essential building blocks for quantum optimization algorithms, and proposes clear metrics and benchmarking problems to facilitate meaningful comparisons between quantum and classical optimization techniques. With the ultimate aim of accelerating progress toward quantum advantage in the field of combinatorial optimization, the paper serves as an important reminder that useful quantum advantages for optimization problems remain well within the realm of theoretical possibility, despite doubts that have been expressed by some in the research community.

Examining the challenges and opportunities of quantum optimization

Quantum optimization is likely one of the most misunderstood and polarizing domains in quantum algorithms research. Early claims suggested quantum computers could efficiently solve hard optimization problems by exploring every possible solution in parallel—a misconception that still shows up occasionally. Others argue that quantum optimization methods can at best provide a quadratic speedup over classical approaches that scale exponentially with problem size—ultimately yielding little value since a quadratic speedup over an exponential runtime is still an exponential runtime.

In the new optimization white paper, the authors explain that the truth, as usual, is more nuanced than either of these extremes. Quantum computers do *not* explore every solution in parallel, at least not in a way that would provide immediate value for optimization. However, the assumption that quantum methods provide only a quadratic speedup for optimization problems is usually based on the worst-case version of problems, and based on the assumption that we have been tasked with finding an optimal solution that is provably better than all possible alternatives.

In the real world, worst-case optimization problem instances are rarely relevant to practical use cases. This is one of the key reasons classical algorithms have proven so useful in practical settings, despite the well known exponential runtimes required to generally solve these problems to provable optimality. In practice, classical algorithms and heuristics can obtain good solutions for many useful problems, even at large problem sizes.

However, there is still a lot of potential to be unlocked through better optimization algorithms. In fields like finance and supply chain management, even small improvements can make a huge impact. Solving real-world problems with purely classical methods involves simplifying them first, for instance, by removing certain factors or approximating the involved dynamics, and finding good solutions for more realistic models could make a huge difference. For some problems, classical algorithms fail to find good solutions altogether—even at relatively small problem sizes.

Quantum computing offers a new set of tools and capabilities that may improve our ability to tackle at least some of the real-world optimization problems that are classically challenging. A "good-enough" solution from a quantum algorithm that's somehow better, that's less costly, or that can be obtained faster than any classical solution has the potential to be immensely valuable.

Is advantage in quantum optimization really possible?

As far as we know, quantum computers will never provide exponential speedups for all instances of all optimization problems. However, we do know special cases of problems that gain exponential speedups from quantum optimization techniques over classical alternatives.

For example, some optimization problems can be reduced to integer factoring, where Shor's algorithm offers an exponential speedup over all known classical methods. This is the most prominent example of exponential advantage in quantum optimization, although not the most useful one, as such problems are unlikely to appear in practice. Still, there are other cases that promise similar speed-ups for efficiently finding better-than-classical solutions to more relevant problem classes, such as this recent result from researchers at Google, and examples like these are encouraging for quantum optimization in general.

While quantum algorithms with provable performance guarantees like the above-mentioned usually require fault tolerance, we also already have quantum optimization algorithms that we can run on today's noisy hardware, and which are already capable of returning good solutions for at least some problems. It is entirely possible that new algorithms—or new variants of existing algorithms—will be discovered that enable quantum methods to rival or surpass the solution quality of classical methods using noisy hardware.

These algorithms are usually heuristics, particularly if executed on a noisy quantum computer. Heuristics are algorithms without a priori performance guarantees that are often based on a deep intuitive understanding of the considered problem, or which are achieved by terminating exact optimization algorithms prematurely.

Heuristics appear all throughout both quantum and classical computing. In fact, *most* classical optimization algorithms that we use in practice are heuristics. Genetic algorithms, A* search, and simulated annealing are all examples of influential classical optimization methods that developers have used for decades and that often work very well in practice.

All of this is to say that, despite their lack of performance guarantees, heuristics are not a bad thing. In many cases, they are the best we can hope for because we know these problems to be difficult in general for both quantum and classical methods. What we need are new quantum heuristics that work well for some of those problems where classical algorithms struggle. Thus, our job as a community is to find exact, approximate, or heuristic quantum optimization algorithms that work better than any classical technique—at least for some problems—as well as develop systematic benchmarks to understand the path to practical quantum advantage in optimization.

New quantum optimization research makes an impact

Today, researchers are beginning to demonstrate that quantum computers, with the help of classical post-processing methods called error mitigation, can deliver accurate expectation values for certain valuable problems. Given a system and a property we want to measure, the expectation value is a weighted average of the possible outcomes from the quantum computer. These are very useful calculations for

chemistry and physics, but for optimization, we're often more interested in samples outputted from the processors, rather than expectation values.

Now, a paper recently published in *Nature Computational Science* highlights how to extract value when sampling from noisy quantum computers in the near-term. Specifically, the authors formally show how to determine the sampling overhead to compensate for noise in quantum optimization algorithms. In this particular context, the overhead turns out to be only a fraction of the computational overhead we get from error mitigation methods used to obtain unbiased estimators of expectation values.

In other words, if you have a quantum circuit that you know with reasonable probability will return a good solution to your optimization problem, you can now quantify the additional number of samples you need to draw from that circuit to counteract the effects of noise. This is a powerful insight that is essentially telling you both how to quantify the effect of the noise in your circuit, and what you must do to compensate for it.

Building on this, the authors show that a function called the Conditional Value at Risk (CVarR) can give us provable bounds on the noise-free expectation values—again with significantly less overhead than the error mitigation methods for expectation values.

What is CVaR, exactly? CVaR, or expected shortfall, is an important function used in finance that gives information about the tail of a distribution. In finance, it tells an investor the average amount of money they can expect to lose when the market turns south. In the context of quantum optimization, because we know how much more often we need to sample to get solutions that are at least as good as the noise-free case, we can also use it to derive lower and upper bounds for the expectation value of interest—i.e., we can potentially use it to identify the minimum value that a solution to our optimization problem can achieve.

Where other more common error mitigation methods like probabilistic error cancellation (PEC) and zero noise extrapolation (ZNE) are computationally expensive and provide exact expectation values, CVaR is computationally cheap and provides boundaries on expectation values, rather than an exact output. The result is noise-free information concerning the outputs of a quantum computer—information that we can use in our quantum optimization algorithms.

CVaR was previously proposed in 2019 as a robust loss function to train parametrized circuits and is still very popular today. However, back then its usage was motivated solely by intuition. These new results close the gap in our theoretical understanding of the CVaR as a loss function and demonstrate its error mitigating capabilities for training parameterized circuits.

Optimizing as a community

Theoretical results like those seen in the recent CVaR paper show potential directions to scale quantum optimization methods on noisy hardware. They also highlight how important it is that we begin combining theory work with empirical research to explore the potential of theoretical proposals in practice.

In classical computing, there are many examples of algorithms that are shown to work well empirically long before they are fully understood from a theoretical perspective. Things are different in quantum computing, where the limited capabilities and availability of quantum hardware have historically meant that quantum algorithms are primarily developed theoretically before they are tested empirically.

However, these limitations are becoming less and less relevant every day. Now that the quantum community has access to gate-based quantum devices with hundreds of qubits that are capable of running circuits beyond exact classical simulation methods, we must begin doing more work that combines theoretical and empirical research. This also highlights the importance of systematic benchmarking to understand the path towards quantum advantage in optimization.

27. D-Wave Launches "Quantum Realized" Brand Campaign to Illustrate Benefits of Today's Quantum Computing

by Alex Daigle

https://ir.dwavesys.com/news/news-details/2025/D-Wave-Launches-Quantum-Realized-Brand-Campaign-to-Illustrate-Benefits-of-Todays-Quantum-Computing/default.aspx?utm_source=substack&utm_medium=email

D-Wave Quantum Inc., a leader in quantum computing systems, software and services, and the world's first commercial supplier of quantum computers, today launched a new integrated brand campaign, "Quantum Realized," to showcase the benefits of today's quantum computing.

The new campaign launched with an open letter from D-Wave CEO Dr. Alan Baratz published in *The Wall Street Journal* about the status of quantum computing's commercial viability. Dr. Baratz's letter presents the "Quantum Realized" framework, which includes three benchmarks to evaluate a quantum company's value:

1. The company provides quantum technology that is better or faster at solving computationally complex problems than a classical computer alone.
2. Its quantum systems are highly performant, highly reliable, and highly available.
3. It has proven commercial customer successes in proof-of-concepts and in-production application deployment.

D-Wave is currently the only company that meets all the above criteria. To read Dr. Baratz's letter and learn more about realizing the value of quantum computing today with D-Wave, visit: dwavequantum.com/quantum-realized.

"'Quantum Realized' is D-Wave's most significant brand initiative to date, marking an important moment for the Company as we embark on the next phase of our commercial and technical initiatives," said Dr. Baratz. "We believe that D-Wave is the first company capable of delivering on the value of quantum computing today, with a cash balance of $320M, multiple 5,000+ qubit systems solving real customer problems now, an unparalleled 99.9% quantum cloud service up-time, and the ability to address important problems that will never be solved on a CPU or GPU. This is quantum realized."

The Quantum Realized brand campaign will span digital and print advertising channels, and events, including D-Wave's annual user conference, Qubits 2025, and the Company's sponsorship of the International Year of Quantum Science and Technology, an initiative that aims to raise public awareness about quantum computing.

28. Quantum Computing Is A Long-Term Cybersecurity Risk, But Deserves Immediate Attention, Analysts Report

by Matt Swayne
https://thequantuminsider.com/2025/02/01/quantum-computing-is-a-long-term-cybersecurity-risk-but-deserves-immediate-attention-analysts-report/

Quantum computers will not be capable of breaking high-security encryption for decades, according to a new MITRE report. But the study warns that the U.S. government and intelligence agencies must act now to safeguard sensitive data from adversaries banking on quantum breakthroughs.

The report, aimed mainly at the Intelligence Community (IC) and written by MITRE researchers Yaakov Weinstein and Brandon Rodenburg, assesses the state of quantum computing and its implications for national security. The primary concern is that once a sufficiently powerful quantum computer exists, it could render today's encryption obsolete. The researchers predict that an RSA-2048 encryption key – currently used to secure classified information – will remain safe for at least the next few decades. They are saying this timeline should hold unless there are unexpected advances in quantum computing.

While the study suggests quantum threats are not immediate, it stresses that adversaries, particularly China, are already planning for a future where quantum decryption is feasible.

"While U.S. industry currently leads the way in quantum computing, other nations, especially China, are not far behind," the analysts write.

They add that China has made significant progress in related fields, such as quantum communication and cryptographic key distribution.

The report warns that China's leadership in these areas could provide an advantage in quantum computing, potentially widening a military and technological gap that the U.S. might struggle to close. Even if China does not develop a quantum computer before the U.S., it could still decrypt sensitive intelligence it has harvested once the technology is available.

MEASURING QUANTUM PROGRESS

MITRE's study evaluates quantum computing progress using quantum volume (QV), a metric developed by IBM that considers both the number of qubits and their ability to perform computational tasks without errors. Although other experts would suggest that QV is not the only, or even the best, way to measure quantum progress.

With that limitation in mind, based on historical QV trends, MITRE estimates that a quantum computer capable of breaking RSA-2048 encryption is unlikely to emerge before 2055-2060.

However, the report notes that some experts believe this timeline is too conservative. Optimistic projections suggest that recent advances in quantum error correction and algorithm design could accelerate development, potentially bringing quantum decryption capabilities by 2035.

Quantum error correction can suppress, though not eliminate, errors during computation, the MITRE report states, adding that protecting against these errors is essential to making quantum computers practical for real-world applications.

BEYOND CYBERSECURITY: THE BROADER QUANTUM IMPACT

While much of the focus is on the security threat, the report also highlights potential benefits of quantum computing. These include breakthroughs in materials science, pharmaceuticals and artificial intelligence. Quantum computers could solve optimization problems far faster than today's best supercomputers, making them valuable for logistics, supply chain management, and defense applications.

Machine learning, another area of national security interest, could also be transformed by quantum computing. MITRE researchers suggest that quantum algorithms might enable AI systems to learn from smaller datasets, leading to faster and more accurate decision-making.

THE URGENCY OF POST-QUANTUM CRYPTOGRAPHY

Even though large-scale quantum computers are decades away, MITRE emphasizes that U.S. agencies must start transitioning to post-quantum cryptography (PQC) now. The report echoes recent moves by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA), both of which are developing new cryptographic standards resistant to quantum attacks.

"The IC has an important role to play in protection from and the utility of quantum computers," the research team writes. "The IC must protect its classified data from the threat of a quantum computer, and it should monitor the state of quantum computers to prepare for future threats and capabilities and determine use cases for a future quantum computer. By acting decisively and quickly, the IC will demonstrate the seriousness of the quantum computing threat."

The analysts add that adversaries are already stockpiling encrypted communications in hopes of decoding them later. This "harvest now, decrypt later" strategy could lead to major security breaches in the future if agencies delay transitioning to quantum-safe encryption.

A CALL FOR STRATEGIC INVESTMENT

MITRE's findings reinforce the need for sustained investment in quantum research, not just for security but also for technological leadership. The study notes that U.S. industry leads in quantum computing today, but warns that dominance is not guaranteed. It calls for careful monitoring of global developments and a coordinated national strategy to ensure the U.S. remains at the forefront of quantum technology.

Additionally, the report raises concerns about the quantum supply chain, noting that adversaries could attempt to weaken the U.S. access to critical quantum components such as cryocoolers and lasers. MITRE recommends proactive efforts to secure domestic supply chains and prevent foreign dependence on key quantum materials.

WHAT'S NEXT?

The study concludes that while quantum computers capable of breaking encryption are not imminent, the intelligence community cannot afford to wait. The MITRE researchers recommend decisive and swift action to take on this quantum computer threat.

To mitigate risks, specifically, the report recommends immediate action in three key areas:

- **Accelerating the transition to post-quantum cryptography** to safeguard sensitive information before quantum computers arrive.
- **Enhancing monitoring of adversarial quantum programs** to ensure the U.S. is not caught off guard by an unexpected breakthrough.
- **Investing in quantum research and supply chain security** to maintain U.S. leadership and avoid reliance on foreign components.

MITRE is a not-for-profit company that operates federally funded research and development centers (FFRDCs) and engages in public-private partnerships to address national security, infrastructure and

technological challenges. The organization collaborates with government agencies and industry to enhance safety, stability, and operational effectiveness across critical sectors. Its research supports policy development, emerging technology integration, and risk mitigation strategies to strengthen national resilience.