Crypto News

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

April 02, 2025

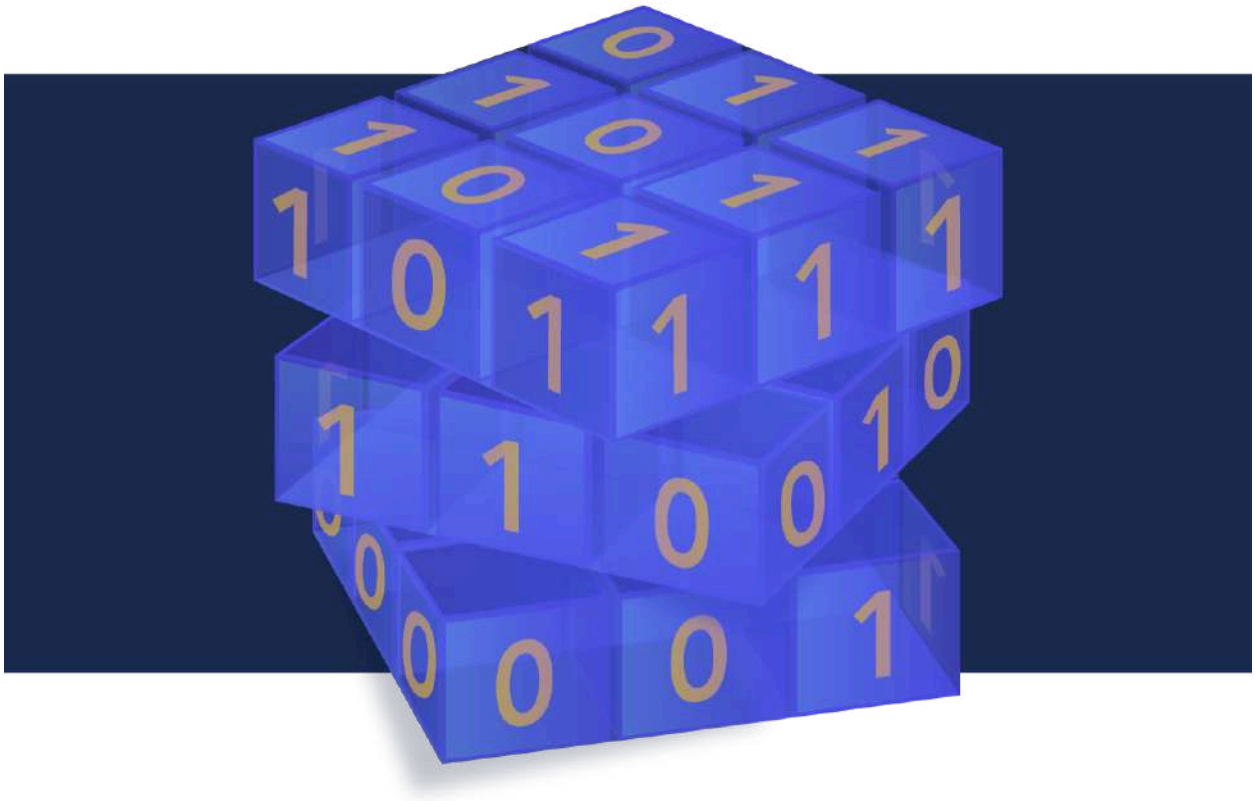


Table of Contents

Editorial

Dear Crypto readers,

It is amazing that there is so much new stuff worth reading every month… This April is not any different. You can pick great articles on a broad range of topics, from very practical to more forward looking. My difficult job is to try and ease this choice for those of you, who do not have enough time to read them all. So, with all the necessary caveats (personal choice only, does not mean that the others are not interesting…), let's give you my views.

Since time is of the essence, I would start with the short paper from NCSC (the British counterpart of NSA) in **7**, which provides a timeline for migration, with the full executive summary and the link to the whole article. Key takeaway: migration has to be completed by 2025. No time to lose! This goes hand-in-hand with **5**, which explains that quantum applications will arrive in five years. And if, by extraordinary you have not seen the blog on the CSA website yet, make sure that you read **9** from our member, Cory, who explains how and when you need to switch the post-quantum.

If you want to make some order in the hype surrounding quantum, I have to admit that **16** is my favorite. You will get a hint at the difference between marketing and true facts… And I suggest you add **23**, to see a complete list of quantum computers manufacturers and an estimate of how many computers they have sold (not so many yet).

With the recent turmoil in international relations (!) a bit of geopolitics is a must. So have a look at **13**, about the Chinese space achievement and their goal to build an operational QKD satellite constellation, and at **14** and **25**, to see what India has in mind.

If you have missed the NIST announcement on the selection of a back-up to their ML-KEM, check **17**. There you can also find an interesting link about the implementation of the new algorithms.

Finally, although I personally fully disagree with its conclusions, **2** provides a contrarian view on the need for PQC, which could be interesting to discuss in one of our next QSS working group calls. So, look for the dates there: Quantum-safe Security Working Group | CSA and join us.

Have a good reading, and a quantum-safe month!

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

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

1. How quantum cybersecurity changes the way you protect data

by Michael Nadeau
https://www.techtarget.com/searchcio/tip/How-quantum-cybersecurity-changes-the-way-you-protect-data

Quantum computing is becoming real and will soon be able to solve problems well beyond the capabilities of today's fastest supercomputers. In the wrong hands, however, quantum computers will also create a new pain level for cybersecurity professionals.

Recent advancements suggest that a cryptographically relevant quantum computer (CRQC) -- one that can break commonly used encryption algorithms -- is getting closer to reality. In February 2025, for example, Microsoft announced its Majorana 1, which it claims is the first quantum processor to use more stable topological quantum bits (qubits), the basic units of quantum information. Microsoft believes its quantum processor can eventually scale to 1 million qubits on a single chip.

Majorana 1 is a long way from meeting its potential, but its announcement should be a warning to organizations that have yet to take post-quantum cryptography (PQC) seriously. Quantum computers will render current encryption algorithms obsolete and help sophisticated adversaries find new ways to compromise critical systems. Preparing for that inevitability starts with adopting PQC algorithms.

Why quantum cybersecurity is important

The biggest quantum computing cybersecurity risk is the ability to quickly crack popular public key cryptography and encryption algorithms such as Rivest-Shamir-Adleman (RSA), Diffie-Hellman and the Advanced Encryption Standard (AES). Nation-states are the only adversaries with the resources to create a quantum system for this purpose, and it's believed they are collecting sensitive encrypted data for when that time comes. This is referred to as "harvest now, decrypt later."

"Our adversaries are consuming everything possible on encrypted networks," said John Prisco, CEO of consultancy Safe Quantum. "We know that once there is a CRQC, every secret message using RSA-2048 or RSA-4096 will be decrypted. Nothing encrypted in this way will remain a secret in the near future."

Decrypting previously stolen data isn't the only threat a CRQC poses. With a CRQC, "all digital communications that we use today leveraging asymmetric cryptography will also be broken," said Ray Harishankar, IBM Fellow and lead for IBM Quantum Safe. "Bad actors can perform fraudulent authentication and masquerade as anyone, and consequently, a number of bad things can happen. It's not as cut and dry as Y2K, when things happen [at a specific time]. It will happen gradually when powerful quantum computers become available, and nation actors have access to them."

Organizations that should be most concerned are financial services, government agencies, academic and research institutions with sensitive intellectual property, and medical services and research. "We shouldn't make it any easier for the Chinese to steal our intellectual property," Prisco said. "Medical science is also at risk. Patient data remains relevant for a human lifetime. We need a lifelong security program to protect personal medical info."

Post-quantum cybersecurity should concern all executive management and not just the CISO. "Anyone who has data that has value over five, seven, 10 years -- patent information, drug discovery information, formulae information -- those have [the] potential for being exfiltrated and causing damage," he said. "People who manage that data, chief data officers, are going to be concerned. It is broader than a CISO problem because it is a CIO problem. It is a chief risk officer problem. It is a CEO problem. It is even a board problem because all they need is damage [from one incident] and your brand reputation is at risk."

How quantum computing is changing encryption

Today's encryption schemes, such as RSA, are "secure" not because they can't be broken but because of the time and processing power needed to break them. "Public key cryptography coupled with RSA encryption could be broken by computers of today, including supercomputers, in about 1,000 years," Prisco said. "A CRQC can do it in an hour or less."

To counter the threat, researchers have developed numerous PQC algorithms. Examples include Rainbow and Supersingular Isogeny Key Encapsulation (SIKE), both of which were approved by NIST but have since been broken.

"That should worry the U.S. quantum strategists who are taking an all-their-eggs-in-one-basket approach. Defense-in-depth is necessary to compete with today's security protection schemes," Prisco said.

Why organizations should prepare for quantum computing threats now

Potential threats from quantum computers have been known since at least 1994, when Peter Shor developed Shor's algorithm for prime factorization, which is considered capable of breaking today's encryption when used with a CRQC. Quantum computers are proliferating, even if none are powerful enough to crack standard encryption algorithms. IBM has deployed 75-plus quantum computers, with more than a dozen utility-scale systems currently online that users can experiment with using the cloud, according to Harishankar.

The key question is: When will a cryptographically relevant quantum computer arrive? That's difficult to answer because much of the research is secretive. It is estimated that a quantum computer would require anywhere from several thousand to tens of millions of qubits to execute Shor's algorithm.

"We started with five qubits in 2016, and now we are at 156-plus qubits," Harishankar said. "We are able to get more and more reliable qubits as well. We have stated that by 2029 or 2030, we will have a

fault-tolerant quantum computer with 200 logical qubits." IBM has made public its own quantum development roadmap through 2033.

That might not be enough to have a CRQC, though. Harishankar's best estimate is that it will happen sometime in the mid-2030s. If you think that gives you plenty of time to prepare, think again. "History tells us that changing cryptography at scale doesn't happen in seven to 10 years. It takes more time," he said. "Unless people start thinking and planning today, they cannot complete the work in seven to 10 years."

How organizations can prepare for quantum cybersecurity

The most important way organizations can prepare for PQC is to begin the transition to quantum-secure algorithms and keys. It's a long process that includes the following steps:

- **Select a PQC algorithm.** NIST has three PQC algorithms ready for use and is finalizing the draft standards for two others. Organizations should choose a primary algorithm for general encryption -- such as Federal Information Processing Standard (FIPS) 203 -- and one for digital signatures. NIST has designated some algorithms as backups in case the primary algorithms become vulnerable.

- **Assess the PQC algorithm's effect on IT infrastructure.** A PQC algorithm will have bigger key sizes and produce increasingly fragmented network traffic, which increases performance overhead and implementation complexity.

- **Adapt network security devices.** The additional complexity and performance requirements will place more demands on firewalls and network intrusion detection systems, which will need to handle a higher volume of fragmented traffic due to larger cryptographic keys and ciphertexts.

- **Review hosting and other cloud-based services and software to ensure they are quantum-ready.** Even if you do all you can to make your own network quantum-secure, you probably have processes and data running in the cloud. If they aren't quantum-secure, you're still vulnerable to PQC attacks. Zoom, Apple and Microsoft are among the providers who say their cloud offerings are "quantum-safe."

- **Take a crypto-agile approach.** Crypto-agility enables you to switch to another algorithm without much business disruption if your post-quantum encryption algorithm is compromised. "As we transform and remediate the current software to support post-quantum cryptography, we have to do it with crypto-agility in mind so that you're not caught in this trap of having to do major work in replacing them again and again and again," Harishankar said. "I know it's a little bit of extra work now, but it's going to save you immensely downstream."

What is the future of quantum cybersecurity?

The post-quantum cybersecurity world will certainly be more complex, but one constant will remain: the constant cat-and-mouse games between cyber adversaries and defenders.

"I see quantum-resistant algorithms as failing over time," Prisco said. "No one knows if the Chinese have already broken the CRYSTALS lattice algorithms of NIST. Let's have a defense-in-depth approach that uses quantum science in addition to mathematical algorithms. It would be astounding if the NIST program provided security for 50 years like the Turing Laureates, Whit[field] Diffie and Mart[in] Hellman, did. I don't think that is a good bet."

2. Beyond encryption: Why quantum computing might be more of a science boom than a cybersecurity bust

by Rob T Lee
https://venturebeat.com/security/beyond-encryption-why-quantum-computing-might-be-more-of-a-science-boom-than-a-cybersecurity-bust/

Last August, the National Institute of Standards and Technology (NIST) released the first three "post-quantum encryption standards" designed to withstand an attack from a quantum computer. For years, cryptography experts have worried that the advent of quantum computing could spell doom for traditional encryption methods. With the technology now firmly on the horizon, the new NIST standards represent the first meaningful step toward post-quantum protections.

But is quantum computing the threat to encryption it's been made out to be? While it's true that quantum computers will be able to break traditional encryption more quickly and easily, we're still a long way from the "No More Secrets" decryption box imagined in the 1992 movie *Sneakers*. With energy demands and computing power still limiting factors, those with access to quantum computers are likely considering putting the technology to better use elsewhere – such as science, pharmaceuticals and healthcare.
Remember the electron microscope theory?

I've spent a long time working in digital forensics, and it's given me a unique perspective on the challenges of quantum computing. In 1996, Peter Gutman published a white paper, "Secure Deletion of Data from Magnetic and Solid-State Memory", which theorized that deleted data could be recovered from a hard drive using an electron microscope. Was this possible? Maybe – but ultimately, the process would be incredibly laborious, resource-intensive and unreliable. More importantly, it wasn't long before hard drives were storing information in such a densely-packed manner that even an electron microscope had no hope of recovering deleted data.

In fact, there is almost no evidence that such an electron microscope was ever successfully used for that purpose, and modern testing confirms that the method is neither practical nor reliable. But the fear was real – and it led to the U.S. Department of Defense (DOD) issuing its famous "7-pass wipe" method of data erasure to eliminate any forensic evidence that an electric microscope could theoretically detect. Should we take such extra precautions with sensitive or classified data? Of course. But the threat was nowhere near as dire as it was made out to be. When it comes to quantum computing, we may be heading down a similar road.

The practical reality of quantum computing

First, it's important to understand how quantum computing works. Despite the way movies like to portray hackers, it isn't a magic wand that will instantly end cryptography as we know it. It will still need to be fed individual messages and tasked with breaking encryption – which means attackers will need to have a pretty good idea of which messages contain valuable information. That might sound easy, but more than 300 billion emails are sent each day, along with trillions of texts. There are ways to narrow the scope of the search, but it still requires the attacker to throw an awful lot of computing power at the problem.

That leads me to the real issue: Computing power is not infinite. Quantum computing is at the cutting edge of technology, which means your average script kiddie or hacker collective isn't going to be able to get their hands on it. The only players who will have access to quantum computers (and the energy needed to run them) will be nation-state actors and large corporations like Google, Microsoft and AI companies. To put it simply, quantum computing is initially going to be expensive and not as fast to market as many have opined – and that means nation-states will only have so much computing power at their disposal. The question, then, is this: Is breaking down encryption protocols really what they plan to spend it on?

The true use cases for quantum

The answer is a strong…maybe. To me, the real advantages in quantum rests in research, economic competition and global influence. That doesn't mean quantum computers won't be put to use cracking encryption if a hostile nation-state gets its hands on something they know is good – but it won't be the primary way the technology is used. Look at it this way: If you're a foreign power with access to the most advanced computer models on earth, what would you use them for? Would you go on a wild goose chase through millions of encrypted communications, or would you devote that critical time, energy and compute to cure cancer, eradicate dementia or create advanced new materials? To me, that's a no-brainer. An individual attacker might be after short-term gains, but nations will think more long-term.

Quantum computing is likely to drive significant breakthroughs in the development of new materials and catalysts, leading to the creation of stronger, lighter composites for manufacturing and more reactive catalysts for chemical processes. That alone has the potential to revolutionize multiple industries, providing far greater long-term gain for the nation deploying the technology. Quantum computing has also shown promise in the pharmaceutical industry, helping researchers develop more effective drugs and other treatments in a fraction of the time. The technology is even being used to enhance space travel capabilities by enabling faster trajectory calculations, making navigation more accurate and optimizing fuel usage.

It comes down to a cost-benefit analysis. Only nation-states and large corporations will have access to quantum computing anytime soon – and will they really spend their limited computing power cracking encryption algorithms when they could instead be boosting their economic output and dominating financial markets? This isn't to say that every use case for quantum computing is good – in the wrong hands, it could certainly be used in dangerous ways. But with so much focus on the so-called "quantum apocalypse" some believe is looming, context matters.

Is breaking encryption on the list of use cases for quantum computing? Yes. But it's not high on the list. So before we spend billions of dollars to rip and replace every cryptographic algorithm in use, it might be time to take a deep breath and consider how quantum computing will actually be used.

3. Certified randomness using a trapped-ion quantum processor

https://thequantumfacts.com/certified-randomness-using-a-trapped-ion-quantum-processor/

A groundbreaking study published in *Nature* has demonstrated a significant leap forward in quantum computing applications. Researchers from JPMorganChase, Quantinuum, Argonne National Laboratory, Oak Ridge National Laboratory, and The University of Texas at Austin have successfully implemented "certified randomness" – a process generating truly random numbers that can be mathematically proven to be genuine.

The team utilized Quantinuum's 56-qubit H2-1 trapped-ion quantum computer to generate random bits through a protocol developed by Scott Aaronson, a computer science professor at UT Austin. This protocol leverages Random Circuit Sampling (RCS) to produce randomness that classical computers simply cannot replicate.

Classical computers cannot generate true randomness on their own, typically relying on hardware random-number generators that could potentially be compromised. The new quantum approach ensures randomness even if an adversary had commandeered the quantum computer, making it theoretically impossible to manipulate the output while maintaining certification.

The process works in two steps: first, the quantum computer is given challenges it can only solve by selecting one of many possible solutions at random – tasks beyond the capabilities of even the most powerful classical supercomputers. Second, this randomness is mathematically certified as genuine using classical supercomputers with a combined performance of 1.1 ExaFLOPS. Through this method, researchers certified 71,313 bits of entropy.

As Marco Pistoia, Head of Global Technology Applied Research at JPMorganChase noted, "*This development of certified randomness not only shows advancements in quantum hardware but will be vital to further research, statistical sampling, numerical simulations, and cryptography.*"

The breakthrough was enabled by Quantinuum's recent upgrade to its System Model H2 quantum computer, which improved on existing industry standards by a factor of 100 thanks to high fidelity and all-to-all qubit connectivity.

This achievement represents a significant shift from theoretical quantum advantage to practical application, demonstrating that today's quantum computers can perform useful tasks beyond the capabilities of classical computing. The certified randomness protocol has important implications for cryptography, security, fairness in processes like jury selection, lotteries, and e-games where multiple parties need verification that random numbers were freshly generated.

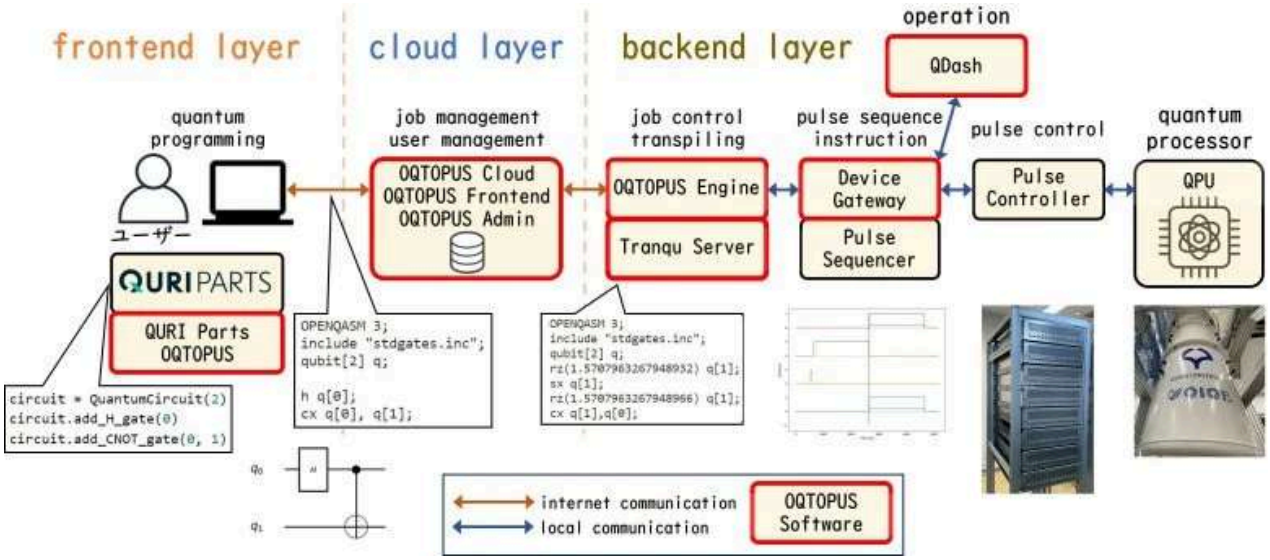
4. Scientists Launch Open-Source Quantum Computer OS

by Osaka University
https://scitechdaily.com/scientists-launch-open-source-quantum-computer-os/

The University of Osaka, Fujitsu Limited, Systems Engineering Consultants Co., Ltd. (SEC), and TIS Inc. (TIS) have announced the release of an open-source operating system for quantum computers on GitHub. Named the Open Quantum Toolchain for Operators and Users (OQTOPUS), this system represents one of the world's most comprehensive open-source efforts in the field of *quantum computing*.

OQTOPUS is designed to be flexible and customizable, allowing users to tailor the system to their specific needs. Its release is expected to accelerate the practical deployment of quantum computing by significantly reducing the complexity of setting up and operating quantum systems, particularly in cloud environments.

Previously, universities and companies had to develop extensive custom software to enable cloud-based quantum computing. With OQTOPUS, the collaborative team has streamlined this process by providing a complete, ready-to-use operating system, from setup to execution, making quantum computing more accessible than ever before.



Early Adoption and Future Plans

Additionally, the quantum computing cloud service offered by the University of Osaka has begun integrating OQTOPUS into its operations and Fujitsu Limited will make it available for research partners using its quantum computers in the second half of 2025.

Moving forward, the research team will drive the advancement of quantum computing through the continuous expansion of OQTOPUS's capabilities and the development of a thriving global community. Dr. Keisuke Fujii at the Center for Quantum Information and Quantum Biology (QIQB) of The University of Osaka mentions, "this will facilitate the standardization of various quantum software and systems while driving the creation of innovative quantum applications."

The research was funded by the Japan Science and Technology Agency and the National Institutes for Quantum Science and Technology.

5. Google Executive Says Quantum Applications Could Arrive In Five Years

by Matt Swayne
https://thequantuminsider.com/2025/03/26/google-executive-says-quantum-applications-could-arrive-in-five-years/?utm_source=resonance-newsletters.beehiiv.com&utm_medium=newsletter&utm_campaign=the-quantum-insider-weekly-commercializing-quantum-predicting-quantum-and-more-news&_bhlid=842976549a31c868dcbc057b7e98d7576dc389f1

One of Google's top quantum computing executives says practical quantum applications are just five years away.

Julian Kelly, director of hardware at Google Quantum AI, told CNBC's Deirdre Bosa that the company is approaching a milestone: a quantum computer capable of performing useful tasks that today's most powerful machines cannot.

"We think we're about five years out from a real breakout, kind of practical application that you can only solve on a quantum computer," said Kelly in an interview aired yesterday.

His comments add to a growing debate about how quickly quantum computing will become more than a scientific curiosity. The field, long viewed as experimental, is now drawing fresh attention — and scrutiny — as big tech firms invest in developing machines that operate on the rules of quantum physics rather than conventional computing logic.

Quantum computers process information using qubits, short for "quantum bits." Unlike traditional bits that are either a 0 or 1, qubits can seemingly exist in multiple probabilistic states, thanks to the principles of quantum mechanics. This gives them the potential to handle extremely complex problems, such as simulating chemical reactions or optimizing massive systems, tasks classical computers struggle to perform efficiently.

"Quantum computers speak quantum mechanics — they can access the way the universe works at the most fundamental level," Kelly told CNBC.

BIG TECH = BIG QUANTUM

Google has previously demonstrated progress in quantum computing, including a 2019 claim of "quantum supremacy" — where a quantum machine completed a task faster than the best classical supercomputers. More recently, the company made headlines with an advance in quantum error correction, a critical step toward building reliable quantum systems. That advance was announced in December, as reported by CNBC.

Meanwhile, Microsoft has taken a different path. In February, the company introduced a quantum chip based on a particle called a Majorana, which it said required creating an "entirely new state of matter." That work is still being challenged by the scientific community.

Still, even the most advanced machines remain far from the capabilities needed to deliver widespread practical value. Google's current top system runs with 105 qubits. Experts estimate that a quantum computer will need over a million error-corrected qubits to tackle the kinds of problems that would have commercial or scientific value beyond what today's supercomputers can do.

NEAR-TERM APPLICATIONS

Kelly acknowledged that gap, but said the earliest uses of quantum computing could arrive before reaching that scale. He pointed to potential near-term applications in simulating advanced physics.

"The first applications are likely to be in areas where you've got some system that's sort of just out of reach of what a classical computer [can] do," he said to CNBC.

One speculative application, Kelly said, involves using quantum machines to generate novel data that could help train artificial intelligence models. While he was cautious about overselling that idea, he said the intersection between AI and quantum computing is a subject of interest.

"One of the potential applications that you can think of for a quantum computer is generating new and novel data," Kelly said.

However, he clarified that today's AI systems won't simply be ported to run on quantum computers, noting that the underlying models are fundamentally incompatible with the architecture of quantum machines.

Quantum computing's perceived potential has helped propel investment, particularly as tech leaders and investors look for the next breakthrough in hardware after the boom in AI processors. Graphics processing units, or GPUs, made by Nvidia have powered the recent wave of AI development, and attention has begun to turn toward whether quantum chips could drive a similar revolution.

Though Nvidia doesn't make quantum chips, it held a "Quantum Day" event last week. The summit featured representatives from Amazon, Microsoft, and a dozen quantum companies discussing the promise of the technology. According to CNBC, the event was seen by some as a signal that Nvidia is taking a more active role in the quantum space, even if only as an ecosystem enabler.

The meeting also followed public remarks by Nvidia CEO Jensen Huang, who in January had downplayed the near-term prospects of quantum computers. His comments, as reported by CNBC, triggered a dip in the share prices of several publicly traded quantum companies.

But last week, Huang softened his stance.

"Of course, quantum computing has the potential and all of our hopes that it will deliver extraordinary impact," Huang said. "But the technology is insanely complicated."

He added that his earlier comments were "wrong," though he still maintained that many engineering hurdles remain before quantum computing becomes mainstream.

TIMELINE DIVIDE

Industry observers remain divided on the timeline. Some see the recent advances by Google and Microsoft as signs that quantum computing is slowly but steadily progressing toward real-world utility. Others say predictions of a five-year breakthrough have been made before – and missed.

What is clear is that interest is rising. Venture capital investment in quantum startups is growing, and governments are increasing funding to compete in what many see as a strategic race. China, the U.S., and the European Union have all launched national quantum initiatives in recent years.

For now, companies like Google are focused on scaling up their machines and improving their reliability through better error correction and system integration. According to CNBC, Kelly remains confident that the hardware and software are evolving quickly enough to deliver something useful within the decade.

What that "something" is, and whether it's truly beyond the reach of classical computers, remains to be seen.

6. ETSI launches first post-quantum encryption standard

by Alex Scroxton
https://www.computerweekly.com/news/366621214/ETSI-launches-first-post-quantum-encryption-standard

The European Telecommunications Standards Institute (ETSI) has this week debuted its first post-quantum cyber security standard, designed to guarantee the protection of critical data and communications in the quantum-enabled future.

Responding to the potentially existential threat to current encryption methods posed by large-scale quantum computers – which will likely be able to efficiently solve the complex maths relied on by current asymmetric public key cryptography (PKC) – ETSI has developed specification TS 104 105 – or, to give it its full name, *Efficient quantum-safe hybrid key exchanges with hidden access policies* – to help ensure that only authorised users are able to access sensitive data.

The standard defines a scheme for Key Encapsulation Mechanisms (KEMs) with Access Control (Kemac) – dubbed Covercrypt – that ETSI claims will ensure pre- and post-quantum security through hybridisation.

In layman's terms, it will lock and anonymise session keys based on user attributes, and enable those who meet the encapsulation policy requirements to retrieve them while keeping those who don't away.

ETSI said its standard also heralded a breakthrough in efficiency – it takes a few hundred microseconds to encapsulate and decapsulate said keys. It can supposedly be easily and readily integrated into existing security products, the body added.

"ETSI's latest specification marks a significant milestone in the transition to post-quantum cryptography," said Matt Campagna, chair of the Quantum Safe Cryptography (QSC) working group at ETSI. "This standard is fundamental to the quantum future, we are empowering organisations to safeguard their sensitive data both for today, and for the decades ahead.

"The work we've done in the Cyber QSC working group underlines our commitment to providing secure, future-proof solutions that can withstand emerging threats, while also helping to build a healthy industrial ecosystem and a sustainable economy," he said.

ETSI said organisations should begin to use quantum-resistant encryption as soon as possible to future-proof their data security, safeguard their most sensitive data and remain compliant with yet-to-emerge standards.

The launch of the standard comes in the wake of guidance issued by the UK's National Cyber Security Centre, which similarly urged organisations to begin exploring their migration pathways to post-quantum cryptography (PQC).

The NCSC's advice – which can be accessed in full here – sets out a three-phase schedule that will help key industries move to quantum-resistant encryption over the next decade.

The agency said that at-risk organisations – such as financial institutions, healthcare providers, operators of critical national infrastructure and public sector organisations – should have the core of a migration plan in place by 2028, before beginning high-priority upgrades and then moving on to a complete PQC migration by 2035.

The NCSC said much of this work involved the sort of activity that would accompany any large-scale IT migration, and in security terms, activity that should already be at the heart of any business' security practice – so those that are sufficiently on the ball should think about using PQC migration as an opportunity to build additional resilience into their IT systems.

The agency also noted that the ultimate cost of PQC migration could be significant, so it is essential that organisations begin to budget accordingly.

7. Timelines for migration to post-quantum cryptography

by NCSC
https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

Executive summary

The national migration to post-quantum cryptography (PQC), mitigating the threat from future quantum computers, is a mass technology change that will take a number of years.

The NCSC recognises the need both to offer guidance on some of the early-stage migration activities, and to set some indicative timelines that UK industry, government and regulators can follow. In this guidance, the NCSC sets out some key target dates for migration activities.

Although the core timelines are relevant to all organisations, this guidance is *primarily* aimed at technical decision-makers and risk owners of large organisations, operators of critical national infrastructure systems including industrial control systems, and companies that have bespoke IT. Different sectors will have different current states of cryptographic maturity, and so the weight of activities might vary across the three periods, but a focus on those headline dates is important for investment decisions and broader cyber security planning.

The key milestones are:

By 2028

- Define your migration goals
- Carry out a full discovery exercise (assessing your estate to understand which services and infrastructure that depend on cryptography need to be upgraded to PQC)
- Build an initial plan for migration

By 2031

- Carry out your early, highest-priority PQC migration activities
- Refine your plan so that you have a thorough roadmap for completing migration

By 2035

- Complete migration to PQC of all your systems, services and products

There will be a small set of more rarely used technologies for which migration by 2035 may be more difficult. This may impact some sectors more than others, but all organisations should work towards these key dates.

8. Quantum Computers And Their Impact On Data Security

https://evrimagaci.org/tpg/quantum-computers-and-their-impact-on-data-security-275655#google_vignette

The rise of quantum computing technology threatens current encryption methods, urging companies to prepare for compliance and security risks.

Quantum computers are changing the landscape of IT security, posing significant threats to established encryption methods. As the potential for powerful quantum machines looms, the risks for companies increase, with many facing compliance violations and data protection issues if they do not act swiftly. The ability of quantum computers to break asymmetric encryption methods, which are central to secure communication, is one of the biggest threats. Algorithms such as RSA and ECC, which rely on complex mathematical problems, could fall victim to quantum power.

Already, state actors and cybercriminals are collecting encrypted data, preparing to decrypt it in the future with quantum capabilities. Therefore, businesses should begin considering quantum-safe alternatives now. Ignoring the growing threat of quantum computing carries serious legal ramifications. Companies must ensure their IT systems meet legal requirements, particularly regarding GDPR compliance. Failing to protect personal data with up-to-date encryption could be seen as a violation of GDPR regulations. This oversight could not only lead to regulatory fines but also expose companies to contractual liabilities when it comes to confidentiality agreements. A data breach resulting from quantum attacks could result in significant damage, including potential lawsuits.

Moreover, companies engaged in transferring personal data outside the EU must consider this new threat. If they rely on standard contractual clauses for data transfers, they need to evaluate the risks posed by quantum computers. The recommendations made by the German Federal Office for Information Security (BSI) are crucial here. In August 2024, the U.S. National Institute of Standards and Technology (NIST) released three quantum-safe encryption standards, intended to replace existing methods and allow for secure communication in the era of quantum computing. The BSI has echoed this message, urging firms to start transitioning to quantum-safe solutions by 2030.

To maintain compliance and protect sensitive data, companies are encouraged to take several proactive measures. First, they should conduct risk assessments to identify which IT systems and data could be vulnerable to quantum attacks. This assessment involves examining existing regulatory requirements and

industry-specific security standards. Companies also need a clear migration strategy that outlines how they will implement quantum-safe encryption methods.

Collaboration with cloud providers and IT service partners is essential for the successful integration of these advanced technologies. Organizations that act swiftly to implement quantum-safe measures will not only protect their data but also mitigate the risk of regulatory sanctions and liability lawsuits, especially for businesses handling long-term data.

The implications of these changes resonate beyond just corporate infrastructure. A notable case recently highlighted in the news features a Norwegian man, Arve Hjalmar Holmen, who found himself the victim of a false murder accusation generated by ChatGPT. Holmen sought to determine what information the AI chatbot had on him, only for it to create a fabricated narrative accusing him of heinous crimes against his children. This story included critical details about Holmen's real life, such as the number and gender of his children and his hometown, blurring the lines between fact and fiction, thereby violating GDPR regulations. OpenAI faced significant backlash for this failure to provide accurate data, and a complaint was lodged with the Norwegian Data Protection Authority to avoid future incidents similar to Holmen's.

In response to the outcry, ChatGPT has been updated to search the internet for accurate information about individuals, reducing the likelihood of generating harmful misinformation. However, this raises concerns about how AI systems handle personal data and the liability of companies like OpenAI for inaccuracies.

This brings us to another significant event involving online retail giant Amazon, which faced a staggering fine in Luxembourg four years ago for breaches of European data protection law. The decision to impose a fine of 746 million euros has now culminated in a court defeat for Amazon as it seeks to challenge this ruling. This case underscores the high stakes of compliance with data privacy regulations as penalties for violations can be monumental.

The conflation of advanced technologies like AI and quantum computing introduces unique challenges in terms of compliance and the accuracy of personal data. As regulations evolve, companies in all sectors will need to adapt to these changes or risk falling behind and facing serious legal consequences. The timeline is pressing; with quantum-safe standards set to be adopted in the coming years, organizations must act decisively to ensure they remain compliant and safeguard their operations in this fast-changing digital landscape.

In conclusion, quantum computers are not a distant problem but a pressing issue impacting IT security today. Without timely action towards quantum-safe encryption, companies could jeopardize their data integrity and invite regulatory penalties. As the technology evolves, the opportunity to adapt and thrive lies with those who prepare well ahead.

9. How and when you should switch to post-quantum

by Cory Missimore
https://cloudsecurityalliance.org/blog/2025/03/20/nistir-8547-from-pqc-standards-to-real-world-implementations

NIST is helping companies and governments prepare for PQC

As quantum computing technology continues to advance, so does the urgency for organizations to rethink their approach to cybersecurity. Many of the cryptographic standards that protect sensitive information today will eventually become vulnerable to quantum-enabled attacks. Recognizing this looming challenge, the National Institute of Standards and Technology (NIST) has introduced Interagency Report (IR) 8547, which provides guidance on transitioning from classical encryption to Post-Quantum Cryptography (PQC).

This document is not just about anticipating the risks posed by quantum computing – it is a practical roadmap for ensuring organizations can integrate quantum-resistant cryptographic solutions without disruption. The transition is not a question of if, but when and how. Understanding the right timing and the key steps for implementation is crucial for organizations looking to stay ahead of potential security threats.

From Standards to Implementation: The Key Takeaways of NIST IR 8547

The primary goal of NIST IR 8547 is to provide organizations with a structured approach to transitioning to quantum-resistant cryptographic solutions. This shift requires careful planning, as organizations must first assess their cryptographic dependencies before making changes.

The first step involves identifying all systems and assets that rely on encryption, particularly on assets that require encryption, and evaluating which are most vulnerable to future quantum-based threats. This assessment allows organizations to prioritize the transition of their most critical systems—such as long-term sensitive data storage or financial transaction security—before expanding to less immediate risks.

Another significant part of the transition process is ensuring interoperability. Organizations cannot afford to simply replace their existing cryptographic standards overnight. Instead, they will likely operate in a hybrid cryptographic environment, where quantum-resistant solutions are integrated alongside classical encryption methods. This hybrid approach allows organizations to maintain security while gradually phasing out vulnerable cryptographic algorithms.

Another critical aspect of NIST IR 8547 is its emphasis on testing and validation. Before fully transitioning to quantum-resistant cryptographic methods, organizations must conduct controlled trials to ensure that performance, security, and compatibility concerns are adequately addressed. This means working closely with vendors, conducting internal assessments, and refining migration strategies based on real-world results. The adoption of PQC should not be seen as a simple software update but rather as a **long-term strategic transformation** in how organizations protect their digital assets.

When Should You Make the Transition?

One of the most pressing concerns surrounding the transition to PQC is determining the right time to act. Since large-scale quantum computers capable of breaking classical encryption do not yet exist, some organizations may be tempted to delay the transition. However, waiting too long could lead to security vulnerabilities and compliance challenges once quantum computing becomes more widespread.

In the immediate term, organizations should begin preparing by conducting a **comprehensive inventory** of their cryptographic assets. This includes identifying where cryptographic protocols are used, assessing the lifespan of protected data, and determining which systems require long-term security assurances. Sensitive information, such as national security data, financial records, and medical histories, must remain protected for decades. These are the systems that should be prioritized for transition to PQC, even before quantum computing becomes a mainstream threat.

As organizations move forward with this transition, they should also engage with technology vendors and service providers to ensure they are aligned with quantum-resistant security solutions. Many organizations rely on third-party software, cloud services, and hardware that incorporate cryptographic standards. Ensuring that vendors are actively working toward PQC compliance will help streamline the transition and minimize compatibility issues down the line.

The migration to quantum-resistant solutions will not be instantaneous. Over the next several years, organizations should begin adopting **hybrid cryptographic models**, where quantum-safe solutions are gradually introduced alongside existing methods. This allows for rigorous testing, industry-wide validation, and smoother integration. By the time quantum computing becomes a significant threat, organizations that have already implemented PQC in critical areas will be well-positioned to complete the full transition with minimal disruption.

Looking beyond 2030, the expectation is that organizations will have fully transitioned to PQC, with legacy cryptographic systems phased out entirely. However, flexibility will be key—cryptographic research is ongoing, and new developments could influence how PQC is implemented in the future. Organizations should remain adaptable and prepared to update their security strategies as advancements continue.

Real-World Considerations for Implementation

The transition to PQC is not solely a technical challenge – it is also a business and regulatory challenge. Compliance requirements across industries such as finance, healthcare, and government will likely evolve to reflect the necessity of quantum-resistant cryptographic standards. Organizations that proactively begin integrating PQC into their security frameworks will be better positioned to meet future regulatory obligations while maintaining a competitive edge in cybersecurity resilience.

Another major consideration is the impact on supply chains. Many cryptographic functions are embedded within third-party applications and services. Organizations must take a collaborative approach, working

closely with vendors and service providers to ensure a smooth transition. Some vendors may already be working on PQC solutions, while others may require additional guidance or incentives to prioritize these security upgrades. Establishing strong partnerships early on can help minimize potential roadblocks when the transition accelerates.

Cost and resource allocation are also factors that cannot be overlooked. Implementing PQC requires investment in updated infrastructure, workforce training, and testing environments. Organizations should adopt a phased approach to deployment, ensuring that resources are allocated effectively over time. By breaking down the transition into manageable steps—starting with assessment, then integration, and finally full adoption—organizations can spread out costs and avoid the financial strain of a last-minute overhaul.

Take Action Now

The shift to **Post-Quantum Cryptography (PQC)** is not a distant challenge – it is an inevitable transformation that organizations must begin preparing for today. NIST IR 8547 provides a detailed framework for navigating this transition, offering a clear strategy for assessing risks, prioritizing critical assets, and adopting quantum-resistant cryptographic solutions.

Organizations that take a proactive stance by conducting risk assessments, engaging with vendors, and gradually implementing PQC will be better equipped to handle future quantum threats. Waiting until quantum computing reaches full maturity will leave organizations vulnerable to security gaps, regulatory challenges, and costly emergency transitions.

By acting now, organizations can future-proof their security strategies, maintain regulatory compliance, and ensure that their digital assets remain protected in an era of rapidly evolving technology. Quantum computing is on the horizon – **will your organization be ready?**

10. AROBS Polska To Develop Post-Quantum Satellite Communication Security System

by Greg Bock
https://thequantuminsider.com/2025/03/19/arobs-polska-to-develop-post-quantum-satellite-communication-security-system/?utm_source=resonance-newsletters.beehiiv.com&utm_medium=newsletter&utm_campaign=the-quantum-insider-weekly-nvidia-quantum-uk-eyes-pqc-timeline-and-more-news&_bhlid=5eb0579165e038db1ab9323911ad8ed375347b70

AROBS Polska, part of the AROBS Group, the largest technology company listed on the Bucharest Stock Exchange, has been selected by the European Space Agency (ESA) to develop and implement the Post-Quantum Cryptography Algorithms for Satellite Telecommunication Applications (PQC ASTrAL) project. This project, carried out under the ESA Advanced Research in Telecommunications Systems (ARTES) Space Systems for Safety and Security (4S) program within ESA's Connectivity and Secure

Communications directorate, aims to develop a cryptographic system for satellites based on post-quantum algorithms, ensuring the protection of communications against emerging threats posed by quantum computers.

"We are delighted that AROBS Polska has been selected for another ESA project. The rapid advancements in quantum computers pose a major challenge to cybersecurity, as traditional encryption systems become vulnerable to the exceptional processing power of future quantum computers. The compromise of cryptographic keys can have serious consequences, ranging from unauthorized interception of communications to the takeover of devices. In this context, the solution developed by AROBS Polska within the PQC ASTrAL project is a necessary response to a real threat, contributing to the long-term security of satellite communications," stated Voicu Oprean, Founder and CEO of AROBS.

Quantum computer advancements raise significant cybersecurity challenges, with the potential to compromise traditional cryptographic algorithms. To counter this risk, PQC ASTrAL aims to implement a cryptographic system resistant to quantum attacks, allowing satellites to perform authentication, digital signatures, and encryption in a secure and sustainable manner over the long term.

In this project, AROBS Polska is the prime contractor responsible for developing the hardware and firmware hosting the cryptographic IP core, as well as the associated software. ResQuant, a company specializing in hardware-implemented cryptographic solutions, is the subcontractor and is responsible for the cryptographic aspects of the project.

"Securing satellite communications is a complex challenge, especially for long-duration devices with limited physical access. Updating software, cryptographic certificates, and key negotiation mechanisms are critical processes for maintaining security, yet vulnerabilities in current systems might allow attacks through forged digital signatures or compromised cryptographic keys. With the rapid advancements in quantum computers, traditional cryptographic standards no longer provide long-term security guarantees. By integrating post-quantum algorithms and implementing security mechanisms in hardware, PQC ASTrAL significantly reduces these risks by separating cryptographic processing from core systems and minimizing vulnerabilities to cyberattacks. This approach ensures a high level of security for satellite communications, anticipating the industry needs for the years to come," added Michał Szwajewski, CEO AROBS Polska.

The developed system will enable the generation and management of cryptographic keys both on satellites and at mission control stations, encryption and authentication of data, the secure authentication and verification of keys using post-quantum methods standardized in August 2024 by U.S. NIST, as well as the distribution and validation of software packages for satellites. The solution is designed to comply with international security standards and will be compatible with SpaceWire and SpaceFibre, two high-speed aerospace communication protocols that facilitate data transfer between on-board satellite systems and other spacecraft.

"European National Security Agencies are urging the transition of critical infrastructure to post-quantum cryptography. ESA is proud to partner with AROBS Polska to develop a quantum-safe cryptographic system that will protect satellite communication infrastructure from emerging threats, ensuring Europe can safely

leverage quantum computing advances and defend against related attacks," said Laurent Jaffart, ESA's Director of Connectivity and Secure Communications.

AROBS Polska, headquartered in Gdansk, specializes in developing advanced technologies for quantum and optical communications, data processing and storage, as well as satellite control mechanisms and instruments. The company has extensive experience in developing solutions for ESA and other aerospace organizations, actively contributing to innovative projects for securing space communications.

11. Oracle Unveils Java 24 with Focus on AI Integration, Post-Quantum Cryptography and Developer Experience

by TOM SMITH
https://devops.com/oracle-unveils-java-24-with-focus-on-ai-integration-post-quantum-cryptography-and-developer-experience/

Oracle announced the release of Java 24 today (19 March 2025) at JavaOne 2025, marking the 15th consecutive on-time release in the six-month cadence that has transformed the Java ecosystem since 2018. This milestone release comes as Java approaches its 30th anniversary, with Oracle emphasizing three key areas of innovation: AI integration, post-quantum cryptography and improved developer experience – especially for newcomers.

AI-Ready Platform Enhancements

Java 24 introduces several features to make the language more effective for AI workloads. Now in its ninth incubator iteration, the Vector API enables developers to express vector computations that compile to optimized CPU instructions – critical for performance-intensive AI inference tasks.

"We are ensuring that Java is a contender for AI workloads, whether you are generating your code using a generative service or integrating them into your applications," said Chad Arimura, vice president of developer relations at Oracle, during the opening keynote.

Other AI-focused improvements include primitive types in patterns and pattern-matching enhancements, which simplify the integration of business logic with primitive types from AI inference engines. Module import declarations also make incorporating AI services and libraries easier into Java applications.

Post-Quantum Cryptography Foundations

In response to future threats from quantum computing, Java 24 adds three significant security features: A Key Derivation Function API, the Quantum-Resistant Module-Lattice-Based Key Encapsulation Mechanism (ML-KEM) and the Module-Lattice-Based Digital Signature Algorithm (ML-DSA).

These implementations align with FIPS standards and establish foundational building blocks for quantum-safe applications. Donald Smith, vice president of Java product management, explained the approach: "We've been through this before with the migration from TLS 1.2 to 1.3. We will provide the implementation, ensure it's performant and ensure it's stable."

Oracle intends to backport these security features to long-term support releases as standards evolve, ensuring existing Java applications can be secured against "harvest now, decrypt later" attacks.

12. Welinq Launches Its World-Record Storage Solution for Quantum Computing Scale-Out

by Welinq
https://welinq.notion.site/Welinq-Launches-Its-World-Record-Storage-Solution-for-Quantum-Computing-Scale-Out-1b497107255580d8b2e6c53f03f61057

Welinq, a leader in quantum networking technology, has launched the first commercial quantum memory designed specifically for quantum data centers with world-record performance. Quantum computing is reaching a turning point: with more than 100 individual quantum computers deployed in dedicated infrastructures, the next challenge is networking them into scalable, high-performance architectures.

Just as classical data centers rely on distributed computing and high-speed interconnects, the future of quantum computing depends on optical networking and resource sharing between quantum processors. Welinq's quantum memory acts as the backbone of this infrastructure, making it possible to link quantum processors into powerful, scalable networks.

A Fully Integrated, Ready-to-Use Product

Welinq's new memory is a fully integrated system allowing for plug-and-play deployment in quantum data centers and quantum communication networks. Key features include:

- Over 90% on-demand storage-and-retrieval efficiency for single photons—the highest recorded for quantum memory.
- Storage durations of up to 200 microseconds.
- Compact form factor, fitting into a standard 19-inch industrial rack for easy integration.

- Room-temperature operation using a proven neutral-atom approach with technological maturity, eliminating the need for cryogenic systems thanks to the precise trapping of atoms by laser beams.

Julien Laurat, Professor at Sorbonne Université, CSO Hardware and Co-founder of Welinq, the pioneer of this technology, says: "*Quantum memories have been a central focus of research for years, but transitioning from academic demonstrations to a deployable commercial solution in just two years was a major engineering challenge*."

A Key Advancement for Scaling Quantum Technologies

Today, quantum processors operate in isolation, limiting their computing power. Welinq's quantum memory enables quantum processors to work together, forming a distributed quantum architecture—the only viable way to scale quantum computing beyond single QPUs.

- As a quantum buffer, Welinq's memory allows for entanglement distribution and qubit synchronization across processors.
- For quantum communications, it enables the creation of large-scale secure networks, forming the backbone of the emerging quantum internet.

"Welinq's quantum memory will unlock new applications and drive breakthroughs in quantum computing and communication. Its impact will be transformative across industries such as cybersecurity, energy, and healthcare.", says Eleni Diamanti, Research Director at CNRS, Lead of the Paris Center for Quantum Technologies, CSO Protocols and co-founder of Welinq.

Looking Ahead: Building Infrastructures for the Quantum Future

Several units of Welinq's quantum memory are now in production and being deployed across Europe, marking a major milestone in the industrialization of quantum technologies. Welinq is removing the barriers to building the first quantum data centers by providing all the solutions enabling the end-to-end connection between any quantum computers. The company is pioneering quantum networking hardware with efficient quantum photonics devices and storage capabilities, as well as developing high-performance light-qubit interfaces across various quantum computing technologies. This is complemented by a robust software backbone that enables network orchestration.

Earlier this year, Welinq launched the araQne quantum compiler, designed to optimize algorithm partitioning across networked quantum processors efficiently.

Beyond technological advancements, Welinq has fostered a thriving community around distributed quantum computing. The company has recently announced key partnerships with Pasqal, Quandela, and QphoX and has spearheaded AQADOC, the world's first initiative dedicated to distributed quantum algorithms developed alongside industry leaders and end-users in the energy sector.

13. China Establishes Quantum-Secure Communication Links With South Africa

by Matt Swayne
https://thequantuminsider.com/2025/03/14/china-established-quantum-secure-communication-links-with-south-africa/?utm_source=resonance-newsletters.beehiiv.com&utm_medium=newsletter&utm_campaign=the-quantum-insider-weekly-d-wave-makes-waves-nist-s-back-up-algorithm-and-more-news&_bhlid=b0d2579aedbc1ea08f41590a90b06c3ac072aef4

China has successfully extended ultra-secure quantum communication into the southern hemisphere for the first time, linking Beijing and South Africa using a quantum key distribution system, according to an article in the South China Morning Post.

The announcement means that China is advancing efforts to create an intercontinental communication network resistant to hacking, with potential applications in finance, national security, and other sensitive fields.

Yin Juan, a professor at the University of Science and Technology of China and deputy to the National People's Congress (NPC), announced the achievement at the annual plenary meeting in Beijing. The demonstration, spanning 12,800 kilometers (7,954 miles), was enabled by China's quantum communication satellites.

"It is also the first time this kind of secure quantum key distribution experiment has been implemented in the southern hemisphere," said Yin, who played a key role in developing China's first quantum communication satellite, Mozi, also known as Micius.

Another Great Link Forward

China has established multiple satellite-based quantum key distribution (QKD) links to enhance secure communications. The cornerstone of these efforts is the Quantum Experiments at Space Scale (QUESS) project, featuring the satellite known as Micius, launched in 2016. Micius has enabled several significant QKD experiments:

- **China-Austria Link (2017):** Micius facilitated a secure quantum communication channel between China and Austria, covering a ground distance of approximately 7,600 kilometers. This achievement enabled the first intercontinental secure quantum video call in 2017.
- **China-Russia Link:** China has utilized Micius and a network of ground stations to establish secure communications between China and Russia.

How Does It Work?

Quantum communication uses principles of quantum mechanics to securely transmit information. A key component is quantum key distribution (QKD), a technique that allows two parties to share encryption keys in a way that makes eavesdropping detectable. If an unauthorized party intercepts the transmission, the quantum state of the key is disturbed, alerting users to a security breach.

China is considered one of the global leaders in the development of QKD technology. The nation's scientists have been making strides in the technology since 2017, when researchers/scientists used Mozi to establish a secure "quantum call" and transmit images between China and Austria. The latest advance expands that capability and demonstrates real-time secure communication using low-cost quantum micro-nano satellites and mobile ground stations, according to Yin.

A scientific paper detailing the experiment is set to be published in the journal *Nature* in mid-March.

The advancement aligns with Beijing's broader strategy to invest in future technologies, including quantum information science. A draft economic and social development plan from China's National Development and Reform Commission highlights quantum communication as a key area of focus. The country has already established secure communication links with Russia using Mozi and aims to build similar networks among BRICS nations, including South Africa.

China's long-term goal is to launch a global quantum communication service by 2027. Pan Jianwei, a leading physicist and chief architect of the Mozi satellite, has described this effort as a step toward building a fully operational quantum satellite constellation.

The global competition in quantum technology is intensifying.

Yin said that competition in quantum information technology is "essentially a game of national comprehensive scientific and technological strength," SCMP reported.

Recommendations to Optimize China's Quantum Strategy

China is positioning itself as a leader in this field by enhancing basic research, expanding investment in applied quantum technology, and refining policies to attract top talent. During her NPC address, Yin recommended that China optimize its strategy for training and retaining experts in quantum information science.

According to the SCMP, Yin is also fostering international collaboration, adding that science and technology are still a global matter. She added that China should promote high-level international exchanges and cooperation in quantum technology," she said.

Establishing international quantum standards, she added, could allow China to exert greater influence over the future global quantum communication network.

China intends to leverage its quantum satellites to establish secure communications between the BRICS – Brazil, Russia, India, China, and South Africa – bloc of emerging markets, reported SCMP.

Pan Jianwei, known as the "father of quantum" and one of key researchers who built the Mozi satellite, said that China aimed to complete its quantum satellite constellation and then launch an ultra-secure global communications service by 2027, according to SCMP.

While quantum communication holds promise for securing sensitive information, significant challenges remain. Scaling up QKD for widespread use requires overcoming obstacles related to cost, satellite coverage, and integration with existing communication infrastructure.

14. Andhra Pradesh Plans 'Quantum Valley' to Advance India's National Quantum Mission

by Cierra Choucair
https://thequantuminsider.com/2025/03/12/andhra-pradesh-plans-quantum-valley-to-advance-indias-national-quantum-mission/?utm_source=resonance-newsletters.beehiiv.com&utm_medium=newsletter&utm_campaign=the-quantum-insider-weekly-d-wave-makes-waves-nist-s-back-up-algorithm-and-more-news&_bhlid=26834347f4f6496f632414b62ccc11d385c11d42

The Andhra Pradesh government has announced plans to establish a Quantum Valley, a quantum computing hub in Amaravati, as part of India's National Quantum Mission. The initiative, led by Chief Minister N. Chandrababu Naidu, is intended to provide the infrastructure necessary in hopes of establishing the state as a leading center for quantum technology research and development in India.

According to a recent post from The Hindu, Naidu stated, "Just as we led the Information Technology revolution in the 1990s, we want Andhra Pradesh to lead advancements in Quantum Technology, securing a first-mover advantage in this transformative field." To support this effort, the state government is forming a task force to oversee the development of the hub and drive investments into the sector.

Collaboration with Industry and Academia

As noted across sources, the Quantum Valley project is expected to involve collaborations with IIT Madras, Tata Consultancy Services, and IBM, among other institutions. These partnerships are expected to bring together expertise in quantum computing, artificial intelligence, and advanced computational methods.

A high-level meeting was held to discuss the framework for the initiative, with participation from Natarajan Chandrasekaran, Chairman of Tata Sons; S.N. Subrahmanyan, Chairman & MD of L&T; Prof. Abhay Karandikar, Secretary, Department of Science and Technology; J.B.V. Reddy, Head of Quantum Technology Centre, DST; Prof. Satyanarayana Kalidindi, Director, IIT Tirupati; Prof. Kamakoti, Director, IIT Madras; Dr. Amith Singhee, Director, IBM Research India; and Venkat Subramaniam of IBM Quantum India.

As reported by APAC Media, this meeting was a significant step toward shaping Andhra Pradesh's role in India's broader quantum technology efforts. Venkat Subramaniam, IBM Quantum India Leader, described the initiative as a "visionary plan" to position India as a global quantum leader within the decade. In a recent LinkedIn post, he noted that Naidu is focused on "leadership in skilling, research, and industry" and has demonstrated his commitment by convening leaders across government, academia, and industry to bring the vision to reality.

Strategic Goals and Investment Plans

According to IndianWeb2, the Quantum Valley initiative is designed to achieve three primary objectives:

- **Attracting Talent** – The state is focused on designing an environment that draws top-tier researchers, engineers, and scientists in quantum computing.
- **Encouraging Global Investments** – Andhra Pradesh is positioning itself to attract foreign and domestic investments into quantum research and development.
- **Developing Advanced Technologies** – The initiative will focus on quantum computing applications across various fields, including artificial intelligence, cybersecurity, defense, and financial modeling.

The Andhra Pradesh government is expected to integrate quantum computing infrastructure into its technology ecosystem in Amaravati, potentially linking it to a larger DeepTech Research Park, as noted by IndianWeb2.

Alignment with India's National Quantum Mission

India's National Quantum Mission is a ₹6,000 crore (approximately $725 million) initiative intended to support developments in quantum computing, communications, sensing, and materials research. The program is expected to run until 2031 and supports multi-institution collaborations to advance quantum technology capabilities in the country.

The Quantum Valley initiative aligns with the mission's objectives, especially in terms of promoting quantum computing research and work towards its practical applications. According to The Hindu, Naidu emphasized that Andhra Pradesh's strategy is designed to leverage quantum computing for economic growth, akin to the state's previous role in India's IT expansion.

Next Steps and Industry Implications

While details on funding and infrastructure for the Quantum Valley project are still emerging, including confirmation from listed collaborators, the potential input from major technology firms and research institutions suggests a structured approach toward building a quantum technology ecosystem in Andhra Pradesh.

As noted by APAC Media, this initiative is expected to accelerate India's progress in quantum computing, supporting both domestic research initiatives and global collaborations. The government's task force, once operational, will likely provide further insights into specific funding sources, technology roadmaps, and potential policy frameworks supporting quantum innovation in the region.

15. Beyond Classical: D-Wave First to Demonstrate Quantum Supremacy on Useful, Real-World Problem

by Alex Daigle
https://www.dwavequantum.com/company/newsroom/press-release/beyond-classical-d-wave-first-to-demonstrate-quantum-supremacy-on-useful-real-world-problem/

D-Wave Quantum Inc., a leader in quantum computing systems, software, and services and the world's first commercial supplier of quantum computers, today announced a scientific breakthrough published in the esteemed journal Science, confirming that its annealing quantum computer outperformed one of the world's most powerful classical supercomputers in solving complex magnetic materials simulation problems with relevance to materials discovery. The new landmark peer-reviewed paper, "Beyond-Classical Computation in Quantum Simulation," validates this achievement as the world's first and only demonstration of quantum computational supremacy on a useful problem.

An international collaboration of scientists led by D-Wave performed simulations of quantum dynamics in programmable spin glasses—computationally hard magnetic materials simulation problems with known applications to business and science – on both D-Wave's Advantage2TM prototype annealing quantum computer and the Frontier supercomputer at the Department of Energy's Oak Ridge National Laboratory. The work simulated the behavior of a suite of lattice structures and sizes across a variety of evolution times and delivered a multiplicity of important material properties. D-Wave's quantum computer performed the most complex simulation in minutes and with a level of accuracy that would take nearly one million years using the supercomputer. In addition, it would require more than the world's annual electricity consumption to solve this problem using the supercomputer, which is built with graphics processing unit (GPU) clusters.

"This is a remarkable day for quantum computing. Our demonstration of quantum computational supremacy on a useful problem is an industry first. All other claims of quantum systems outperforming classical computers have been disputed or involved random number generation of no practical value," said Dr. Alan Baratz, CEO of D-Wave. "Our achievement shows, without question, that D-Wave's annealing quantum computers are now capable of solving useful problems beyond the reach of the world's most powerful supercomputers. We are thrilled that D-Wave customers can use this technology today to realize tangible value from annealing quantum computers."

Realizing an Industry-First Quantum Computing Milestone

The behavior of materials is governed by the laws of quantum physics. Understanding the quantum nature of magnetic materials is crucial to finding new ways to use them for technological advancement, making materials simulation and discovery a vital area of research for D-Wave and the broader scientific community. Magnetic materials simulations, like those conducted in this work, use computer models to study how tiny particles not visible to the human eye react to external factors. Magnetic materials are widely used in medical imaging, electronics, superconductors, electrical networks, sensors, and motors.

"This research proves that D-Wave's quantum computers can reliably solve quantum dynamics problems that could lead to discovery of new materials," said Dr. Andrew King, senior distinguished scientist at D-Wave. "Through D-Wave's technology, we can create and manipulate programmable quantum matter in ways that were impossible even a few years ago."

Materials discovery is a computationally complex, energy-intensive and expensive task. Today's supercomputers and high-performance computing (HPC) centers, which are built with tens of thousands of GPUs, do not always have the computational processing power to conduct complex materials simulations in a timely or energy-efficient manner. For decades, scientists have aspired to build a quantum computer capable of solving complex materials simulation problems beyond the reach of classical computers. D-Wave's advancements in quantum hardware have made it possible for its annealing quantum computers to process these types of problems for the first time.

"This is a significant milestone made possible through over 25 years of research and hardware development at D-Wave, two years of collaboration across 11 institutions worldwide, and more than 100,000 GPU and CPU hours of simulation on one of the world's fastest supercomputers as well as computing clusters in collaborating institutions," said Dr. Mohammad Amin, chief scientist at D-Wave. "Besides realizing Richard Feynman's vision of simulating nature on a quantum computer, this research could open new frontiers for scientific discovery and quantum application development."

Advantage2 System Demonstrates Powerful Performance Gains

The results shown in "Beyond-Classical Computation in Quantum Simulation" were enabled by D-Wave's previous scientific milestones published in Nature Physics (2022) and Nature (2023), which theoretically and experimentally showed that quantum annealing provides a quantum speedup in complex optimization problems. These scientific advancements led to the development of the Advantage2 prototype's fast anneal feature, which played an essential role in performing the precise quantum calculations needed to demonstrate quantum computational supremacy.

"The broader quantum computing research and development community is collectively building an understanding of the types of computations for which quantum computing can overtake classical computing. This effort requires ongoing and rigorous experimentation," said Dr. Trevor Lanting, chief development officer at D-Wave. "This work is an important step toward sharpening that understanding, with clear evidence of where our quantum computer was able to outperform classical methods. We believe that

the ability to recreate the entire suite of results we produced is not possible classically. We encourage our peers in academia to continue efforts to further define the line between quantum and classical capabilities, and we believe these efforts will help drive the development of ever more powerful quantum computing technology."

The Advantage2 prototype used to achieve quantum computational supremacy is available for customers to use today via D-Wave's Leap™ real-time quantum cloud service. The prototype provides substantial performance improvements from previous-generation Advantage systems, including increased qubit coherence, connectivity, and energy scale, which enables higher-quality solutions to larger, more complex problems. Moreover, D-Wave now has an Advantage2 processor that is four times larger than the prototype used in this work and has extended the simulations of this paper from hundreds of qubits to thousands of qubits, which are significantly larger than those described in this paper.

16. Decoding Quantum Hype: What Google, Microsoft, and AWS Are Really Announcing

by Carmen Recio
https://www.finos.org/blog/decoding-quantum-hype-what-google-microsoft-aws-are-really-announcing?utm_source=substack&utm_medium=email

The delay in getting commercial value on real world applications from quantum computing can be attributed to one overarching fact, the hardware is not ready yet. Whereas classical information is represented on transistors as "bits," quantum information is represented on physical quantum bits, aka "qubits." Now, how does one engineer a qubit? There are different proposals for this. However, physical qubits remain in relatively short supply, and like early transistors are far too error-prone for reliable computation. We need breakthroughs.

Social media has erupted over the past few months with grand announcements from Google Quantum AI, then Microsoft, and now AWS. Unfortunately, like an archaeological dig, the valuable artifacts of knowledge we're looking for have been buried under layers of hype, misinformation, and jargon. These artifacts have been recovered, however, and are on display for all to see.

Google Quantum AI's "Willow"

The Announcement

In December 2024, Google introduced its Willow quantum chip, which represents a major advancement in quantum computing. Willow significantly reduces errors as it scales, addressing a long-standing challenge in quantum error correction. The announcement also highlighted that the chip can perform certain computations in under five minutes that would take a supercomputer 10 septillion years, emphasizing its capacity to solve complex problems beyond the reach of classical computing.

What does that mean?

The key point here is Willow's ability to achieve "below threshold" error rates while increasing qubits. This breakthrough marked a crucial step towards commercially viable quantum computers. Let's explain what that means.

The "Willow" chip accomplished several things. First, it doubled the number of physical qubits that were previously available on a Google Quantum AI chip. Second, without getting technical, physical qubits can retain information for a short period of time, and this duration was multiplied by five. This duration, called "coherence," provides a window of opportunity for computation. Computation must be completed within this window, and this window is now roughly five times longer than it used to be, allowing roughly five times as many operations during the execution of an algorithm. Third, the accuracy, or "fidelity," of performing operations improved.

Most importantly, "Willow" demonstrated that "logical qubits" can improve coherence further. The crucial point here is that using more physical qubits, extends coherence as we predict it should. We can add more physical qubits to our logical qubits, thus opening up the "window" long enough to faithfully execute our desired algorithms.

Microsoft's "Majorana 1"

The Announcement

On February 19, Microsoft introduced the Majorana 1, a quantum computing chip based on "topological" qubits. This advancement marks a significant step in quantum technology, aiming to develop a scalable, million-qubit processor that addresses complex industrial challenges. Majorana-based qubits promise to reduce measurement, control, and error correction issues prevalent in other qubit types.

Skepticism

At the time of this writing, there is insufficient evidence to prove that its "Majorana 1" chip is what they claim it to be. Skepticism is heightened by the knowledge that Microsoft has previously retracted a related paper. However, the excitement stems from the possibility of topological qubits finally becoming a reality.

What does that mean?

Whereas Willow's key breakthrough adds physical qubits to create better logical qubits, topological qubits can be thought of as being protected by physics itself. The potential benefits include enhanced scalability, (up to a million qubits on a single processor), reliability, (reduced need for extensive error correction), and the capability to solve industrial-scale problems more efficiently. Instead of needing millions or even billions of physical qubits to do what we want to do, the number of naturally-resilient topological qubits we would need is substantially less.

If Microsoft's claims withstand peer review, the modality is decades behind others. However, that could be short-lived depending on how robust they turn out to be. Speculatively, they could shoot right past the other modalities, analogous to transistors overtaking vacuum tubes. Again, speculatively, that would change the projected timelines for commercially-useful quantum computing. What's interesting is that Microsoft is pointing to the age of the paper that is currently in question. Although the paper has not satisfied peer review, Microsoft's public statements are reportedly based on more recent, yet-to-be-published data. Again, there is skepticism based on the historical retraction. However, there is a combination of optimism and hope that this unpublished data will satisfy peer review, because that would indeed be exciting.

AWS's "Ocelot"

The Announcement

AWS has announced Ocelot, a new quantum computing chip developed by the AWS Center for Quantum Computing at Caltech. Ocelot significantly reduces the costs of quantum error correction by up to 90% compared to current methods, marking a breakthrough towards fault-tolerant quantum computers. The chip uses "cat qubits," which inherently suppress certain errors, and integrates error correction directly into its architecture. This approach could make quantum computers smaller, more reliable, and cheaper, accelerating the timeline for practical quantum computers by up to five years.

What does that mean?

The "Ocelot" chip can be thought of in some sense as being somewhere in-between "Willow" and "Majorana 1." This type of qubit, called a "cat qubit," is in the same family of "superconducting" qubits as Willow's "transmon" qubits, but they are engineered to have lower error rates. An explanation would get rather complicated, so the key takeaway is fewer errors. Cat qubits still need to be encoded as logical qubits, but substantially fewer cat qubits are needed per logical qubit to achieve the same error rates as compared to transmons. Therefore, to perform comparable computation, we would need the fewest topological qubits, more cat qubits, and even more transmon qubits.

Like Google Quantum AI, AWS demonstrated that larger error correction codes produce stronger benefits. However, AWS demonstrated that it could implement comparable codes using noticeably fewer physical qubits. As the codes get larger, the savings in regard to physical qubits will become even more pronounced. It is important to note that there are differences in coherence times and various error rates, but the key takeaway is that cat qubits can detect and correct errors with fewer total physical qubits compared to transmons. Commercially-useful algorithms will run on relatively small cat qubit quantum computers compared to their transmon counterparts.

Conclusion

Google Quantum AI and AWS advancements in error correction, have marked a crucial step towards commercially viable quantum computers.

The announcement of Microsoft's Majorana 1 chip is relevant as it signifies a notable technological advancement. However, it is unlikely to significantly shorten the timelines for practical, useful quantum computing due to existing challenges. While there is genuine progress, media coverage has tended to be overly hyped. This development strengthens Microsoft's position but does not definitively place them at the forefront of quantum computing, given the strong competition in the field.

Even though the hardware isn't fully developed yet, it's now a question of when, not if. Additionally, quantum technology isn't plug and play. Thus, the financial sector should proactively work on understanding how to integrate quantum computing into their operations to be prepared when commercially viable quantum computers become available.

17. NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption

by Chad Boutin
https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption?utm_source=substack&utm_medium=email

Last year, NIST standardized a set of encryption algorithms that can keep data secure from a cyberattack by a future quantum computer. Now, NIST has selected a backup algorithm that can provide a second line of defense for the task of general encryption, which safeguards internet traffic and stored data alike.

Encryption protects sensitive electronic information, including internet traffic and medical and financial records, as well as corporate and national security secrets. But a sufficiently powerful quantum computer, if one is ever built, would be able to break that defense. NIST has been working for more than eight years on encryption algorithms that even a quantum computer cannot break.

Last year, NIST published an encryption standard based on a quantum-resistant algorithm called ML-KEM. The new algorithm, called HQC, will serve as a backup defense in case quantum computers are someday able to crack ML-KEM. Both these algorithms are designed to protect stored information as well as data that travels across public networks.

HQC is not intended to take the place of ML-KEM, which will remain the recommended choice for general encryption, said Dustin Moody, a mathematician who heads NIST's Post-Quantum Cryptography project.

"Organizations should continue to migrate their encryption systems to the standards we finalized in 2024," he said. "We are announcing the selection of HQC because we want to have a backup standard that is based on a different math approach than ML-KEM. As we advance our understanding of future quantum computers and adapt to emerging cryptanalysis techniques, it's essential to have a fallback in case ML-KEM proves to be vulnerable."

Encryption Based on Two Math Problems

Encryption systems rely on complex math problems that conventional computers find difficult or impossible to solve. A sufficiently capable quantum computer, though, would be able to sift through a vast number of potential solutions to these problems very quickly, thereby defeating current encryption.

While the ML-KEM algorithm is built around a mathematical idea called structured lattices, the HQC algorithm is built around another concept called error-correcting codes, which have been used in information security for decades. Moody said that HQC is a lengthier algorithm than ML-KEM and therefore demands more computing resources. However its clean and secure operation convinced reviewers that it would make a worthy backup choice.

Present and Future Standards

HQC is the latest algorithm chosen by NIST's Post-Quantum Cryptography project, which has overseen efforts since 2016 to head off potential threats from quantum computers. HQC will take its place alongside the four algorithms NIST selected previously. Three of those algorithms have been incorporated into finished standards, including ML-KEM, which forms the core of the standard called FIPS 203.

The other two finished standards, FIPS 204 and FIPS 205, contain digital signature algorithms, a kind of "electronic fingerprint" that authenticates the identity of a sender, such as when remotely signing documents. The three finished standards are ready for use, and organizations have already started integrating them into their information systems to future-proof them.

A draft of the fourth standard, built around the FALCON algorithm, also concerns digital signatures and will be released shortly as FIPS 206.

HQC is the only algorithm to be standardized from NIST's fourth round of candidates, which initially included four algorithms meriting further study. NIST has released a report summarizing each of these four candidate algorithms and detailing why HQC was selected.

NIST plans to release a draft standard built around HQC for public comment in about a year. Following a 90-day comment period, NIST will address the comments and finalize the standard for release in 2027.

Draft Guidance for KEM Algorithms

One thing HQC has in common with ML-KEM is that they are both what experts call "key encapsulation mechanisms," or KEMs. A KEM is used over a public network as a sort of first handshake between two parties that want to exchange confidential information.

NIST has recently published draft guidance for implementing KEM algorithms. This guidance, *Recommendations for Key Encapsulation Mechanisms* (NIST Special Publication 800-227), describes the basic definitions, properties and applications of KEMs. It also provides recommendations for implementing and using KEMs in a secure manner. NIST hosted a virtual Workshop on Guidance for KEMs in February, and the draft was open for public comment until March 7, 2025.

18. Quantum Singularity Ahead? China's Zuchongzhi-3 Reshapes Quantum Race

by Luis E. Romero
https://www.forbes.com/sites/luisromero/2025/03/10/quantum-singularity-ahead-chinas-zuchongzhi-3-reshapes-quantum-race/?utm_source=substack&utm_medium=email

Chinese scientists have unveiled the Zuchongzhi-3, a 105-qubit superconducting quantum processor that reportedly operates 10^15 times faster than the world's most powerful classical supercomputer. This breakthrough, developed by researchers at the University of Science and Technology of China (USTC), represents a dramatic escalation in the global quantum computing competition, with performance claims that go neck-to-neck with Google's Willow. As the race heats up, the quantum computing singularity seems closer than ever. However, skeptics argue it is still decades away, even as new and increasingly impressive breakthroughs and advancements occur more frequently.

The Technical Achievement: Fidelity and Coherence

Zuchongzhi-3's architecture represents a significant upgrade from its predecessor, Zuchongzhi-2, featuring 105 qubits arranged in a 15×7 array with 182 couplers to enhance connectivity. The processor achieves impressive operational fidelities, with single-qubit gates at 99.90%, two-qubit gates at 99.62%, and readout fidelity at 99.13%. Most notably, its coherence time of 72 microseconds enables more complex quantum operations before decoherence occurs. This performance improvement allowed researchers to conduct an 83-qubit, 32-cycle random circuit sampling experiment that demonstrated quantum computational advantage over classical computers by 15 orders of magnitude.

The Global Quantum Race: Zuchongzhi-3 and Willow Matchup

The Zuchongzhi-3 announcement intensifies what has become a high-stakes international competition. Google, which first claimed "quantum supremacy" in 2019 with its 53-qubit Sycamore processor, recently unveiled its 105-qubit Willow chip. While matching Zuchongzhi-3's qubit count, Willow takes a different approach by focusing heavily on quantum error correction – allowing it to perform computations in under five minutes that would theoretically take classical supercomputers approximately 10 septillion years.

Meanwhile, Microsoft has pursued an entirely different strategy with its Majorana 1 processor. Rather than using traditional superconducting qubits, Microsoft created an entirely new state of matter—a topological

superconductor – to build a more stable quantum system. While currently featuring only 8 qubits, Microsoft claims this approach offers a path to million-qubit systems within a relatively small quantum computing fridge, potentially addressing quantum computing's fundamental stability challenges.

Beyond Laboratory Demonstrations: Is the Quantum Singularity Near?

While these developments demonstrate remarkable technical achievements, significant questions remain about when quantum computers will transition from laboratory demonstrations to practical applications. The diversity of approaches – from China's emphasis on computational speed to Google's focus on error correction and Microsoft's topological architecture – reflects different strategies for overcoming quantum computing's inherent challenges.

19. AdGuard becomes the latest VPN to add post-quantum encryption

by Chiara Castro
https://www.techradar.com/vpn/vpn-services/adguard-becomes-the-latest-vpn-to-add-post-quantum-encryption

AdGuard just became the latest VPN provider to add quantum-resistant encryption to its software.

Specifically, AdGuard VPN now integrates a combination of classic encryption methods with one of the post-quantum algorithm standards released by the National Institute of Standards and Technology (NIST) in August last year. The feature was rolled out on macOS and Windows on March 6, 2025, with the mobile apps expected to get the upgrade later in the month.

The firm now follows in the footsteps of Google Chrome and some of the best VPN providers on the market by upgrading its encryption protections to ensure user data is protected against new threats posed by quantum computing.

The need for quantum-proof encryption

"We are on the brink of the quantum technology era, and data protection must stay ahead of the threats, not just react to them. By implementing post-quantum cryptography, we are laying the foundation for a secure internet in the future," said Denis Vyazovoy, AdGuard VPN CPO.

Experts predict that it's just a matter of time before quantum computers break current RSA-based encryption methods. This is mainly because these machines will have the ability to process computations that today's computers can't handle, within minutes.

Recent releases such as Google's Willow quantum chip and Microsoft's Majorana 1 chip, AdGuard explains, "are pushing quantum computing closer to solving complex real-world problems." This may be a portent of what the industry has long feared – that current encryption will soon become obsolete.

Quantum computers are still some years away from becoming mainstream, but cybercriminals are thought to have already adopted "harvest now, decrypt later" attacks. These involve malicious actors collecting encrypted data and decrypting it once quantum machines are up for the task.

It's exactly with this in mind that NIST experts released the first sets of quantum-safe algorithms last year designed for specific tasks, namely protection for key exchanges (ML-KEM) and identity authentication (ML-DSA and SLH-DSA).

As mentioned earlier, AdGuard VPN has implemented a hybrid encryption approach that includes the classic X25519 elliptic curve algorithm with the post-quantum Kyber768-based ML-KEM768.

This dual-layer encryption approach, the provider explains, "ensures robust protection against both current and future risks, enabling secure session keys that are resilient to quantum computing advancements."

This is exactly what the likes of Google, Signal, Tuta Mail, ExpressVPN, NordVPN, Mullvad VPN, Windscribe, and PureVPN have also done.

Put simply, having a hybrid encryption method ensures that tried and tested algorithms always protect your data, even if the post-quantum protection fails.

If you're using the latest version of AdGuard VPN on desktop, you should already be able to enable this feature through the settings menu. This advanced security option is also expected to land on the iOS and Android VPN apps in the next couple of weeks.

20. eMemory and PUFsecurity Cryptography Solution Secures the Future of Computing

https://www.eetindia.co.in/ememory-and-pufsecurity-cryptography-solution-secures-the-future-of-computing/

eMemory Technology Inc. and its subsidiary PUFsecurity, a pioneer in Physical Unclonable Function (PUF)-based security IP, have launched the world's first PUF-based Post-Quantum Cryptography (PQC) solution.

The groundbreaking innovation combines eMemory's cutting-edge NeoPUF technology with advanced PQC algorithms to deliver unparalleled security for the next generation of computing, safeguarding devices against the emerging threats posed by quantum computing.

As quantum computing advances, traditional cryptographic systems, such as RSA and Elliptic Curve Cryptography (ECC), face increasing vulnerability to quantum attacks. In response, eMemory and PUFsecurity have developed a forward-looking solution that leverages the inherent randomness and uniqueness of PUF technology alongside PQC algorithms, including Kyber (ML-KEM) for key encapsulation and Dilithium (ML-DSA) for digital signatures. By using PUF-generated randomness as the seed for PQC within PUFsecurity's crypto coprocessor (PUFcc), which features a built-in hardware root of trust (PUFrt), this innovation ensures resilient protection against quantum threats while maintaining efficiency and scalability for modern applications, from cloud computing to IoT devices.

This groundbreaking PUF-based PQC solution enables on-chip generation of quantum-resistant keys without relying on external key injection. By harnessing NeoPUF's quantum-tunneling mechanism, which exploits natural silicon variations to produce highly random and unclonable identifiers, this technology provides a secure foundation for key generation, storage, and authentication. This eliminates vulnerabilities associated with traditional key provisioning processes and offers a streamlined, cost-effective path to quantum-safe security.

"We are thrilled to introduce the first PUF-based PQC solution, a milestone that positions eMemory and PUFsecurity at the forefront of securing future computing," said Charles Hsu, founder of eMemory and PUFsecurity. "As the threat of quantum computing looms, eMemory and PUFsecurity have joined forces to deliver a proactive, hardware-based approach that not only meets today's security needs but also prepares our partners and customers for tomorrow's challenges."

The launch comes at a critical time, as governments and industries worldwide accelerate efforts to standardize PQC to counter "harvest now, decrypt later" threats, where sensitive data encrypted today could be decrypted by quantum computers in the future. This PUF-based PQC solution addresses these concerns by embedding quantum-tunneling NeoPUF and next-generation quantum-resistant cryptography directly into the silicon, ensuring data protection across the device lifecycle.

"Security is the cornerstone of the connected world, and our new PUF-based PQC solution sets a new standard for trust and resilience," added Michael Ho, President of eMemory. "By combining our expertise in embedded memory with PUFsecurity's leadership in hardware security, we are empowering chip designers to build quantum-safe systems with confidence."

Available now, this solution is designed for seamless integration across multiple foundry platforms, offering flexibility for applications in AI, automotive, cloud infrastructure, and beyond. eMemory and PUFsecurity invite industry partners to explore how this innovation can enhance their security strategies and prepare them for the quantum era.

21. STMicroelectronics reveals solutions for post-quantum cryptography, bringing quantum resistance to embedded systems

by Alexander Jurman
https://www.einnews.com/pr_news/792388379/stmicroelectronics-reveals-solutions-for-post-quantum-cryptography-bringing-quantum-resistance-to-embedded-systems

STMicroelectronics has introduced hardware cryptographic accelerators and associated software libraries for general-purpose and secure microcontrollers, ready for future generations of embedded systems to resist quantum attacks.

As quantum computers are beginning to outperform classical computers in research trials, industries are starting to prepare now for their use to become mainstream. New government specifications are emerging to standardize Post-Quantum Cryptography (PQC), leveraging new techniques based on mathematical problems that are difficult for quantum computers to solve. The PQC standards published to-date use the award-winning Keccak algorithm -- a highly resistant hash algorithm which has been invented by ST experts.

Solutions compliant with these standards are needed now, so that product developers can build-in protection according to current best practice and continue to strengthen resistance as the state of the art evolves. ST's new solutions are available for STM32 developers in the X-CUBE-PQC software library, and for Stellar automotive microcontrollers that contain the SHA-3 hardware accelerator. There are also new software libraries and hardware IPs for secure microcontrollers, targeting Common Criteria and FIPS 140-3 and supporting ML-KEM, ML-DSA and XMSS/LMS PQC algorithms.

"Quantum computers are expected to bring advantages to activities such as finance, scientific research, earth observation, and many more. On the other hand, they could overpower some current types of cryptography in equipment used on a daily basis," said Jacques Fournier, Director of Security Platform at STMicroelectronics. "ST is the first to provide quantum resistant features across all its product ranges, for all customers, for all required levels of security."

The post-quantum cryptographic assets ST is announcing today are ready to use, empowering customers to bring quantum resistance to critical security features of their products like firmware update, secure boot, and authentication mechanisms.

ST's Jacques Fournier will address the embedded world Exhibitor Forum in Nuremberg on March 12, 2025. Visitors can discuss the latest quantum-resistant algorithms with the company's security experts and see related demonstrations at the ST booth, 4A-148, during the event.

22. Quantum Computing Threatens Traditional Encryption

by Norman Willox
https://www.iotworldtoday.com/quantum/quantum-computing-threatens-traditional-encryption

As quantum computing advances, traditional encryption methods—including the public key encryption techniques RSA and ECC—are nearing obsolescence. The failure to implement post-quantum cryptography solutions in time will leave sensitive communications, financial transactions, and national security data vulnerable to decryption by quantum-enabled adversaries. The urgency to act is no longer theoretical; it is a pressing cybersecurity challenge that demands immediate action.

Store Now, Decrypt Later Risk

Cybercriminals and nation-state actors are already employing store now, decrypt later tactics, harvesting encrypted data today with the expectation of decrypting it once quantum computing reaches the necessary scale. This means that sensitive corporate, government, and personal information exchanged now may be exposed in the near future, leading to permanent data breaches that cannot be undone.

Compounding this threat, AI-driven cyberattacks are accelerating in sophistication, automating reconnaissance, data exfiltration, and cryptanalysis processes. The convergence of AI-powered threats and quantum decryption will create a cybersecurity environment where traditional encryption defenses are rendered ineffective.

Consequences of Delayed Post-Quantum Cryptography Adoption

Failing to transition to post-quantum cryptography solutions in time will result in the following:

Permanent Privacy Loss
Once decrypted, sensitive information is exposed indefinitely, affecting individuals, corporations, and governments.

Regulatory and Legal Risks
Organizations failing to implement quantum-resistant encryption may face regulatory penalties, lawsuits, and reputational damage.

Competitive Disadvantage
Companies delaying PQC adoption will fall behind competitors that are securing their intellectual property and customer data.

Financial System Vulnerabilities
Quantum-enabled decryption could disrupt banking transactions, compromise digital assets, and threaten the stability of financial markets.

Erosion of Public Trust
A failure to secure encrypted communications will weaken trust in digital platforms, leading to reduced adoption of online services.

Immediate Actions for Security Professionals

To mitigate these risks, organizations must proactively implement quantum-resistant cybersecurity strategies by:

Deploying NIST-Approved PQC Algorithms
Transitioning to lattice-based, hash-based, and multivariate cryptographic solutions to safeguard data from quantum decryption.

Implementing a Zero-Trust Security Model
Strengthening authentication, access control, and endpoint security to minimize exposure.

Securing Communication Channels
Moving away from vulnerable email, VoIP, and conferencing platforms in favor of quantum-resistant alternatives.

Enhancing AI-Driven Threat Detection
Using AI-powered security tools to identify and mitigate quantum-era cyber threats proactively.

Time to Act is Now

Quantum computing is no longer a distant concern; it is an imminent security challenge requiring immediate action. Organizations that fail to adopt PQC solutions in 2025 risk irreversible damage to their data security and privacy. Delays will carry severe financial, regulatory, and operational consequences. Security professionals must act now to ensure cryptographic resilience before quantum decryption capabilities become a widespread reality. The cost of inaction is too great to ignore.

23. How Many Quantum Computers Are There in the World? Estimates Suggest Over 100 in 2025

by Quantum News
https://quantumzeitgeist.com/how-many-quantum-computers-are-there/?utm_source=substack&utm_medium=email

The difficulty in pinpointing the number of quantum computers stems from several factors, including differing definitions of what constitutes a quantum computer, underreporting by some countries, and varying levels of accessibility. Some systems remain confined to laboratory settings, while others are accessible via cloud services, expanding their reach but complicating efforts to track them comprehensively.

The global count of quantum computers remains uncertain due to several factors. First, the definition of a quantum computer varies, encompassing gate-based models like those developed by IBM and Google, quantum annealers such as D-Wave's systems, and hybrid setups that integrate classical and quantum elements. This diversity complicates enumeration.

IBM and Google are prominent in the gate-based model. IBM offers cloud access to multiple quantum computers featuring varying qubit counts. Google has advanced its quantum processors toward error correction and practical applications. D-Wave specializes in quantum annealing for optimization tasks, providing distinct systems from traditional gate models.

Academic institutions often host quantum setups primarily for research, while startups explore innovative approaches, though their contributions are less documented. Additionally, some nations may develop quantum computers covertly, leading to underreporting and further opacity in global counts.

Putting a Number on Number of Quantum Computers on The Planet: 100

IBM has led the deployment of superconducting quantum computers via the quantum cloud. They have a public roadmap and announced that they will deploy numerous systems to partners and clients worldwide, including universities and research institutions. They've likely built and deployed dozens of systems, gradually increasing in qubit count and performance over time. *Reasoned Estimate: 20-30+ quantum computers*. This is based on the publicly announced partnerships, their Quantum Network, and the yearly goal of deploying multiple systems.

Google focuses on superconducting quantum computers and famously achieved "quantum supremacy" (a demonstration of a quantum computer outperforming a classical one on a specific task) in 2019. While they don't offer widespread cloud access like IBM, they have built multiple generations of processors for internal research and select collaborations. *Reasoned Estimate: 5-10 quantum computers*. Google's focus has been pushing capability boundaries with fewer advanced, highly controlled systems rather than broad deployment.

Rigetti builds superconducting quantum computers and provides cloud access through its Quantum Cloud Services. It has partnerships with various organizations and has manufactured several generations of its "Aspen" series chips. *Reasoned Estimate: 5-10 quantum computers*. Rigetti's strategy involves internal research and providing access to external users, suggesting a moderate number of deployed systems with a mix of internal and externally accessible machines. They are actively selling their Novera 9 qubit chip.

IonQ utilizes trapped-ion technology, which offers potential advantages in qubit coherence and connectivity. They offer access through significant cloud providers like Amazon Braket, Microsoft Azure Quantum, and Google Cloud. While they don't disclose the number of physical systems, their public roadmap and published research indicate ongoing system development and deployment. Ion traps are generally more complex to scale in physical size than superconducting circuits. *Reasoned Estimate: 3-7 quantum computers*. The focus on cloud accessibility through partners and the complexity of scaling trapped-ion systems suggests fewer competent machines.

D-Wave specializes in quantum annealing, a type of quantum computing suited for optimization problems. Its systems are commercially available and have been purchased by various organizations. It has released several generations of its "Advantage" system. Quantum annealers are distinct from gate-based quantum computers. *Reasoned Estimate: 5-10 quantum annealers*. D-Wave has been commercially selling its systems for a more extended period than most other companies on this list, and it is focused on a specific type of quantum computation.

Quantinuum, formed from the merger of Honeywell Quantum Solutions and Cambridge Quantum, uses trapped-ion technology. It has publicly stated that it operates multiple systems and provides commercial access. *Reasoned Estimate: 3-7 quantum computers*. Like IonQ, Quantinuum utilizes trapped-ion technology, which is inherently more difficult to scale in terms of the number of physical systems. It focuses on high-fidelity, fully connected qubits.

PsiQuantum is known for its work in Photonic Quantum Computing, which uses photons instead of ions or superconducting circuits. They have raised substantial amounts of funding and made advancements in manufacturing and quantum computation. Due to the very nature of Photonic quantum computing, scaling up is much more involved than other methods. *Reasoned Estimate: 1-2 Quantum computers*. They are still in a growth and development phase, and their main focus is on fault tolerance, which is only an issue once many qubits have been achieved.

IQM, based in Finland, focuses on building superconducting quantum computers, particularly for on-premise deployment at supercomputing centers and research labs. They've secured significant funding and have partnerships with several European organizations. IQM emphasizes co-design, tailoring their hardware to specific application needs. They've delivered at least one system to a supercomputing center (VTT in Finland) and have announced others. *Reasoned Estimate: 30-50 quantum computers*. IQM's strategy of on-premise deployment, coupled with their relatively recent founding (compared to IBM or D-Wave), and the known delivery to VTT and announced projects, points to a smaller, but rapidly growing, number of deployed systems. Back in 2024, they claimed 30 machines in production.

Microsoft's primary focus in quantum computing is developing the *Azure Quantum* ecosystem. This cloud platform provides *partners* like IonQ, Quantinuum, Rigetti, and Pasqal access to quantum hardware. They are also heavily invested in quantum software development (Q#, QDK) and research into topological qubits. The Jury is still out about how many, but recent claims about creating a topological qubit (Majorana 1) have created excitement. *Reasoned Estimate: 1 (of their own) quantum computers*.

Pasqal, a French company, is developing quantum computers based on neutral atom technology. Neutral atoms, trapped and controlled by lasers, offer another promising path to scalability and coherence. Pasqal offers cloud access to their systems and partners with various research institutions and industrial clients. They've announced the sale of systems to HPC centers. *Reasoned Estimate: 2-5 quantum computers*. Similar to IonQ and Quantinuum, the complexity of scaling neutral atom systems, combined with their focus on both cloud access and on-premise deployments,

Atom Computing, based in the US, uses neutral atoms as their qubit modality. They've publicly demonstrated a system with many qubits (though qubit count alone isn't the sole performance measure) and are pursuing a roadmap toward fault-tolerant quantum computing. They are relatively new but have made rapid progress. *Reasoned Estimate: 1-3 quantum computers*. Given their recent entry and the focus on a large-scale, next-generation system, they likely have fewer prototype or early-generation machines, primarily for internal development and testing.

Xanadu, a Canadian company, focuses on photonic quantum computing, using light (photons) as qubits. They offer cloud access to their "Borealis" and earlier "X-series" photonic quantum processors. Photonic quantum computing has potential advantages in terms of scalability and connectivity. *Reasoned Estimate: 2-4 quantum computers*. Xanadu's cloud-based access model and the publication of results from their Borealis system suggest they have a few operational systems, though likely fewer than companies focusing on superconducting circuits with wider commercial deployment.

Infleqtion (formerly ColdQuanta), based in the US, is pursuing multiple quantum technologies, including neutral atom quantum computing (with their "Hilbert" system) and quantum sensing/timing. They supply components and systems for quantum research and are developing their own quantum computer. *Reasoned Estimate: 1-3 quantum computers (for the computing aspect specifically)*. Infleqtion's diversified approach, with a focus on both components and a complete system, along with their relative newness in the quantum *computing* market (they have longer experience in other quantum areas), suggests a small number of early-stage computing systems.

QuEra Computing, spun out of research from Harvard and MIT, focuses on neutral-atom quantum computers. Their Aquilon quantum computer is available on Amazon Braket. Like Atom Computing and Pasqal, their neutral atom technology is known for its scalability and reconfigurability. *Reasoned Estimate: 1-3.* They have one known publicly available machine and are a newer company.

Oxford Quantum Circuits (OQC) is a UK-based company building superconducting quantum computers. It offers cloud access through its "Lucy" system and emphasizes a unique 3D architecture ("Coaxmon") designed for improved scalability and coherence. *Reasoned Estimate: 1-3 quantum computers*. OQC is a relatively new company focusing on a distinct architecture and cloud-based access, suggesting a small number of initial systems.

Seeqc focuses on developing the entire quantum computing stack, from hardware to software, but with a particular emphasis on cryogenic control and readout electronics. They are building superconducting quantum computers but aim to provide key components and integrated systems to other quantum

computing companies. *Reasoned Estimate: 1-3 quantum computers (in terms of full systems)*. Seeqc's role as both a system developer and a component supplier suggests they likely have a small number of complete systems, with much of their effort focused on enabling other players.

Universal Quantum is a UK-based company working on trapped-ion quantum computers. They are focused on a unique architecture that uses microwave-based gates and a scalable, modular approach. *Reasoned Estimate: 1-2 quantum computers*. Universal Quantum is still mainly in the research and development phase, working on a novel architecture, indicating a small number of prototype-level systems.

EeroQ is developing quantum computers based on electrons on helium. This is a relatively unexplored approach with potential advantages regarding coherence and scalability. *Reasoned Estimate: 0-1 (likely a prototype)*. EeroQ is in the research phase, exploring a fundamentally different qubit technology. It's unlikely they have a fully functional quantum computer at this stage, but they are developing somewhat experimental setups.

Silicon Quantum Computing (SQC) is an Australian company building quantum computers based on silicon qubits. This approach leverages existing semiconductor manufacturing technology. *Reasoned Estimate: 0-1 (likely a prototype)*. SQC is pursuing a long-term vision of silicon-based quantum computing, and while they have made significant progress in fabricating and controlling individual qubits, a fully functional, multi-qubit system is likely still under development.

Quantum Motion is a UK-based company focused on silicon-based quantum computing. It collaborates with academic institutions and leverages CMOS technology. *Reasoned Estimate: 0-1 (likely a prototype)*. Like SQC, Quantum Motion is in the research and development stage, working towards a scalable, silicon-based platform.

Beyond Vertically Integrated Quantum Computing

The quantum computing landscape is far more extensive than the companies building complete quantum computers. While estimates suggest between 45 and 130 complete quantum systems (including annealers) have been constructed by major players like IBM, Google, Rigetti, IonQ, D-Wave, and others, a vast and crucial ecosystem of companies providing essential components, software, and services exists.

This ecosystem includes specialists in cryogenics (Bluefors, Oxford Instruments), control electronics (Zurich Instruments, Keysight), microwave components, laser systems (Toptica, M Squared), quantum software (Q-CTRL, Riverlane, Classiq), and specialized materials and fabrication. These companies, research institutions, and consulting firms form the vital infrastructure enabling the development and advancement of quantum computing technology, making their contributions indispensable even though they don't produce complete quantum computers themselves. The health and growth of this broader supply chain are critical indicators of the overall progress of the field.

24. Microsoft and Amazon quantum advancements spark questions about the future of encryption

by CHRISTOPHER BUDD
https://www.geekwire.com/2025/microsoft-and-amazons-quantum-advancements-spark-questions-about-the-future-of-encryption/

With recent announcements of new quantum computing advancements, Microsoft, Amazon and Google have set a new countdown clock ticking on today's encryption — now an even shorter race than expected.

In one lane: those building quantum computers that can easily break the encryption that makes today's internet private. In the other lane: those building post-quantum cryptography (PQC), the next generation of encryption that can stand up to quantum computers.

It's not clear right now who's going to win this race and what security and privacy on the internet will be (or if it will be at all). But it is clear this is now coming faster than expected.

Effective encryption relies on algorithms that are computationally infeasible to crack. These algorithms are used to encrypt and decrypt data, keeping it private from everyone except those who have the keys.

But all encryption can be cracked with enough computing power. This is why over the past 30 years we've seen encryption algorithms retired and replaced; computing power has rendered the old ones ineffective. The old 1024-bit key encryption that was at the heart of the "crypto wars" of the 1990s is long-since retired and quaint now for that very reason. Cracking that encryption today is barely a speedbump.

The recent announcements from AWS, Google, and Microsoft make clear that the computing power that can be directed to break encryption is about to increase by an order of magnitude we've never seen before.

In December, Google announced "Willow." In February, Microsoft announced "Majorana 1." And less than two weeks after Microsoft, Amazon announced "Ocelot." All three announcements represent major, different innovations around quantum computing, a fundamentally different approach to designing processors that almost literally will put these new computers light years ahead of today's. Google's announcement gives good context:

> *Willow performed a standard benchmark computation in under five minutes that would take one of today's fastest supercomputers 10 septillion (that is, 10^25) years — a number that vastly exceeds the age of the Universe.*

Microsoft CEO Satya Nadella wrote on LinkedIn: "We believe this breakthrough will allow us to create a truly meaningful quantum computer not in decades, as some have predicted, but in years."

These developments represent significant leaps forward in terms of computing power, leaps that are truly unprecedented.

As with all unprecedented leaps forward, we can't begin to understand all the changes this will bring. But we can see one thing clearly in what Google and Microsoft say: in a few years, there will be computational power available that makes what is computationally infeasible today a problem solved in mere seconds.

That means that tomorrow's quantum computers will be able to crack today's encrypted information in mere seconds, or less. All of your encrypted information today will be easily readable when quantum computing becomes readily available.

Fortunately, there has been work underway in anticipation of this eventuality. The National Institute of Standards (NIST) has been working since 2016 on its Post-Quantum Cryptography project. NIST has been in the lead on encryption throughout the history of our industry and it is making progress on this project. In August, NIST released its first three finalized Post-Quantum Encryption Standards.

Microsoft, AWS and Google aren't only doing work that can break today's encryption: they're also actively involved with work on the solution of post-quantum cryptography.

All three have recently provided updates about the work they're doing in conjunction with NIST and its work to develop and deploy PQC. Google's announcement was in August; Microsoft's in September; and AWS' in December. These predate the new, recent hardware developments but all show the kind of broad, deep commitments that a problem of this size and scope requires. This is a good thing.

But having encryption standards that are being adopted is not broad deployment. There's a very long road ahead before your online banking app is regularly using PQC invisibly to protect your information. In technology, the devil is in the deployment: it always comes down to the "last mile" problem of getting the newest technology into the hands, homes and offices of regular people. Historically it's taken years for new encryption to achieve wide adoption.

That is why we're in a race now. And why everyone in technology needs to get engaged and start thinking about PQC today. Startups need to start making the question of "how are we going to deal with PQC" part of their plans and design decisions now.

Two truisms in the industry apply here. First, it's easier to break than it is to build. Second, encryption is hard and easy to screw up. These mean effectively defending encryption against quantum computing is going to take a lot of hard work. Work that needs to start now.

These latest developments are showing us that the road ahead for encryption is going to be very fast moving and very bumpy. Today's encryption is facing an extinction-level event from quantum computing. And companies that don't move fast will get caught up in that extinction-level event.

25. India Risks Falling Behind Without a Multi-Pronged Approach to Quantum Computing, Niti Aayog Report Says

by Matt Swayne
https://thequantuminsider.com/2025/03/06/india-risks-falling-behind-without-a-multi-pronged-approach-to-quantum-computing-niti-aayog-report-says/?utm_source=resonance-newsletters.beehiiv.com&utm_medium=newsletter&utm_campaign=the-quantum-insider-weekly-spain-invests-ibm-ceo-s-quantum-prediction-and-more-news&_bhlid=e0f3699f4c11316c3f0150a33c533eefcbee3ff7

India must adopt a broad quantum computing strategy to secure its technological future, according to a new study from a national think tank.

A report published in the March 2025 edition of *Future Front*®, Niti Aayog's quarterly technology insights publication, outlines the importance of quantum computing and its implications for national security, economic growth, and global competitiveness. By "multi-pronged" strategy, the study, produced in collaboration with the Data Security Council of India, means that India's position in the quantum computing race depends on coordinated efforts across research, education, industry partnerships and security preparedness. India, in fact, has a wealth of advantages in those areas, the report suggests, but must improve coordination.

Writing in the report, BVR Subrahmanyam, CEO of NITI Aayog, writes: "Quantum technologies will play a defining role in securing critical infrastructure, strengthening defense capabilities, and safeguarding our digital sovereignty. However, leadership in this domain will require more than technological prowess—it demands a bold vision, strong policy frameworks, and an ecosystem that fosters cutting-edge research, talent development and large-scale deployment."

The Indian government launched the National Quantum Mission (NQM) in 2023, budgeting 6,003 crore to build the country's quantum ecosystem, according to the Economic Times.

Niti Aayog (National Institution for Transforming India) is a public policy think tank for the Indian government.

A Multi-Pronged Strategy

The study recommends a comprehensive approach with several key components:

1. **Investment in Research and Development:** The report stresses the need for substantial government funding to support both basic and applied research. It recommends the creation of dedicated labs and research centers to explore quantum algorithms, materials, and hardware

development. These facilities would serve as incubators for next-generation ideas and ensure that India remains competitive on the global stage.

2. **Education and Skill Development:** Recognizing that technology is only as effective as the talent behind it, the study calls for the expansion of academic programs in physics, computer science, and engineering. By fostering a new generation of quantum scientists and engineers, India can build a workforce capable of advancing research and translating discoveries into commercial applications.
3. **Public-Private Partnerships:** The report urges closer collaboration between government agencies, academic institutions, and the private sector. Such partnerships would facilitate the sharing of knowledge and resources, driving innovation through a collective effort. Industry experts, as cited in the study, argue that bringing together diverse perspectives is essential to accelerate progress and overcome technical hurdles.
4. **International Collaboration and Standards:** While emphasizing self-reliance, the study also acknowledges that quantum computing is a global challenge. It recommends that India actively engage in international forums and standard-setting bodies to ensure that its interests are represented and to benefit from shared advancements in the field.
5. **Regulatory and Security Frameworks:** With the potential to break existing cryptographic systems, quantum computing poses a unique threat to national security. The study highlights the need to develop quantum-resistant encryption methods and robust regulatory frameworks to safeguard critical infrastructure and data. This dual focus on innovation and security is seen as crucial for maintaining both economic competitiveness and public safety.

Quantum Computing Advances

The Niti Aayog report states that the urgency for a quantum computing strategy is intensified because of the dramatic advances that scientists are making in quantum technologies, although challenges remain. The report lists details of several key advances in quantum computing that are shaping the field globally. These developments include improvements in qubit stability, error correction, and quantum algorithms, all of which bring quantum systems closer to practical applications. The advances include:

- **Longer Qubit Coherence**: Qubits, the fundamental units of quantum computation, must maintain their quantum state long enough to perform complex calculations. The report highlights recent breakthroughs in extending qubit coherence times, particularly through neutral atom architectures, which have demonstrated significantly improved stability.
- **Enhanced Qubit Control and Fidelity:** High-fidelity operations are critical for executing reliable quantum computations. Advancements in superconducting and trapped-ion qubit technologies have resulted in more accurate quantum gate operations, reducing computational errors and making quantum processors more dependable.
- **Progress in Quantum Error Correction**: Quantum computers are highly sensitive to noise, requiring robust error correction techniques. The report points to new hardware-based error correction methods, including Google's Willow chip, which integrates self-correcting mechanisms to improve computational stability. Additionally, research into surface codes and topological qubits is advancing fault-tolerant quantum computing.

- **Diversity in Qubit Modalities:** Rather than a single dominant approach, the field is progressing through multiple competing qubit designs. The report notes that superconducting circuits, trapped ions, photonic qubits, and neutral atoms are all being explored for scalability and performance. This diversity ensures that the field remains flexible, allowing breakthroughs in one area to influence others.
- **Developments in Topological Qubits:** Topological qubits are considered a promising approach for reducing errors at the hardware level. Microsoft's Majorana-based qubit research is among the efforts in this area, aiming to create more stable quantum processors that require less external error correction.
- **Advances in Quantum Algorithms and Software** Beyond hardware, progress is being made in quantum algorithms that improve computational efficiency. Quantum machine learning, optimization, and simulation techniques are expanding the range of problems quantum computers can solve. Leading companies and research institutions are also refining quantum programming languages, making it easier to develop practical applications.
- **Maturing Quantum Ecosystem and Supply Chain** The report notes that a growing network of suppliers and manufacturers is emerging to support quantum computing. Advances in specialized materials, cryogenic systems, and quantum chip fabrication are moving the industry toward scalable, commercially viable quantum systems.

National Security and Economic Implications

The report states that quantum computing's ability to solve complex problems could lead to advances in industries such as healthcare, logistics, and finance. Quantum algorithms could improve drug discovery, optimize supply chains, and enhance financial modeling.

At the same time, the technology could disrupt cybersecurity by rendering current encryption methods obsolete. The study warns that countries with early access to quantum computing will have a strategic advantage in intelligence gathering and defense.

A Coordinated Effort And Long-Term Commitment

The report proposes a national strategy that includes establishing quantum research centers, increasing funding for interdisciplinary research, and forming a task force to oversee implementation. It states that a fragmented approach could result in inefficiencies, while a coordinated effort would maximize investment impact.

The report notes that countries investing in quantum computing will shape global technology standards and influence international regulations. Without a clear national strategy, India risks falling behind in a field that is expected to define future economic and security landscapes.

The study acknowledges that widespread adoption of quantum computing will take time but emphasizes that early investments are necessary to build the infrastructure and expertise needed for long-term

success. It points to the importance of sustained funding and policy support to ensure India remains competitive.

Industry and Academic Perspectives

The study also includes input from researchers and industry leaders who stress the urgency of quantum investments.

One report considers the transition from theoretical research to practical, scalable quantum computing as a critical juncture in technology today, one that India must seize to build a resilient and forward-looking ecosystem.

Industry representatives suggest that a well-supported quantum strategy could attract private investment and foster commercial applications. The report states that building a robust quantum ecosystem would position India as a global leader in quantum research and innovation.

Moving Forward

The study provides a roadmap for India's quantum computing strategy, recommending targeted investments, workforce development, and security measures. It concludes that a well-planned, multi-pronged approach would ensure that India remains competitive in a rapidly evolving technological landscape.

Subrahmanyam writes: "Our future success hinges on our ability to proactively harness transformative technologies for inclusive economic growth and national security. Among these, quantum computing stands as a revolutionary force—one that has the potential to fundamentally reshape problem-solving, cryptography and strategic decision-making."

The goal is the creation of a "Frontier Tech Nation", Debjani Ghosh, Distinguished Fellow, NITI Aayog; Chief Architect, NITI Frontier Tech Hub.

"At the NITI Frontier Tech Hub, our mission is to position India as a Frontier Tech Nation," Ghosh writes. "We actively engage with experts to build deep insights and accelerate India's readiness in emerging technologies – fostering innovation, driving adoption, and ensuring economic and societal progress."

26. Space-Based Quantum Key Distribution: A Deep Dive Into QKD's Market Map And Competitive Landscape

by Matt Swayne
https://thequantuminsider.com/2025/03/05/space-based-quantum-key-distribution-a-deep-dive-into-qkds-market-map-and-competitive-landscape/?utm_source=resonance-newsletters.beehiiv.com&utm_medium=newsletter&utm_campaign=the-quantum-insider-weekly-d-wave-makes-waves-nist-s-back-up-algorithm-and-more-news&_bhlid=f30b6cb606dc5905e6be8a93d9310411cd8789fa

Quantum Key Distribution (QKD) is emerging as a foundational technology for secure communication in the quantum era, according to a new report and market map from Space Insider. Unlike conventional encryption, which faces vulnerabilities against quantum computing attacks, QKD ensures data security by leveraging quantum mechanics to detect eavesdropping attempts.

While terrestrial QKD has seen successful deployments over fiber networks, its range is inherently limited. To overcome these constraints, space-based QKD leverages satellites to establish long-distance quantum-secure communication channels, enabling global encryption without relying on trusted relay nodes.

According to *Space Insider*, space-based QKD is at a critical juncture, transitioning from experimental validation to early-stage commercialization. Their latest Space-Based QKD Market Map identifies key players, tracks emerging technologies, and outlines investment opportunities, offering a comprehensive view of the market's trajectory. Additionally, *Space Insider* has released a detailed report analyzing the sector's technology trends, competitive landscape, and projected market size.

Progress and Challenges in Space-Based QKD

Since China's *Micius* satellite demonstrated quantum key distribution over 7,800 km in 2016, governments and commercial players have intensified development efforts. Notable advancements include:

- **ESA's EAGLE-1 Mission**, set to commence European trials in 2025.
- **China's continued leadership**, with multiple QKD satellite launches scheduled this year.
- **NASA and DARPA's quantum-secure communication research**, laying the groundwork for future networks.
- **SealSQ's planned launch of six QKD satellites in 2025**, marking a significant commercial milestone.
- **Canada's first QKD demonstrator**, adding to the expanding global ecosystem.

Despite these advances, commercial adoption of space-based QKD remains limited. High infrastructure costs, complex deployment requirements, and relatively low technology readiness levels (TRLs) have slowed its expansion into the private sector. While terrestrial QKD benefits from existing fiber-optic networks, space-based systems require dedicated satellites, ground stations, and advanced quantum payloads, making them a costly investment.

According to *Space Insider*, widespread commercial adoption of space-based QKD is unlikely before 2035, with government and defense sectors continuing to dominate investment throughout the next decade.

QKD vs. Post-Quantum Cryptography: A Coexisting Future

The cybersecurity community remains divided on the best approach to counter quantum threats. Two competing solutions are at the forefront:

- **Quantum Key Distribution (QKD)**: Provides physically unbreakable security by enabling the detection of eavesdropping attempts but requires a dedicated quantum communication channel.
- **Post-Quantum Cryptography (PQC)**: A software-based alternative that integrates into existing networks but lacks eavesdropping detection.

Both technologies are expected to coexist, with QKD reserved for ultra-sensitive applications in diplomacy, national security, and financial transactions, while PQC provides a more scalable yet less inherently secure solution.

Market Growth and Competitive Landscape

Despite technical and adoption hurdles, space-based QKD is projected to experience steady growth. The market is expected to expand from $500 million in 2025 to $1.1 billion by 2030, representing a compound annual growth rate (CAGR) of 16%, driven primarily by government-backed initiatives. Cumulative investments in secure global communication infrastructure are estimated to reach $3.7 billion by 2030.

Key market drivers identified by *Space Insider* include:

- **National Security Imperatives**: Over 60% of general QKD demand between 2025 and 2030 is projected to come from government, defense, and diplomatic sectors.
- **Growing Cybersecurity Threats**: The rise of quantum computing necessitates secure encryption methods, particularly for critical infrastructure and intelligence operations.
- **Government-Funded Demonstrations**: Major space agencies—including ESA, NASA, and China's CNSA—are actively funding QKD research and demonstration missions.

However, commercial adoption will remain limited until post-2035, as technology matures and deployment costs decrease.

The Technology Landscape: QKD System Architecture

A typical space-based QKD system consists of:

- **Quantum Payload**: Single-photon sources, polarization encoders, and entanglement-based transmitters.
- **Secure Communication System**: Adaptive optics, large-aperture telescopes, and quantum random number generators.
- **Ground Station Infrastructure**: Optical receivers, analyzers, and conventional communication links for key validation.

Among various QKD protocols, the BB84 protocol remains the most widely used due to its relative simplicity, while entanglement-based QKD (E91, BBM92) provides higher security but is more complex and costly. A hybrid approach using Measurement-Device-Independent QKD (MDI-QKD) is emerging as a practical solution to eliminate detection-device vulnerabilities.

Industry Leaders in Space-Based QKD

The space-based QKD sector remains in its early stages, with most players focused on technology development and demonstration. *Space Insider*'s market map tracks 40 companies actively working on space-based quantum security solutions, including:

- **SealSQ**: Launching six satellites in 2025 to drive commercial adoption of quantum-secure communications.
- **ColdQuanta (Infleqtion)**: Specializing in cold atom quantum technology with a history of space-based deployments.
- **SpeQtral**: Developing satellite-based QKD solutions with government and commercial partnerships.
- **evolutionQ**: Advancing quantum-safe cybersecurity tools and space-based QKD networks.
- **Antaris**: Partnering with quantum security firms to develop QKD-enabled satellite software.

While China leads in operational space-based QKD systems, North America and Europe are working to close the gap through increasing public and private sector investment.

Strategic Considerations and Investment Outlook

For companies evaluating entry into the space-based QKD market, key considerations include:

- **Infrastructure Costs**: Deploying quantum satellites and upgrading ground stations require significant upfront capital.
- **Regulatory and Compliance Factors**: National security concerns could restrict commercial operations or impose compliance burdens.

- **Technology Maturity Timelines**: Companies investing now may not see substantial returns until after 2035, when commercial use cases become viable.

While long-term profitability remains uncertain, early-stage players stand to benefit from government contracts, research grants, and public-private partnerships.

The Space Insider Space-Based QKD Market Map

Space Insider has developed a market map highlighting 33 pioneering companies across the QKD ecosystem, covering:

- **QKD Satellite Technology & Components** – Spaceborne quantum cryptography systems and secure communication payloads.
- **Ground-Based QKD Infrastructure** – Optical ground stations and quantum-compatible communication networks.
- **QKD Network Deployment & Simulation** – Large-scale implementation strategies for quantum-secure networking.
- **Quantum Cryptography & Security Mechanisms** – Quantum-resistant encryption and security layers ensuring robust data protection.

The Road Ahead

While commercial adoption of space-based QKD remains a long-term prospect, continued advancements in quantum communications are laying the groundwork for a future where unbreakable encryption becomes a global standard. For industry stakeholders, staying ahead in the QKD market requires a deep understanding of emerging technologies, strategic partnerships, and evolving investment landscapes.

The Space Insider Market Intelligence Platform provides a continuously updated analysis of this rapidly evolving sector. Our latest Space-Based QKD Market Map identifies key players, tracks emerging technologies, and outlines investment opportunities, offering an in-depth view of the market's trajectory. We have also published a comprehensive report analyzing technology trends, the competitive landscape, and market size of the space-based QKD sector.

For a complete space-based QKD deep dive, please head to *Space Insider*.

27. The Coming Quantum Boom: A New Industry a Century in the Making

by HARRY GOLDSTEIN
https://spectrum.ieee.org/quantum-mechanics

Why build an industry around a scale that cuts across established verticals? This question occurred to me on a long flight to Paris, to attend the opening ceremony of the 2025 International Year of Quantum Science and Technology (IYQ), at UNESCO headquarters last month. I was part of an IEEE delegation led by 2025 IEEE President Kathleen Kramer. The event celebrated the 100th anniversary of several seminal quantum-science publications, including Wolfgang Pauli's paper on his exclusion principle; Werner Heisenberg's "Quantum-theoretical Re-interpretation of Kinematic and Mechanical Relations," the first mathematically consistent formulation of quantum mechanics; and Max Born's and Pascual Jordan's treatise on matrix mechanics in "On Quantum Mechanics."

That Paris event made me realize that quantum engineering has evolved very differently from, say, nanotechnology. In the early 2000s, governments around the world launched initiatives to nurture the nascent field of nanotechnology. Fast-forward two decades and nanotechnology has essentially been absorbed into verticals like semiconductors, advanced materials, and drug delivery. Like Bill Joy's infamous gray goo, a silo-busting "nanotechnology industry" never materialized.

The quantum regime, however, is already its own thriving industry, perhaps because the science of it is so unique. Quantum engineering involves math and phenomena that are fundamentally different from the classical physics engineers have so successfully exploited up to now. And many quantum technologies are aimed at doing things that otherwise couldn't be done at all. For instance, quantum cryptography is a completely different way of encrypting messages that uses quantum entanglement, which has no classical analogue.

As Contributing Editor Edd Gent reports in "The Future of Quantum Computing Is Modular," companies like Xanadu, IonQ, IBM, and Weling are scaling up quantum computers to tackle real-world problems that challenge conventional computers, like factoring large numbers and modeling the weather. Their approaches differ, but their goals are similar: to connect quantum processors in the same computer, data center, and among remote locations.

And then there are the quantum sensors based on defects in diamonds that Quantum Catalyzer is trying to commercialize. As CEO Amanda Stein tells *IEEE Spectrum* Associate Editor Dina Genkina in "5 Questions," those sensors could be used in extreme environments to "detect magnetic fields, temperature, pressure, potentially even gravity."

Regardless of their operating environment, all quantum tech must be fabricated in facilities that maintain exquisite control of temperature, vibration, and electromagnetic effects, and they are staffed by

multidisciplinary teams of quantum engineers and electrical engineers. The skill sets that quantum employers seek go well beyond traditional EE training. While many EEs have a basic understanding of quantum mechanics, the quantum engineers I talked to in Paris were adamant that EEs looking to make a quantum leap, as it were, need to understand quantum mechanics at a deep level. It doesn't hurt to also be familiar with superconductivity or be handy with laser control systems.

According to IEEE Life Member Hausi A. Müller, professor of computer science at the University of Victoria, B.C., and chair of the IEEE Quantum Technical Community, the need for EEs with quantum chops will likely grow at an accelerated pace in the near term, as funding from governments seeking a quantum advantage in cryptography pours into startups and established companies alike.

Whether you're already deep in the weeds or just quantum-curious, you can seek out opportunities for learning and networking with the world's top quantum engineers and scientists at this year's IEEE Quantum Week, 31 August to 5 September in Albuquerque.