Crypto News

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

February 04, 2025

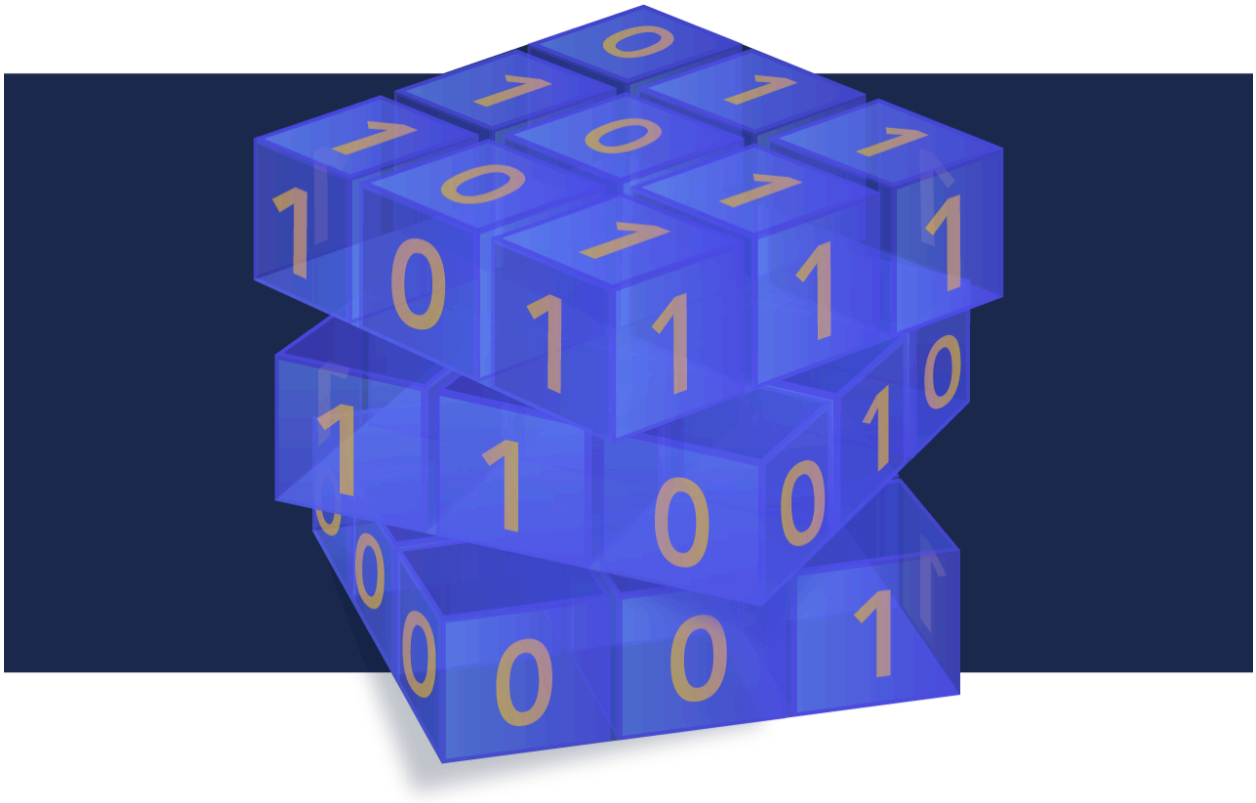


Table of Contents

Editorial

Dear readers,
Welcome to your monthly supply of CryptoNews, brought to you by Dhananjoy and the QSS group.

This month, we revisit the controversy about the expected arrival time of a useful quantum computer. Last month, Jensen Huang, CEO of Nvidia predicted between 15 to 30 years. This month (see [28]) reputed crypto expert Bruce Schneier stated that it "always remains 10 years in the future, which means that no one has any idea". Both predictions are in contradiction to what we can see in this newsletter. [6], which depicts the rapid progress Google's Willow chip, ends on an optimistic note: "In another five years, fault tolerance will be a lot closer. And useful commercial quantum applications in some form or another should be quite doable". In fact, as assessed in [11], "Useful quantum computing is inevitable—and increasingly imminent". There is speedy progress on all fronts, hardware, error correction and software, as seen in [8], [9], [30] and [33], with [35] presenting an interesting "who's who" on quantum computing, with another optimistic end: "As investments pour in and innovations continue, the future of quantum computing looks brighter than ever."

Fortunately, progress on the quantum-safe front is also forthcoming, as seen for example in [5], [24], where Microsoft advocates getting Quantum-Ready, and [32]. Another news close to my heart (disclaimer: I am working at ID Quantique) is [17], the first delivery of a national security certification for a QKD product. The quantum computer may be arriving faster than we expected, but we are getting ready.

Have an interesting read!

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. Both are active members of the CSA QSS WG. The guiding principle of the QSS WG is to address key generation and transmission methods and to help the industry understand quantum-safe methods for protecting their networks and their data.

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

1. South Korea announces winners of KpqC competition

https://pqshield.com/south-korea-announces-winners-of-kpqc-competition/?utm_campaign=PR%20Social%20Amplification&utm_content=323379062&utm_medium=social&utm_source=linkedin&hss_channel=lcp-11835470

This month, South Korea selected its final four algorithms as part of the Korean Post-Quantum Cryptography (KpqC) competition.

The competition, running since 2021, was designed to standardize algorithms for use in the nation's cryptography, in accordance with the country's PQC master plan, published in 2023.

As with many nations, South Korea has been making considerable effort to transition its cryptography to PQC to safeguard against the quantum threat. This step is a key milestone, coming as it does at the end of a four-year project, initially launched by the National Intelligence Service (NIS) in collaboration with the National Security Research Institute (NSR).

We've summarized the four selected algorithms below.

Digital Signatures

- **HAETAE.** HAETAE is a close variant of ML-DSA (Dilithium) that uses a more complex but also more efficient technique when it comes to rejection sampling. As a result, it achieves more compact signatures.

- **AIMer.** AIMer is a digital signature algorithm with much larger signature sizes than NIST-standardized ML-DSA, comparable with SLH-DSA in terms of performance. It runs more slowly than lattice-based schemes. It is based on the recent "MPC-in-the-head" design.

PKE/KEMs

- **SMAUG-T.** Comparable with ML-KEM (Kyber), SMAUG-T relies on the same Module Learning With Errors assumption with some small differences. It's generally considered equally as secure as ML-KEM and exhibits a similar performance.

- **NTRU+.** NTRU was originally a NIST finalist, but was not selected as a KEM, being surpassed by ML-KEM (Kyber) during the standardization project. NTRU+ can be similarly efficient but can also mean more complicated implementations.

Further afield?

Naturally, this announcement raises the profile of these schemes. However, it will be intriguing to see their reception outside of South Korea. Since many 'ingredients' of these algorithms differ in terms of implementation, a large amount of development effort is needed to use them in implementations, such as those offered by PQShield. However, it's encouraging to see standards develop.

At PQShield we're focused on *implementation* as well as ground-breaking research, but particularly with an eye on physical threat detection; it's worth pointing out that these schemes have yet to be tested or evaluated against the threat of side-channel analysis – and this matters. Even with the current NIST candidates, we regularly observe new attacks, despite the fact that those standards have been rigorously studied and robustly tested for a number of years. It's a pertinent threat for standards of all levels of maturity.

It's great to observe the progress made by South Korea on PQC standardization, particularly as the roadmap set out by the NIS is on schedule for transition by 2035. It aligns with European and US timescales, which is certainly a positive. In the NIS Roadmap, the next phase for South Korea is a focus on 'establishment of procedure' and from 2026, 'supporting systems for cryptography transformation'.

In this year of PQC adoption around the world, there will be many governments and organizations now planning on the transition to crypto agility, with the latest PQC algorithms in place.

2. Hack-Proof Encryption: How AI and Holograms Are Making Data Unbreakable

by OPTICA
https://scitechdaily.com/hack-proof-encryption-how-ai-and-holograms-are-making-data-unbreakable/

By combining AI with holographic encryption, scientists have developed an ultra-secure data protection system.

Their method scrambles laser beams into chaotic patterns, making decryption impossible without a trained neural network. This innovation could revolutionize cryptography.

Holograms for Next-Level Encryption

As the demand for digital security grows, researchers have developed a new optical system that uses holograms to encode information, creating a level of encryption that traditional methods cannot penetrate. This advance could pave the way for more secure communication channels, helping to protect sensitive data.

"From rapidly evolving digital currencies to governance, healthcare, communications, and social networks, the demand for robust protection systems to combat digital fraud continues to grow," said research team leader Stelios Tzortzakis from the Institute of Electronic Structure and Laser, Foundation for Research and Technology Hellas and the University of Crete, both in Greece. "Our new system achieves an exceptional level of encryption by utilizing a neural network to generate the decryption key, which can only be created by the owner of the encryption system."

Revolutionizing Cryptography with AI

In *Optica*, Optica Publishing Group's journal for high-impact research, Tzortzakis and colleagues describe the new system, which uses neural networks to retrieve elaborately scrambled information stored as a hologram. They show that trained neural networks can successfully decode the intricate spatial information in the scrambled images.

"Our study provides a strong foundation for many applications, especially cryptography and secure wireless optical communication, paving the way for next-generation telecommunication technologies," said Tzortzakis. "The method we developed is highly reliable even in harsh and unpredictable conditions, addressing real-world challenges like tough weather that often limit the performance of free-space optical systems."

Scrambling light for security

The researchers developed the new system after discovering that when holograms are used to encode a laser beam, the beam would become completely and randomly scrambled and that the original beam shape could not be recognized or retrieved using physical analysis or calculation. They recognized that this was an ideal way to safely encrypt information.

"The challenge was figuring out how to decrypt the information," said Tzortzakis. "We came up with the idea of training neural networks to recognize the incredibly fine details of the scrambled light patterns. By creating billions of complex connections, or synapses, within the neural networks, we were able to reconstruct the original light beam shapes. This meant we had a way to create the decryption key that was specific for each encryption system configuration."

High-Powered Lasers and Ethanol Magic

To create a physical system that completely and chaotically scrambles light beams, the researchers used a high-power laser interacting with a small cuvette filled with ethanol. The liquid was not only inexpensive but also created the desired chaotic behavior within a short propagation distance of just a few millimeters. In addition to changing the light beam intensity, light that interacted with the liquid also exhibited thermal turbulence that strongly enhanced the chaotic scrambling.

Successful Encoding and Decoding

To demonstrate the new method, the researchers applied it to encrypt and decode thousands of handwritten digits and other shapes like animals, tools and everyday objects from well-established databases used as references for evaluating image retrieval systems. After optimizing the experimental procedure and training the neural network, they showed that the neural network could accurately retrieve the encoded images 90-95% of the time. They say that this rate could be further improved with more extensive training of the neural network.

The Future of Ultra-Secure Communications

The researchers plan to further develop the technology by adding additional levels of protection such as two-factor authentication. Since the biggest hurdle to commercializing the system is the cost and size of the laser system, they are also investigating cost-effective alternatives to expensive, bulky high-power lasers.

3. Post-Quantum Cryptography Alliance Brings Accelerated Computing to Post Quantum Cryptography with NVIDIA cuPQC

by Noah Lehman
https://www.linuxfoundation.org/press/post-quantum-cryptography-alliance-brings-accelerated-computing-to-post-quantum-cryptography-with-nvidia-cupqc

The Post-Quantum Cryptography Alliance (PQCA), a part of the Linux Foundation, today (29 Jan 2025) announced that its open source project, Open Quantum Safe (OQS), now integrates the NVIDIA cuPQC library to support and encourage the transition to quantum-resistant cryptography.

By leveraging cuPQC's functionality within its LibOQS library, the Open Quantum Safe Project can provide users GPU-accelerated implementations of cryptographic primitives that are safe against attacks from future quantum computing technology – which threaten to crack other commonly used cryptosystems.

Although quantum computing is still in its early stages, post-quantum cryptography (PQC) is a pressing challenge, as `harvest now, decrypt later' attacks hoard today's sensitive and poorly protected data, with the aim of decrypting it using future quantum devices. This highlights the pressing need to adopt quantum-secure cryptographic primitives, a challenge compounded by the lack of secure, fast, and flexible implementations of key PQC algorithms.

"Ensuring adoption of post-quantum cryptography is one of the most pressing issues in data security", said Hart Montgomery, CTO of LF Decentralized Trust. "Working with NVIDIA to integrate cuPQC into LibOQS is a huge move towards meeting this challenge."

New PQC standards mean that large ISP, SCP, and NSP enterprises must be able to perform millions of cryptographic operations every second in order to remain secure. Previous CPU-based implementations have been limited to performing tens of thousands of operations per second, whereas cuPQC is able to perform over a million.

Through cuPQC, LibOQS will provide GPU-accelerated implementations of NIST-approved ML-KEM and ML-DSA cryptographic primitives. Tailored for GPU hardware, these implementations offer hardware-level security, speed through parallelized algorithms, and 'crypto-agility' – the ability to easily switch in new algorithm developments through their seamless integration at the software-level.

"cuPQC's exceptional performance enables security frameworks to bring practical Post Quantum Cryptography to data-intensive environments," said Tim Costa, Senior Director of CAE, Quantum and CUDA-X at NVIDIA. "cuPQC's integration with liboqs is a crucial step toward widespread adoption of Post Quantum Cryptography"

By leveraging cuPQC, LibOQS now supports applications with high throughput requirements, such as TLS offloading, cryptographic key generation and management, batched signature verifications and many other tasks essential by large-scale users such as data centers and cloud service providers.

The integration also enables the cryptographic research community, ensuring they have access to the powerful tools needed for developing future iterations of quantum-resistant cryptographic protocols.

Open Quantum Safe is a project within the Linux Foundation's PQCA, which aims to facilitate a smoother migration to PQC for industry users. The new functionality in LibOQS is now publicly available to all users. To learn more about Open Quantum Safe and the PQCA, please visit https://pqca.org/.

4. Build a Perfect Cryptographic Machine

by STEPHEN CASS
https://spectrum.ieee.org/diy-one-time-pad-machine

Like many nerds, I have an interest in cryptography rooted in the wartime exploits of codebreaker and *Ur*-computer scientist Alan Turing. So I've followed with interest *IEEE Spectrum's* reporting on the burgeoning field of postquantum cryptography. These techniques are designed to frustrate even the immense potential of quantum computing, a technology light-years beyond the electromechanical bombe that Turing used to break the German Enigma cipher. I'm sure those new cryptographic methods will work just fine. But there is one encryption scheme, known even in Turing's time, that is mathematically

secure against not just quantum computers but *any* computer that will ever be invented: the one-time pad.

A one-time pad is a series of random letters or numbers—typically 250 digits. The sender and receiver each have a copy of the pad, which is used for both encryption and decryption, following some simple but strict rules for pen and paper. It's a cipher in which the key changes in an utterly unpredictable way after each character. Without predictability, there's nothing for an attacking computer to get its teeth into.

However, even the most junior codebreaker in possession of two messages encrypted with the same pad would be able to strip off the encryption and read both. It's therefore critical to destroy each pad after you've used it. And it's a bad idea to store the pad on a thumb drive or something similar, because computers and storage devices have a habit of leaving residues of data around, even after the data has been officially deleted.

The one-time pad comes with some other significant limitations. The digits have to be *truly* random—the numbers generated by the pseudo-random algorithms typically used by computers won't cut it. And because you can use a given pad only once, you need a whole bunch of them if you want to send more than a single message. Plus, the pads need to be physically printed and shared by hand—you can't send them over a network.

I decided to build a machine that makes dealing with those problems a little easier. My Pad-O-Matic is built around a CSN-A2 thermal receipt printer I'd bought on a whim a few years back. The printer is connected to the most transparent technology stack I could find: a tortured transistor, a few logic chips, and a microcontroller with about 200 lines of my code. This code does nothing more complicated than division, because if I've learned one thing about cryptography, it's that unless you really know what you're doing, trying to be a clever clogs is a recipe for failure. The Pad-O-Matic is completely stand-alone.

The thermal receipt printer in the Pad-O-Matic lets me print a whole series of pads. I still have to physically share the pads, but at least they're in a compact roll. My correspondent and I can then tear off and destroy each pad after it's been used.

I still needed a good source of randomness—some fundamentally unpredictable physical process to convert into equally unpredictable bits. Fortunately, that problem was already solved for me. I found a neat little battery-powered circuit from *Make:* magazine that relies on the electrical noise produced by forcing electrons the wrong way across a transistor's base and emitter terminals while leaving the collector terminal unconnected. *Make:*'s generator is a simplified version of a circuit by Aaron Logue, but *Make:* fortunately has a copy of the original schematic. This uses 12 and 5 volts instead of the 18 and 5 volts used by *Make:*'s version, so I could use an old power supply I had that also provides enough extra current to drive the thermal printer. The original circuit also has two nice additional features for the cost of a few extra chips.

The first feature is a clean microcontroller interface. It sends one byte at a time in parallel, alerting the microcontroller every time a new byte is available. An alert is needed because the length of time needed

to generate a random byte varies slightly due to the other nice feature: automatic *debiasing*, using four flip-flops and an XOR gate. Debiasing means that even if the electrical-noise generator tends toward, say, more 0s than 1s, the final output will be statistically balanced.

For my microcontroller, I finally got to use an Arduino Uno R4 Minima. Although this latest version of the beloved Uno came out about 18 months ago, I hadn't found a project that needed it—until now. Its bigger memory—32 kilobytes of RAM versus 2 KB in the Rev3—is essential, because the Pad-O-Matic has to generate an entire series of pads—50 in my case—and hold it in memory. With 250 digits per pad, that requires over 12 KB. As the digits live only in RAM, there's no risk of them leaving any trace of themselves behind.

The microcontroller produces digits from the incoming random bytes by first throwing away any byte with a value over 250. Then it performs modular division by 10 on each remaining byte, leaving digits in the range of 0 to 9.

I chose 50 pads per series, even though I had the memory for more, because I actually have to print one series to keep and a copy to share, and then generate and print another series and its copy: The first series is for sending messages from me to my secret correspondent, and the second series is for them to send messages to me. This eliminates the risk of accidentally using the same pad when messages cross each other. A total of 100 pads just about uses up one roll of thermal paper.

I put the whole thing in a wooden enclosure, and presto! At the press of a button, the Pad-O-Matic whirs into life, spitting out perfect—and now marginally more convenient!—cryptographic security.

5. How quantum cryptography is leveraging principles of quantum mechanics to secure data to prevent financial frauds

by Abhinav Singh
https://www.theweek.in/news/sci-tech/2025/01/29/explained-how-quantum-cryptography-is-leveraging-principles-of-quantum-mechanics-to-secure-data-to-prevent-financial-frauds.html

In recent years, India has been witnessing a major surge in digital payment frauds. According to data from the Reserve Bank of India (RBI), the total value of digital payment frauds escalated to Rs 14.57 billion in the fiscal year ending March 2024, marking a more than five-fold increase from the previous year. Besides, a survey by US-based data analytics company FICO revealed that over 34% of respondents in India reported losing money to scams via real-time payments. Notably, while fewer consumers reported losses in 2024 compared to 2023, the percentage of high-value losses (those exceeding Rs 8,00,000) doubled.

In addition to this, a report by BioCatch indicated a 101% increase in reported fraud volumes in the first five months of 2024 compared to the same period in the previous year. Up to 40% of these reported frauds were categorised as voice scams, underscoring the evolving tactics of fraudsters.

Such statistics underscore the pressing need for enhanced security measures and increased user awareness to combat the rising tide of digital payment frauds in India. Newer technologies such as quantum cryptography leverages principles of quantum mechanics to secure data.

"Unlike classical cryptography, which relies on mathematical complexity, quantum cryptography uses the fundamental laws of physics. A primary example is Quantum Key Distribution (QKD), which enables two parties to generate a shared, secret key. Any attempt by an eavesdropper to intercept the key alters the quantum states, revealing the intrusion and ensuring the integrity of the communication," explained Dharshan Shanthamurthy, CEO of Bengaluru-headquartered firm SISA, which offers forensic-driven cybersecurity solutions for the digital payments industry.

Shanthamurthy noted that the integration of quantum cryptography into digital payment systems can address several security challenges.

"Quantum cryptography provides security based on physical laws rather than computational assumptions, making it resistant to current and future computational attacks, including those from quantum computers. As quantum computing advances, traditional cryptographic methods become vulnerable. Quantum cryptography, particularly QKD, ensures that any interception attempt is detectable, safeguarding data against both classical and quantum attacks. QKD facilitates the secure distribution of cryptographic keys, a critical component in digital payment security. This ensures that encryption keys remain confidential and integral, preventing unauthorised access and fraudulent transactions," he said.

Implementing quantum cryptography in digital payments involves integrating QKD systems with existing payment infrastructures. This requires the development of quantum networks capable of transmitting quantum keys over distances relevant to financial transactions.

Additionally, payment protocols must be adapted to incorporate quantum-generated keys, ensuring compatibility and seamless operation. Broadly quantum mechanics provides a level of security that is fundamentally resistant to both current and emerging threats, ensuring the integrity and trustworthiness of digital financial transactions.

Recently SISA launched Post-Quantum Cryptography services to secure digital payments. The aim has been to give industry support to the government's quantum mission. "The UNGA (United Nations General Assembly) has announced the year 2025 as the year of International Quantum Science, this initiative by SISA is also in line with the government of India's national quantum mission to increase the skill resources in quantum technology."

"Quantum supremacy, the point where quantum computers surpass classical ones, is expected within the next five to ten years, with the quantum computing market forecast to reach $50 billion by 2030. These

advancements pose a critical threat to the digital payments ecosystem, as quantum technology risks rendering traditional encryption methods like RSA, ECC, and DSA obsolete, leaving sensitive data and financial transactions exposed. Despite the growing urgency, many organisations remain uncertain about whether to invest and how to prepare for a quantum-secure future," remarked Shanthamurthy.

6. Google's 105-Qubit Willow Chip Achieves Major Quantum Milestones

by Paul Smith-Goodson
https://www.forbes.com/sites/moorinsights/2025/01/28/googles-105-qubit-willow-chip-achieves-major-quantum-milestones/

Google has chalked up several amazing quantum computing records with its newest quantum 105-qubit superconducting chip called Willow. This performance is no surprise, considering Google's heritage of record-setting quantum chips, reaching back to Foxtail in 2017, Bristlecone in 2018 and Sycamore in 2019.

Google announced Willow last month, and I think it is necessary to reemphasize the importance of this research after Jensen Huang, CEO of Nvidia, recently remarked that quantum computing likely won't be useful for another 20 years. Granted, there remains a lot of ground to cover to reach fault tolerance, which will be critical for many practical applications, but there has also been a lot accomplished in quantum in just the past 12 months. Marketplace evidence, research results (including qubit fidelity close to what is needed for fault tolerance) and the roadmaps of many quantum computing companies indicate that useful quantum technology is much closer than Huang believes.

Read on for more on how the new Willow chip performed on the random circuit sampling benchmark. I also discuss what may be the most important piece of this development for future quantum fault tolerance, the results of applying a new error-corrected surface code. To provide more context, I'll also share a historical perspective from Professor John Martinis, who led some of the most important work on earlier generations of Google's quantum chips, and how his work has now paid off – just as he predicted – with Willow.

Willow Hardware And Software Improvements

Willow System Metrics	
Number of qubits	105
Average connectivity	3.47 (4-way typical)
Quantum Error Correction (Chip 1)	
Single-qubit gate error[1] (mean, simultaneous)	0.035% ± 0.029%
Two-qubit gate error[1] (mean, simultaneous)	0.33% ± 0.18% (CZ)
Measurement error (mean, simultaneous)	0.77% ± 0.21% (repetitive, measure qubits)
Reset options	Multi-level reset (|1⟩ state and above) Leakage removal (|2⟩ state only)
T_1 time (mean)	68 µs ± 13 µs[2]
Error correction cycles per second	909,000 (surface code cycle = 1.1 µs)
Application performance	$\Lambda_{3,5,7} = 2.14 \pm 0.02$
Random Circuit Sampling (Chip 2)	
Single-qubit gate error[1] (mean, simultaneous)	0.036% ± 0.013%
Two-qubit gate error[1] (mean, simultaneous)	0.14% ± 0.052% (iswap-like)
Measurement error (mean, simultaneous)	0.67% ± 0.51% (terminal, all qubits)
Reset options	Multi-level reset (|1⟩ state and above) Leakage removal (|2⟩ state only)
T_1 time (mean)	98 µs ± 32 µs[2]
Circuit repetitions per second	63,000
Application performance	XEB fidelity depth 40 = 0.1%
Estimated time on Willow vs classical supercomputer	5 minutes vs. 10^{25} years

[1] Operation errors measured with randomized benchmarking techniques and reported as "average error"

[2] Chip 1 and 2 exhibit different T_1 due to a tradeoff between optimizing qubit geometry for electromagnetic shielding and maximizing coherence

Willow has improved on earlier generations of Google's quantum chips in several ways. For starters, the use of tunable qubits and couplers in Willow has provided it with much faster gates and operations that help achieve lower error rates. This speed also allows hardware to be optimized or adjusted during operation. Variances in superconducting qubits can sometimes create high error rates, but tuners allow nonconforming qubits to be reconfigured and aligned with other qubits to eliminate errors.

Next up is the duration of quantum states. A major limitation of quantum computing has been the length of time qubits can maintain their quantum states. Willow has increased that time by 5x, from 20 microseconds to 100 microseconds. This allows more complex problems to be run.

A third advantage of Willow is that Google's logical qubits can now function below the critical quantum error correction threshold. The QEC threshold arises from a theory developed in the 1990s, and until now it has been a barrier to efficient quantum computing. In the Willow chip, however, error rates are reduced by one-half as physical qubits are added in scale. Thanks to this, as Google increases the size of its surface code from 3x3 to 5x5 to 7x7 the encoded logical qubits maintain their coherence for longer times. Increasing grid size allows for more complex error patterns to be corrected, similar to more redundancy in classical error correction. It also means that logical qubits can maintain their quantum states longer than the underlying physical qubits.

This leads me to the single most important part of Google's Willow announcement: Willow is the first quantum processor to demonstrate an exponential reduction in error rates as the number of qubits is increased. Traditionally, adding qubits causes the error rate to increase.

Other factors necessary for fault-tolerant quantum computing have also been demonstrated by Google researchers. For one thing, having a repeatable performance over several hours without degradation is needed to run large-scale fault-tolerant algorithms – and Willow has now demonstrated that capability.

Benchmarking Quantum Processors

Google uses random circuit sampling as an ongoing benchmark to compare new experimental quantum processors against supercomputers running classical algorithms. It is important to point out that random circuit sampling is not useful as an application in itself; it is only a threshold test. But if a system fails to pass RCS, there is no need for further testing.

Five years ago, the Google quantum research group claimed that the 53 superconducting qubits of its 54-qubit Sycamore chip (one qubit was faulty) had achieved quantum supremacy – meaning that it outperformed comparable classical computing. Back then, Google researchers said they were able to complete a RCS benchmark computation in 200 seconds that theoretically would take a classical supercomputer 10,000 years to complete. IBM disputed the claim using calculations indicating it was possible for a classical computer to achieve the same results. However, it was eventually accepted by the quantum community that if Google had used all 54 qubits, it would have taken a classical supercomputer much longer than 10,000 years to equal Sycamore's achievement.

This year, in another quantum supremacy test, Google pitted the new 105-qubit Willow chip against the same RCS benchmark experiment that the Sycamore chip ran in 2019. Willow ran the RCS benchmark in under five minutes; it has been determined that today's best classical supercomputer would need 10 septillion years to run the same benchmark (that's a 1 followed by 25 zeros). In short, because Willow performs below the error correction threshold, it is able to conduct random circuit sampling far beyond what is possible with classical computers.

If you're not familiar with quantum computing, these comparisons may seem confusing at first. But they are directly attributable to the number of qubits involved. The Willow chip has 105 qubits compared to Sycamore's 53. Each additional qubit results in an exponential increase in computing power, not a linear increase. The difference in the execution time between the tests in 2019 and the ones conducted in recent months today becomes understandable in this context. Because Willow has 52 more qubits than Sycamore, it has 2^52 (4.5 quadrillion) more computational states.

Besides the increase in qubits, many other improvements have been made to quantum systems since 2019. Algorithms are a billion times better because of extensive experimentation by the large community of computer scientists in the ecosystem. Plus, quantum processors have improved significantly in various ways, including in the quality of qubits.

Following its 2019 benchmark results, Google published a road map with a 10-year timeline for developing a large error-corrected quantum computer with 1,000 logical qubits using 1,000,000 physical qubits. As shown in the diagram above, the roadmap has six milestones; after its latest achievement with Willow, Google is now approaching the third milestone.

For another perspective on the Willow chip, I recently discussed Google's achievement with Prof. John Martinis, who led the Google team that designed and tested the Sycamore chip. Prof. Martinis is currently working on a quantum startup called Qoloab with his cofounders Alan Ho (another Google veteran) and Prof. Robert McDermott.

During that conversation, I recalled remarks that Prof. Martinis made about a yet-to-be-developed quantum computer chip for a Forbes article I published nearly five years ago. "Google's plan is roughly to build a million-qubit system in about 10 years, with sufficiently low errors to do error correction," he said. "Then at that point you will have enough error-corrected logical qubits that you can run useful, powerful algorithms that you now can't solve on a classical supercomputer. And maybe even at a few hundred qubits, with lower errors, it may be possible to do something special-purpose."

Those remarks are very close to describing how Google's Willow chip has actually played out.

How Long Until We See Commercial Quantum Applications?

Google currently believes that it will be able to produce useful commercial quantum applications in the next five years or less. Many quantum scientists believe it will take at least another decade before quantum computers are able to handle world-affecting computations in areas such as climate change, drug discovery, materials science and financial modeling.

Of course, Google is not the only company on this path. There is a great deal of experimentation and collaboration being done with logical qubits. One notable example is Microsoft, which has done exciting work with both Quantinuum's H-2 trapped-ion processor and Atom Computing's neutral-atom processor.

Google acknowledges there are many challenges remaining. While the maximum code distance used in the Willow research was 7, to obtain the necessary error rate for fault tolerance would require a distance-27 logical qubit, which would need almost 1,500 physical qubits to create it. For quantum error correction, a higher distance means that an error code can handle more errors before it fails. A larger distance means the code has more layers of checks and balances that can detect and repair errors before they cause problems.

That is just one of the many challenges that must be overcome to achieve fault tolerance. While some might believe Google's timeline is overly optimistic, I believe the company is on track. In another five years, fault tolerance will be a lot closer. And useful commercial quantum applications in some form or another should be quite doable.

7. SoftBank, Quantinuum Forge Partnership to Make Quantum Computing Practical

by Matt Swayne
https://thequantuminsider.com/2025/01/28/softbank-quantinuum-forge-partnership-to-make-quantum-computing-practical/

SoftBank Corp. and Quantinuum announced a partnership to advance quantum computing into practical applications, including plans for a quantum data center. According to a joint statement, the collaboration will address AI's current limitations and enable next-generation solutions to complex problems.

The initiative, timed with the International Year of Quantum Science and Technology in 2025, aims to unlock business opportunities by combining AI and quantum computing capabilities, according to the statement. Both companies say that quantum computing, integrated with traditional computational

systems, can address challenges such as optimization problems, precise simulations, and uncovering causal relationships that remain unresolved by classical AI.

Ryuji Wakikawa, Head of Research Institute of Advanced Technology, SoftBank Corp., said in the statement, "SoftBank believes in the potential of quantum computers and has been testing and evaluating various internal issues using quantum computers, and has started to obtain certain results. However, as a telecommunications operator, there are still many challenges remaining regarding how to provide quantum computing services in Japan. Through our collaboration with Quantinuum, which possesses the world's highest-performance quantum computer hardware, we aim to be the first in the world to identify problems that can only be solved by quantum computers and look forward to significantly accelerating the practical application of quantum computing."

Dr. Rajeeb Hazra, President and CEO of Quantinuum described its collaboration with SoftBank as a significant milestone for quantum computing, emphasizing the potential to enhance AI capabilities and address longstanding challenges while paving the way for transformative applications across industries.

"Our partnership with SoftBank represents a pivotal moment in the evolution of quantum computing," said Hazra. "By combining our strengths, we are poised to unlock innovative solutions that will not only enhance the capabilities of AI but also tackle challenges that have long been beyond reach. Together, we are laying the groundwork for a future where quantum technologies drive transformative advancements across multiple industries."

QUANTUM COMPUTING'S POTENTIAL

AI has proven effective in solving many problems, but it struggles with tasks requiring the analysis of intricate systems or simulations at high precision. According to the statement, quantum processors could complement existing central and graphics processing units (CPUs and GPUs) in hybrid systems, extending the computational possibilities. Quantum technology's ability to solve specific problems in fields like quantum chemistry or network optimization could make it a critical source of innovation in those fields — and many more.

The partnership reflects the belief that the integration of quantum and classical technologies can open new avenues across industries, including machine learning, material design and communication networks.

Despite its potential, quantum computing faces significant hurdles that hinder its widespread application. The statement highlights several challenges, starting with the financial burden of quantum systems. High development and operational costs, combined with a lack of clear revenue models, discourage companies from adopting the technology.

To address these barriers, Quantinuum and SoftBank plan to explore strategies such as cost-sharing and revenue-sharing to mitigate these risks.

Another obstacle is the scarcity of well-defined use cases. While quantum computing promises to transform fields such as quantum chemistry and machine learning, many of its potential applications remain theoretical. The partnership seeks to identify specific areas where quantum computing can deliver tangible results, such as creating new optical switch materials for telecommunications or enhancing anomaly detection in communication networks.

Technical limitations also present challenges. Current quantum hardware, including the number of qubits and operational precision, falls short of what is required for practical use.

However, these challenges aren't intractable, the teams suggest. Advances in error correction and hybrid algorithms that combine quantum and classical methods are necessary to bridge the gap between experimental systems and real-world applications.

KEY FOCUS AREAS

The partnership will concentrate on two main objectives to accelerate the practical use of quantum computing.

First, the companies plan to develop a quantum data center that integrates CPUs, GPUs, and quantum processing units (QPUs). The Japanese market will serve as a testing ground for their global research, with a focus on creating viable business models for this advanced computing infrastructure.

According to the statement: "With a view toward the realization of a 'quantum data center' capable of performing advanced calculation processing by combining CPUs, GPUs and quantum computers (QPUs), both companies will use the Japanese market as a foothold to conduct global market research in the Asia-Pacific region and other regions, and explore specific business models based on that research."

Second, the collaboration aims to establish clear timelines for quantum applications. SoftBank will contribute business challenges as test cases to determine when specific quantum use cases might become commercially viable. These efforts will focus on areas such as quantum chemistry, where quantum computing could aid in material discovery, and network analysis, where it might improve fraud detection and network optimization.

BROADER IMPLICATIONS AND POSSIBILITIES

Zooming out, and taking some editorial license, there are important facets of this partnership that may rest beyond the tactical pieces of the announcement. For example, SoftBank is not only a globally respected corporation but is also renowned for its ability to identify and capitalize on emerging technological trends. The company is now using that sharp focus on emerging technologies to hone in on quantum computing – a move that shows Quantinuum and the industry's transformative potential and its readiness to shape future markets.

SoftBank's global expertise in AI also positions it as an ideal partner for driving this effort forward, while the announcement also is concrete proof of SoftBank's interest in quantum. SoftBank and Quantinuum would make powerful partners in realizing the vision of "Gen QAi," which could be brought together through a quantum supercomputing system combining high-performance computing (HPC), artificial intelligence (AI), and quantum processing units (QPUs).

As this signals that the integration of AI, HPC, and quantum computing is now moving beyond rhetoric, the collaboration provides a credible scaffolding for turning theoretical concepts into tangible advances.

Ultimately, this partnership also signals a broader trend of moving quantum computing from theoretical research to practical applications.

By addressing business and technical barriers together, SoftBank and Quantinuum hope to shorten the path to commercialization. Their combined efforts highlight the importance of aligning technological advancements with market needs to ensure quantum systems deliver real-world value.

8. Milestone in Quantum Computing Achieved

by OV Desk
https://observervoice.com/milestone-in-quantum-computing-achieved-91912/

Researchers have made significant strides in the field of quantum computing. They have successfully integrated 1,024 silicon-based quantum dots with both digital and analog on-chip electronics. This groundbreaking work operates at cryogenic temperatures, specifically below 1 Kelvin. This innovation is expected to propel the development of scalable quantum computing systems. For years, these systems have struggled to balance scalability, performance, and energy efficiency. The new integration method offers a promising solution to these challenges while remaining compatible with standard silicon manufacturing techniques.

System Combines Quantum Dots and On-Chip Electronics

A team of researchers from Quantum Motion in London, led by Edward J. Thomas and Virginia N. Ciriano-Tejel, conducted this pioneering research. Their findings were published in the journal Nature Electronics. The system they developed demonstrates the ability to connect room-temperature transistor behavior with the unique properties observed in cryogenic environments. This is a crucial advancement because it allows for the effective use of spin qubits within silicon quantum dots. These qubits are known for their high control fidelities, making them suitable for large-scale integration. The research paper highlights how this integration can bridge the gap between different operating conditions, which has been a significant hurdle in quantum computing development.

Key Role of Quantum Dots and Rapid Characterisation

The quantum dots utilized in this system are nanoscale structures specifically designed to trap and manipulate individual electrons. This capability is essential for the functioning of quantum computers. By incorporating these quantum dots into a high-frequency analog multiplexer, the researchers achieved rapid characterization of all 1,024 devices in under 10 minutes. This rapid assessment is made possible through the use of radio-frequency reflectometry, which ensures the integrity of the signals being measured. The study reports a remarkable signal-to-noise voltage ratio exceeding 75, achieved with an integration time of just 3.18 microseconds. This level of performance is critical for the reliable operation of quantum computing systems, as it allows for quick and accurate assessments of device functionality.

Implications for Cost-Effective Quantum Technology Development

The researchers employed automated machine learning tools to extract valuable parameters from the quantum dots. This approach provided insights into the performance and design of these devices. The use of machine learning is particularly beneficial as it helps researchers understand device variability and the factors that influence quantum dot yields. Notably, the study identified correlations between the performance of quantum dots at cryogenic temperatures and the behavior of transistors at room temperature. This discovery opens the door to more cost-effective optimization processes in quantum technology development.

As reported by phys.org, the implications of these findings are substantial. The researchers believe that their work could significantly reduce the cost and complexity associated with developing quantum technologies. If pre-cryogenic methods and process monitoring tools are refined further, the industry could see enhanced scalability and performance in quantum computing systems. This could lead to broader applications across various sectors, making quantum technology more accessible and practical for real-world use.

9. New chip to solve quantum computing roadblocks

by Wisse Hettinga
https://www.eenewseurope.com/en/new-chip-to-solve-quantum-computing-roadblocks/

The goal is to make quantum computers faster, more efficient, and scalable, enabling them to tackle challenges like drug discovery, cybersecurity, and AI

The European Commission is investing in a groundbreaking quantum chip that combines light and electronics for the first time, promising faster, more efficient quantum computers.

Supported by the Quantum Flagship, the ONCHIPS consortium is laying the foundations for a new type of quantum hardware with advanced materials that have never been combined before.

The team hopes to make quantum computers more practical for real-world applications and enable them to solve the most challenging problems we face in the world today– unlocking new possibilities for science, industry, and everyday users.

To make this vision a reality, the ONCHIPS consortium is turning to Germanium-Silicon (GeSi) – a material whose ability to efficiently emit light was only discovered in 2020.

Quantum computers are set to be exceptionally powerful tools for solving certain types of problems, like simulating molecules for drug discovery, optimising complex systems, or breaking encryption. However, researchers seeking to scale them up to the size face significant hurdles.

Just as the first computers of the 1950s were impractical and unsuitable for widespread adoption due to their enormous size and limited processing power, today's quantum computers have their own challenges, particularly with their fundamental building blocks, or 'qubits.'

"One major issue of scalability is that qubits are often limited in their ability to interact with one another," explains project coordinator Professor Floris Zwanenburg, full professor at the University of Twente's MESA+ Institute for Nanotechnology. "As the number of qubits increases, effective communication between them becomes more complex."

But Germanium-Silicon (GeSi) presents a viable solution to overcome these bottlenecks.

"We are combining spin qubits for computation and photonics for communication on a GeSi platform that is compatible with traditional CMOS manufacturing, which could be a total game-changer for scaling quantum computers. By combining spin qubits (electrons) with photonic communication (light), the chip bridges the gap between processing quantum information and transmitting it over long distances. This will significantly help us solve a major bottleneck in quantum scalability," Professor Zwanenburg said.

Strengthening Europe's Quantum Independence

By integrating quantum components with CMOS-compatible GeSi, ONCHIPS brings Europe's quantum ecosystem together with its established semiconductor industry.

The success of the ONCHIPS project could reduce reliance on imported advanced chips for quantum technologies and contribute to Europe's goal of technological sovereignty. The project hopes to bolster Europe's ability to produce advanced quantum chips domestically and position Europe as a pioneer in scalable quantum systems.

Set to conclude in 2026, ONCHIPS brings together a consortium of leading European organisations. The partners include Universiteit Twente in the Netherlands, which coordinates the project, along with Technische Universiteit Eindhoven (Netherlands), Technische Universität München (Germany), Centre

National de la Recherche Scientifique (CNRS) (France), Universität Konstanz (Germany), Budapesti Műszaki és Gazdaságtudományi Egyetem (Hungary), and the Dutch company Single Quantum BV.

10. Broadcom brings network encryption to ransomware fight

by Dan O'Shea
https://www.fierceelectronics.com/electronics/broadcom-takes-ransomware-fight-network-level

Broadcom has introduced new network-level encryption devices with post-quantum cryptography that eliminate the weaknesses that leave application-level encryption practices susceptible to most ransomware attacks.

The company's Emulex Secure Fibre Channel Host Bus Adapters (HBA) encrypt all data as it moves between servers and storage devices, providing network-level security rather than incorporating encryption of applications on an individual basis. Significantly, this translates to real-time detection of ransomware attacks, that application-level encryption does not provide.

Broadcom's new HBAs comply with the recent post-quantum cryptography standards from the National Institute of Standards and Technology, as well as mandates such as the US Commercial National Security Algorithm (CNSA) 2.0, the European Union's Network and Information Security (NIS) 2, Digital Operational Resilience Act (DORA), and others that have been developed to bring enterprises into the age of post-quantum encryption and zero trust security architectures.

Jeff Hoogenboom, vice president and general manager, Emulex Connectivity Division, Broadcom, told *Fierce Electronics,* "Zero trust principles, and specifically network-based encryption, are key to protecting against the collection and exfiltration of critical business data. The most sensitive business data often has value that extends well into the future. It is widely assumed that well-funded malicious actors are storing some of that data for decryption in the future, when new Gen AI or quantum methods enable that capability. Post-quantum encryption is designed to be resistant to both current and future decryption methods."

The post-quantum protections provided by the Emulex Secure Fibre Channel HBAs include silicon-root-of-trust, digital signing and key encryption, as well as in-flight encryption, Hoogenboom said.

He added that "a majority of Emulex customers will have capability of using in-flight encryption in 2025, regardless of segment. The reason is that all of the multinational server OEMs have decided to make the Emulex Secure HBA their standard offering starting with the new Intel platform launches that will happen this spring. Further, many of the storage array OEMs have decided to offer the Emulex Secure HBA starting as early as the second half of 2025."

That rollout should be welcomed by enterprises that continue to be inundated with weekly reports of new ransomware attacks capable of gouging their financial resources. Broadcom referred to a Ponemon Institute study that put the average cost of a single ransomware attack last year at about $5.37 million, and these attacks are only expected to become larger and more sophisticated with growing use of generative AI and near-future deployment of more quantum computers.

Broadcom's HBAs may offer a practical way of fighting back against this trend, as they leverage existing Fibre Channel infrastructure widely deployed in many data centers, and at less cost and complexity that application encryption, Hoogenboom said.

"From a business perspective, until today, customers have only had one option to protect their data via encryption, which is to encrypt one application at a time," he stated. "The application-based encryption approach introduces complex and costly key management, it eliminates the ability to compress and dedupe storage, and most importantly, it destroys the ability to recognize a ransomware attack in real-time. Emulex Secure HBAs encrypt all data without introducing any of these restrictions."

The company's 32G and 64G Secure HBAs are available now in one-port, two-port, and four-port configurations.

11. Useful quantum computing is inevitable—and increasingly imminent

by Peter Barrett
https://www.technologyreview.com/2025/01/27/1110540/useful-quantum-computing-is-inevitable-and-increasingly-imminent/

On January 8, Nvidia CEO Jensen Huang jolted the stock market by saying that practical quantum computing is still 15 to 30 years away, at the same time suggesting those computers will need Nvidia GPUs in order to implement the necessary error correction.

However, history shows that brilliant people are not immune to making mistakes. Huang's predictions miss the mark, both on the timeline for useful quantum computing and on the role his company's technology will play in that future.

I've been closely following developments in quantum computing as an investor, and it's clear to me that it is rapidly converging on utility. Last year, Google's Willow device demonstrated that there is a promising pathway to scaling up to bigger and bigger computers. It showed that errors can be reduced exponentially as the number of quantum bits, or qubits, increases. It also ran a benchmark test in under five minutes that would take one of today's fastest supercomputers 10 septillion years. While too small to be commercially useful with known algorithms, Willow shows that quantum supremacy (executing a task that

is effectively impossible for any classical computer to handle in a reasonable amount of time) and fault tolerance (correcting errors faster than they are made) are achievable.

For example, PsiQuantum, a startup my company is invested in, is set to break ground on two quantum computers that will enter commercial service before the end of this decade. The plan is for each one to be 10 thousand times the size of Willow, big enough to tackle important questions about materials, drugs, and the quantum aspects of nature. These computers will not use GPUs to implement error correction. Rather, they will have custom hardware, operating at speeds that would be impossible with Nvidia hardware.

At the same time, quantum algorithms are improving far faster than hardware. A recent collaboration between the pharmaceutical giant Boehringer Ingelheim and PsiQuantum demonstrated a more than 200x improvement in algorithms to simulate important drugs and materials. Phasecraft, another company we have invested in, has improved the simulation performance for a wide variety of crystal materials and has published a quantum-enhanced version of a widely used materials science algorithm that is tantalizingly close to beating all classical implementations on existing hardware.

Advances like these lead me to believe that useful quantum computing is inevitable and increasingly imminent. And that's good news, because the hope is that they will be able to perform calculations that no amount of AI or classical computation could ever achieve.

We should care about the prospect of useful quantum computers because today we don't really know how to do chemistry. We lack knowledge about the mechanisms of action for many of our most important drugs. The catalysts that drive our industries are generally poorly understood, require expensive exotic materials, or both. Despite appearances, we have significant gaps in our agency over the physical world; our achievements belie the fact that we are, in many ways, stumbling around in the dark.

Nature operates on the principles of quantum mechanics. Our classical computational methods fail to accurately capture the quantum nature of reality, even though much of our high-performance computing resources are dedicated to this pursuit. Despite all the intellectual and financial capital expended, we still don't understand why the painkiller acetaminophen works, how type-II superconductors function, or why a simple crystal of iron and nitrogen can produce a magnet with such incredible field strength. We search for compounds in Amazonian tree bark to cure cancer and other maladies, manually rummaging through a pitifully small subset of a design space encompassing 10^{60} small molecules. It's more than a little embarrassing.

We do, however, have some tools to work with. In industry, density functional theory (DFT) is the workhorse of computational chemistry and materials modeling, widely used to investigate the electronic structure of many-body systems—such as atoms, molecules, and solids. When DFT is applied to systems where electron-electron correlations are weak, it produces reasonable results. But it fails entirely on a broad class of interesting problems.

Take, for example, the buzz in the summer of 2023 around the "room-temperature superconductor" LK-99. Many accomplished chemists turned to DFT to try to characterize the material and determine whether it was, indeed, a superconductor. Results were, to put it politely, mixed—so we abandoned our best computational methods, returning to mortar and pestle to try to make some of the stuff. Sadly, although LK-99 might have many novel characteristics, a room-temperature superconductor it isn't. That's unfortunate, as such a material could revolutionize energy generation, transmission, and storage, not to mention magnetic confinement for fusion reactors, particle accelerators, and more.

AI will certainly help with our understanding of materials, but it is no panacea. New AI techniques have emerged in the last few years, with some promising results. DeepMind's Graph Networks for Materials Exploration (GNoME), for example, found 380,000 new potentially stable materials. At its core, though, GNoME depends on DFT, so its performance is only as good as DFT's ability to produce good answers.

The fundamental issue is that an AI model is only as good as the data it's trained on. Training an LLM on the entire internet corpus, for instance, can yield a model that has a reasonable grasp of most human culture and can process language effectively. But if DFT fails for any non-trivially correlated quantum systems, how useful can a DFT-derived training set really be? We could also turn to synthesis and experimentation to create training data, but the number of physical samples we can realistically produce is minuscule relative to the vast design space, leaving a great deal of potential untapped. Only once we have reliable quantum simulations to produce sufficiently accurate training data will we be able to create AI models that answer quantum questions on classical hardware.

And that means that we need quantum computers. They afford us the opportunity to shift from a world of discovery to a world of design. Today's iterative process of guessing, synthesizing, and testing materials is comically inadequate.

In a few tantalizing cases, we have stumbled on materials, like superconductors, with near-magical properties. How many more might these new tools reveal in the coming years? We will eventually have machines with millions of qubits that, when used to simulate crystalline materials, open up a vast new design space. It will be like waking up one day and finding a million new elements with fascinating properties on the periodic table.

12. Infineon and BSI Achieve Post-Quantum Cryptography Certification

by Rashmi
https://www.bisinfotech.com/infineon-and-bsi-achieve-post-quantum-cryptography-certification/

Infineon Technologies AG has achieved a milestone on the way to a quantum-resilient world in collaboration with the German Federal Office for Information Security (BSI). Infineon is the first company ever to receive the Common Criteria EAL6, an industry-leading certification level, for the implementation

of a post-quantum cryptography algorithm in a security controller. Such cryptography enhances security for eSIM, 5G SIM and smart card applications, including personal IDs, payment cards and eHealth cards, against threats resulting from highly capable quantum computers. The world's first certification is a milestone on the way to a quantum-safe future in our daily lives.

Thomas Rosteck, Division President Connected Secure Systems at Infineon, said , "There is no question that quantum computers will be a reality; Therefore, we need to push forward with theCriteria EAL 6 certification for post-quantum security is a testament to our dedication in critical infrastructure and helping maintain the security of our customers' data in a post-quantum world. This once again underpins Infineon's leadership in the security industry."

The international Common Criteria standard sets guidelines and criteria for the security of IT products and systems and is internationally recognized. By certifying Infineon's secured implementation of a PQC algorithm with Common Criteria EAL 6, the BSI underlines the importance of resistance against classic attacks, like fault attacks, as well as quantum computer attacks. The ML--KEM algorithm was implemented on a TEGRION™ security controller, Infineon's latest brand of 28 nm security controllers based on Infineon's revolutionary security architecture Integrity Guard 32. The Common Criteria scheme was developed in collaboration among various governments and is recognized by governments around the globe. The certification itself takes place through various national institutions. Infineon's TEGRION security controller has been evaluated and certified by the German BSI under the German Certification scheme.

EAL6 is a highly advanced level of assurance, indicating that the product or system has undergone a comprehensive and rigorous evaluation to confirm its security claims. The certified security controller combines high-performance processing with advanced cryptographic capabilities, providing a robust foundation for post-quantum cryptography. With this certification, Infineon is setting a new standard for the industry, paving the way for widespread adoption of post-quantum cryptography and for a safer digital future.

13. Palo Alto Networks Makes Post Quantum Cryptography API Available

by Michael Vizard
https://securityboulevard.com/2025/01/palo-alto-networks-makes-post-quantum-cryptography-api-available/

Palo Alto Networks this week released an open application programming interface (API) framework that organizations can use to more easily deploy encryption keys that are not likely to be broken by a quantum computer.

Rich Campagna, senior vice president for product management for Palo Alto Networks, said the Quantum Random Number Generator (QRNG) Open API framework also ensures there will be interoperability between the post quantum algorithms that will be used to create stronger encryption keys.

Developed in collaboration with Anametric, ID Quantique, Qrypt, Quantinuum, Quantropi and Quside, the QRNG Open API framework makes use of quantum mechanics principles to encrypt data in a way that generates truly random numbers.

Available via the Palo Alto Networks GitHub repository, the QRNG Open API is designed to be embedded into any application. Palo Alto Networks will later this year add support for it to its next-generation firewalls (NGFWs).

No one knows for certain when quantum computers will break existing encryption schemes used to encrypt data, however, it is generally expected to occur within the next five years, said Campagna.

The National Institute of Standards and Technology (NIST) has already defined a set of post-quantum cryptography (PQC) standards that the QRNG Open API framework makes easier to implement.

Replacing existing encryption frameworks can take years, so NIST is encouraging organizations to start the process now in anticipation of existing encryption schemes being eventually cracked, also known as "Q-Day."

In the meantime, it is suspected that nation-states are already harvesting encrypted data in the expectation they will be able to decrypt it one day soon, using a quantum computer. The sooner organizations replace legacy encryption schemes the less likely it will be that data they thought was secure today might one day be used to extort payments for not disclosing, or simply dumped into a repository on the Dark Web for anyone to see.

The challenge, of course, is convincing senior business and IT leaders to make available the resources required to replace existing encryption algorithms. Given all the competing priorities organizations have today, it's often difficult for cybersecurity teams to convince executives to address a threat now that might not manifest for years.

Of course, recent quantum computing advances such as the Willow project being advanced by Google suggest those advances are occurring at a faster rate, and researchers in China claim they have already used a quantum computer to break a 50 integer RSA algorithm. No longer widely used, that achievement may be a harbinger of similar research efforts to break more advanced cryptography frameworks.

Undoubtedly, havoc will ensue when Q-Day does eventually arrive. Many organizations will still be relying on legacy encryption frameworks to protect data. Hopefully, that data remains protected, rather than in a repository that cybercriminals are now gleefully using to uncover any number of secrets. After all, if it was worth encrypting in the first place, chances are that even years from now the data is going to still retain some of its value.

14. Galaxy S25 has post-quantum cryptography, other security features

by Mihai Matei
https://www.sammobile.com/news/galaxy-s25-post-quantum-cryptography-other-security-features/

Security and privacy have become greater concerns in the era of AI and interconnected device ecosystems. The new Galaxy S25 employs a wide range of security features and is Samsung's first phone series to introduce post-quantum cryptography against even the most dangerous quantum-based cyber attacks.

Thanks to the Snapdragon 8 Elite chip, the Galaxy S25 series is powerful enough to process most of its Galaxy AI features on the device without accessing or sending personal information to any servers.

Features like Now Brief rely on the Personal Data Engine to analyze data on-device and deliver personalized experiences. However, this personal data has to be stored safely on the Galaxy S25 and kept private.

For Galaxy S25 users, personalized AI data is securely locked behind Knox Vault, which now has a new future-proof security layer, i.e., post-quantum cryptography.

In essence, post-quantum cryptography, or PQC, consists of cryptographic algorithms that should be secure against cryptanalytic attacks performed by a quantum computer.

The Personal Data Engine gathers data for personalized AI experiences only from native Samsung apps and recognizes many languages and dialects, including but not limited to the following:

- Arabic, (Simplified) Chinese, Dutch, English, French, German, Hindi, Indonesian, Italian, Japanese, Korean, Polish, Portuguese, Romanian, Russian, Spanish, Swedish, Thai, Turkish, and Vietnamese.

Furthermore, the Personal Data Engine itself is customizable and only functions under the parameters set by users through the Personal Data Intelligence menu on the Galaxy S25. If this feature is turned off, all the analyzed user data is deleted instantaneously from Knox Vault.

Samsung also provides better security for Galaxy S25 users through a new Knox Matrix dashboard, additional Maximum Restriction settings, and enhanced Theft Protection.

The Galaxy S25 series is now available for pre-order, and Samsung offers different early adopter bonuses depending on the market. Hit the pre-order button below for more details.

15. UTC Doctoral Candidate Develops Self-Encrypting AI

by Chuck Wasserstrom
https://www.chattanoogan.com/2025/1/22/498183/UTC-Doctoral-Candidate-Develops.aspx

In a world where data security is an ever-growing concern, Joshua Tyler – a computational engineering doctoral candidate and electrical engineering research associate at the University of Tennessee at Chattanooga – has broken new ground.

Mr. Tyler, who is on track to receive his third UTC degree in May, has developed the world's first usable Artificial Intelligence network that can learn how to encrypt itself. This AI network, he said, can provide nearly unbreakable cryptography – significantly improving the security of communications.

Mr. Tyler and his faculty mentor, Dr. Don Reising, a Guerry and UC Foundation associate professor of electrical engineering, have uploaded a draft of their publication to arXiv—an open-access repository for scholarly papers. They have already submitted their invention disclosure to the University of Tennessee Research Foundation for a provisional patent.

Mr. Tyler's AI network, he explained, learns to encrypt data "by transforming an encryption key onto the original unencrypted data. The goal is to ensure that the encrypted message is unique to the key while the original message is still recoverable on the other end."

"This ensures that when deployed, each encryption is unique and significantly extends the network's lifespan," said Mr. Tyler, who received a bachelor's degree in electrical engineering in 2020 and a master's degree in 2022.

The research builds on a concept initially proposed by Google, known as Adversarial Neural Cryptography. While Google demonstrated the potential for AI-driven cryptography, its approach faced significant limitations—particularly in ensuring the encryption key's influence on the encrypted message and additional communication overhead.

"I copied over Google's setup and trained their network on my side," he said. "The network was encrypting the information, but we found out that there wasn't a lot of uniqueness on the encrypted side when we were switching keys, so that makes the overall life of the network shorter. You'd only get to encrypt one message per network."

Dr. Reising, who has worked with Mr. Tyler for more than six years, said he "basically challenged Josh to go and find a way to get this thing to generate a unique code or a unique encoded message."

"And that's what he did," Dr. Reising said. "He went off and worked on developing his own technique." Dr. Reising recalled a pivotal moment during the process.

"I asked him, 'What architecture are you using? Are you using CNN? Are you using an LSTM? What are you using?'

"And he's like, 'No, I'm not using any of those. I made my own.'

"I said, 'What do you mean you made your own?'

"He said, 'I made my own and it's a deep learning network.' That was crazy and it was pretty awesome."

By rethinking the structure of AI networks, Mr. Tyler developed a "novel neural network architecture" that addresses these challenges.

The result is a network that offers nearly unbreakable encryption and unparalleled adaptability in safeguarding sensitive data.

"I changed the network architecture so that the influence of the key was still maintained through the entire structure of the network," he said.

A crucial feature of Mr. Tyler's system is its rapid adaptability, which allows it to retrain itself in seconds to produce entirely new cryptographic algorithms. This new architecture ensures that each encryption remains unique, effectively overcoming the limitations of previous methods.

"Every time you retrain the network, you get a different cryptographic algorithm," Mr. Tyler said. "So then, even if you use the same key across two differently trained networks, you'll get a new encryption scheme."

"These things train really fast so that we can have a new cryptographic algorithm in about 16 seconds."

16. Accenture Invests in QuSecure to Protect Against Future Quantum Threats with Crypto Agility

by Alison Geib, Denise Berard, and Dan Spalding
https://newsroom.accenture.com/news/2025/accenture-invests-in-qusecure-to-protect-against-future-quantum-threats-with-crypto-agility

Accenture has made a strategic investment, through Accenture Ventures, in QuSecure™, a leader in post-quantum cybersecurity. Together, Accenture and QuSecure offer comprehensive post-quantum crypto agility solutions to help government agencies and private sector businesses mitigate emerging quantum risks.

Headquartered in San Mateo, Calif., QuSecure is a privately held company founded in 2019. QuSecure's QuProtect software offers an end-to-end quantum security-as-a-service architecture that combines zero-trust, next-generation quantum-resilient technology and crypto agility to protect networks, cloud systems, edge devices and satellite communications against today's cyberattacks and future quantum threats, all with minimal disruption to existing systems.

"Organizations need a reliable, quantum-resilient cybersecurity solution that not only adheres to the National Institute of Standards and Technology's (NIST) post-quantum encryption standards but that can be easily integrated across all parts of a communications network," said Tom Patterson, emerging technology security lead at Accenture. "We're investing in trusted providers like QuSecure to help our clients future-proof their global networks today to protect high-risk data faster."

Post-quantum encryption standards protect a variety of electronic information, such as private email messages and e-commerce transactions. NIST is advising computer system administrators to start transitioning to NIST's newly released standards as quickly as possible. According to the Financial Services Information Sharing and Analysis Center (FS-ISAC), the shift to crypto agility must start immediately and is a long-term strategy rather than a one-time implementation.

"In a progressively digital world, as AI and quantum threats to encryption evolve at an ever-faster pace, it is critical that we evolve from encryption management that requires several years to upgrade algorithms to orchestrated crypto agility—the ability to push a button and upgrade your entire system at once," said Rebecca Krauthamer, co-founder and CEO of QuSecure. "The ability to orchestrate cryptography at the enterprise scale—swapping out cryptographic algorithms at any endpoint, anywhere—is critical to a robust cybersecurity strategy. QuSecure and Accenture have a shared vision to provide organizations with a long-term solution to upgrade and manage their encryption standards."

In 2023, Accenture and QuSecure collaborated to establish the first successful multi-orbit data communications test secured with post-quantum cryptography (PQC), which refers to cryptographic methods that are secure against an attack by a quantum computer. This demonstrates that crypto agility, successfully rotating to a less vulnerable algorithm, is real and possible.

Recently, Banco Sabadell successfully completed a joint project with Accenture and QuSecure to explore the adoption of PQC technologies in the bank's infrastructure. This project represents a significant step toward strengthening defenses against quantum attacks with Banco Sabadell employing QuSecure's software for crypto agility to update encryption.

"Crypto agility is critical for the banking industry, allowing for the seamless integration of new cryptographic standards without the need to rebuild entire systems," said Joan Puig, Group CISO of

Banco Sabadell. "Our project, in collaboration with Accenture and QuSecure, enabled us to explore the impact of adopting post-quantum cryptography technologies on the bank's infrastructure. By embracing crypto agility and testing quantum technologies we're ensuring our preparedness for the quantum future."

To help maintain security in a post-quantum world, Accenture developed an eight-step roadmap to help clients secure their data and communications and is collaborating with companies like QuSecure. Working with other industry leaders, Accenture has designed a Quantum Security Maturity Index to give corporate boards and executives a way to measure their quantum security infrastructure against their peers and identify areas for improvement.

QuSecure will also join Accenture Ventures' Project Spotlight, an engagement and investment program focused on working with companies that create or apply disruptive enterprise technologies. Project Spotlight offers extensive access to Accenture's domain expertise and its enterprise clients, helping startups harness creativity and deliver on the promise of their technology. Additional cybersecurity, quantum security and space companies that have joined Project Spotlight include Reality Defender, Aliro Quantum and Tenchi Security.

17. ID Quantique's Clavis XG: The World's First Quantum Key Distribution (QKD) Product to Obtain National Security Certification

by IDQ

https://www.idquantique.com/clavis-xg-series-qkd-obtains-national-security-certification/?utm_term=Read%20the%20Press%20Release&utm_campaign=BREAKING%20NEWS%20-%20IDQ%27s%20QKD%20receives%20National%20Security%20Certification&utm_content=email&utm_source=Act-On+Software&utm_medium=email&cm_mmc=Act-On%20Software-_-email-_-BREAKING%20NEWS%20-%20IDQ%27s%20QKD%20receives%20National%20Security%20Certification-_-Read%20the%20Press%20Release

ID Quantique (IDQ), a global leader in Quantum-Safe solutions and Quantum Communications, today announced that its high-performance Clavis XG series has become the first product of its class globally to receive an official national security approval from South Korea's National Intelligence Service (NIS).

The QKD evaluation program of Clavis XG encompassed both the QKD system and the embedded Quantum Key Management platform (QKMS), Clarion KX. It was designed in collaboration with the Ministry of Science and ICT, and the evaluation testing and validation were performed in collaboration with the National Security Research Institute (NSR), the Korea Research Institute of Standards and Science (KRISS), the Korea Information and Communication Technology Association (TTA), and the IT Security Certification Center (ITSCC), a CC (Common Criteria) certification body responsible for national security evaluation and related regulations, as well as the management of Common Criteria Recognition Arrangement (CCRA).

This national accreditation acknowledges Clavis XG as the first quantum-safe cryptography system based on quantum-physics and BB84 QKD protocol to meet stringent national security standards, setting a new milestone in the global quantum cryptography market.

While most government organizations must follow the guidelines and policies of their respective national security authorities, NSR's multi-year security evaluation effort marks a significant milestone for the global QKD industry. IDQ will continue to support the undergoing international efforts for a standardized evaluation of quantum-physics based security solutions. Independent security accreditation programs that are designed and performed by experts in national security test labs enable a higher degree of confidence necessary for the migration to quantum-safe communication across enterprise and government sectors.

"This is a massive leap forward for QKD, a physics-based quantum cryptography technology, which has successfully evolved and matured into a telecom grade security solution. We are thrilled to be able to support the cybersecurity strategy of our customers who seek to combine QKD with Post-Quantum Cryptography to mitigate the Quantum threat. The adoption of Clavis XG and Clarion KX platform will expand rapidly in the areas requiring high-level security, such as government, financial services, energy, critical infrastructure, and healthcare verticals." — Grégoire Ribordy, CEO of ID Quantique

The QKD approval program included rigorous and comprehensive evaluation of optical and digital subsystems of Clavis XG, as well as the software stack and protocols of the embedded Quantum Key Management System, Clarion KX.

The Clavis XG Series has already proved itself in a wide range of deployments in telecommunication network infrastructures and data centers, meeting and exceeding customers' performance requirements. With a compact 19'' rackmount 1U size, it offers the most advanced footprint in the market. Importantly, our partner interoperability program ensures our customers can immediately benefit from seamless integration with the industry leading range of network encryptors, network operation management suites, and SDNs. Together with the embedded and NIST-approved QRNG as well as the Clarion KX Quantum Key Management suite, a field proven and robust platform for complex network topologies and high SLA deployments, IDQ's partners and customers can now accelerate a cost-effective migration of network infrastructure to Quantum-Safe.

18. Windows BitLocker bug leaks AES-XTS encryption

by Admin
https://www.iaesjournal.com/windows-bitlocker-bug-leaks-aes-xts-encryption/

A bug was discovered in the Windows BitLocker encryption tool identified as CVE-2025-21210. This vulnerability has exposed the BitLocker encryption system to a new random attack targeting the

AES-XTS encryption mode. In addition, this vulnerability also allows an attacker who has physical access to manipulate ciphertext blocks and cause sensitive data to be written to disk in plaintext.

A computer forensics expert, Maxim Suhanov, said in his findings that he found the bug exploits a design flaw in the way BitLocker handles crash dump settings.

By modifying a single registry key *(HKLM\System\Control100Cet001\Control\CrashControl)*, an attacker can disable the *dump.sys* crash dump filter driver.

This forces the Windows kernel to write an unencrypted hibernation file directly to disk. The file often contains sensitive data from RAM, such as passwords, encryption keys, and personal information.

Attack Phase:

1. **Determine Target Location:** The attacker must find the exact disk offset that corresponds to the registry key or data structure. This is done by monitoring ciphertext changes in some part of the encrypted disk.

2. **Scramble Ciphertext Blocks:** Once the target location is found, the attacker tampers with specific ciphertext blocks. In AES-XTS mode, it scrambles the associated plaintext block without affecting the other blocks.

This vulnerability poses a serious threat in situations where the device is physically accessible. Examples are:

- **Corporate Espionage:** Attackers could exploit this loophole on a stolen laptop protected by BitLocker with a custom TPM.

- **Data Recovery Abuse:** Devices sent for repair or recycling can be targeted if there are no adequate security measures in place.

While exploitation requires a high degree of technical expertise and physical access, the potential impact is huge due to the exposure of sensitive data stored in RAM.

Fix is available:

Microsoft has released an update for the *fvevol.sys* driver that ensures dumpfve.sys remains listed in the *DumpFilters* registry. If the driver is missing or corrupt, Windows will fail to boot to prevent unencrypted data from being written to disk.

19. SEALSQ Showcases World's First PQC-Optimized Secure Hardware at Davos 2025

by Carlos Moreira
https://www.globenewswire.com/news-release/2025/01/22/3013573/0/en/SEALSQ-Showcases-World-s-First-PQC-Optimized-Secure-Hardware-at-Davos-2025.html

SEALSQ Corp, a company specializing in Semiconductors, PKI, and Post-Quantum technology hardware and software products, today (22 Jan 2025) announced that it will showcase a live demonstration of its PQC-optimized secure hardware platform (QS7001) during the Quantum Security Roundtable at Davos 2025. This milestone demonstration solidifies SEALSQ's position as a global leader in quantum-resilient technology, aligning with the urgent need for secure solutions in the era of quantum computing.

The Quantum Security Roundtable will take place on January 22, 2025, at the Davos Congress Centre in Davos, Switzerland. Organized by Microsoft, WISeKey, and the Cybersecurity Tech Accord – an alliance of leading tech companies committed to improving cybersecurity—the event brings together industry leaders, policymakers, and innovators to discuss the future of quantum technologies and their implications for global security.

A World-First in Quantum-Resistant Secure Hardware

SEALSQ will be the first company to publicly demonstrate PQC algorithms running on secure hardware designed specifically for the quantum era. This hardware platform, optimized for quantum-resistant cryptography, represents a paradigm shift in secure microcontroller design. By efficiently authenticating, signing, and encrypting data while adhering to stringent certifications like FIPS and Common Criteria, SEALSQ's platform sets a new standard for secure transactions in the quantum age.

Key Highlights of the Demonstration:

- **Performance Benchmarking:** The demo will compare the performance of the KYBER and DILITHIUM algorithms running on SEALSQ's quantum-resistant platform with that of a powerful traditional secure microcontroller, the MS6003.

- **Energy and Time Efficiency:** The platform demonstrates superior efficiency, ensuring robust security without compromising speed or energy consumption.

- **Real-World Applications:** Designed for connected devices across AI, blockchain, and IoT ecosystems, SEALSQ's hardware is built to future-proof critical infrastructures against the looming threat of quantum attacks.

The Growing Importance of Quantum-Resistant Technology

The rapid advancement of quantum computing is revolutionizing fields like AI and blockchain, but it also exposes vulnerabilities in current cryptographic systems, including RSA algorithms that safeguard millions of daily transactions. To address this challenge, NIST has endorsed quantum-resistant algorithms like KYBER and DILITHIUM, which provide robust defenses against both quantum and traditional attacks.

In response, SEALSQ's platform combines advanced hardware engineering with state-of-the-art cryptographic algorithms to deliver secure, energy-efficient solutions for the next generation of technology.

20. Tachyum adds post-quantum algorithms to universal processor

by Nick Flaherty
https://www.eenewseurope.com/en/tachyum-adds-post-quantum-algorithms-to-universal-procesor/

European universal chip designer Tachyum has added all four post-quantum cryptography (PQC) algorithms to the software distributions for its Prodigy processor.

Adding the quantum-safe PQC algorithms, approved by the US National Institute of Standards and Technology as a global standard last August, ensures data centre deployments using the company's universal processor are quantum-resistant and future-proofed for data security.

Tachyum's software engineering team has ported and verified the four quantum-resistant asymmetric algorithms – ML-KEM, ML-DSA, SLH-DSA and Falcon. The Prodigy processor also supports the AES-256 standard, which has already been optimized. Tachyum's post-quantum cryptography (PQC) will run on all Prodigy platforms.

"Tachyum takes security very seriously – from both a hardware and software perspective – so the development of quantum computer-proof data security methods is critical to us maintaining such a commitment," said Dr. Radoslav Danilak, founder and CEO of Tachyum. "As such, we will continue to monitor future cryptography standards to ensure that Prodigy-based systems remain capable of providing the highest level of security and optimum performance for customers and partners."

- Tachyum to build 50 exaFLOP supercomputer

The Prodigy Universal Processor allows data centre servers to dynamically switch between different computational domains such as AI/ML, HPC, and cloud with a single homogeneous architecture. This eliminates the need for expensive dedicated AI hardware and can significantly increase server utilization.

Prodigy integrates 192 high-performance custom-designed 64-bit compute cores, to deliver up to 4.5x the performance of the highest-performing x86 processors for cloud workloads, up to 3x that of the highest performing GPU for HPC, and 6x for AI applications. It is currently developing the chip on a 3nm process technology.

21. Germany's Max Planck Institute director stresses quantum 'harvest now, decrypt later' threat

by Charlotte Lee
https://www.taiwannews.com.tw/news/6017895

Chelpis Quantum Corp., a Taiwanese post-quantum cryptography firm, is collaborating with Professor Peter Schwabe, Scientific Director at Germany's Max Planck Institute for Security and Privacy, to strengthen its quantum-safe solutions.

Chelpis CEO Chih Ming-yang (池明洋) aims to transform Taiwan into a cryptography hub and lead the country's migration to quantum-safe cryptography.

"Cryptography, my main focus, is where quantum computers will have the greatest impact within the field of information security," Schwabe told Taiwan News.

Though quantum technology is still in development, experts predict it will eventually solve problems far faster than today's supercomputers. Schwabe highlighted the need to prepare for quantum advancements to counter threats like "harvest now, decrypt later," where data encrypted and stored today could be vulnerable to future quantum attacks.

"It's crucial to secure information now that must remain private for decades," he said, stressing the urgency of adopting quantum-resistant cryptography. Schwabe warned that quantum computers could render many current systems insecure.

Schwabe agreed with Facebook co-founder Mark Zuckerberg and Nvidia CEO Jensen Huang (黃仁勳) that quantum computers capable of breaking current encryption are still years away, but underlined the urgency of developing and implementing post-quantum cryptography.

While acknowledging the difficulty in predicting exactly when such quantum computers will exist, Schwabe suggested a key indicator would be the first successful attack on public key cryptography, likely targeting elliptic curve cryptography, the basis of many modern systems.

Schwabe believes the development of quantum computers is inevitable due to their potential benefits in many fields, though he doubts they will become as commonplace as personal devices like desktop

computers or laptops. Instead, he envisions specialized, remotely accessed quantum workstations used for complex computations.

Post-quantum cryptography adoption

Quantum-resistant algorithms are being implemented despite quantum computers still being under development. The key agreement algorithm, Kyber (ML-KEM) is widely used, Schwabe said.

Other products using it include Apple iMessage. The reason for this implementation is to protect against a potential future scenario where an attacker records encrypted messages today and decrypts them years later using a quantum computer.

Schwabe stressed the importance of preparing for the cryptographic fallout, highlighting the "harvest now, decrypt later" threat. He also noted the lengthy process of migrating all applications to post-quantum cryptography, making early preparation crucial.

Schwabe stated that while some migrations are happening now and others will occur relatively quickly, a significant number of applications will take a very long time to transition. He suggested preparations should have begun earlier.

Schwabe considers migration to post-quantum cryptography complete when systems no longer regularly use exclusively classical cryptography.

This includes securing against "harvest now, decrypt later" attacks and potentially implementing post-quantum authentication. Major web communication platforms, such as the top 100 websites, and browsers have already begun migrating, Schwabe noted.

Focus on high-assurance cryptography

Schwabe also focuses on high-assurance cryptography, ensuring cryptographic systems are rigorously verified for security. He is currently collaborating with Chelpis on research related to "Formosa Crypto," a project involving researchers from more than 10 institutions.

The initiative aims to develop tools for high-assurance cryptography, including the Jasmin programming language and the EasyCrypt theorem prover. These tools enable formal reasoning for computer-verified cryptographic proofs.

The collaboration with Chelpis currently focuses on high-assurance FrodoKEM, a post-quantum cryptographic scheme. Schwabe said the team is building on prior work within Formosa Crypto on schemes like ML-KEM, leveraging similarities to improve and reuse existing methods.

Taiwan's role in post-quantum cryptography

Schwabe believes Taiwan is uniquely positioned to drive advancements in post-quantum cryptography. The country has already made considerable progress in designing secure cryptographic systems, implementing them in both software and hardware, and conducting formal verification.

As a global leader in semiconductor manufacturing, Taiwan also plays a critical role in developing hardware solutions for quantum-resistant cryptography. "Dedicated hardware will be crucial, especially for embedded applications that require both efficiency and security," Schwabe noted.

Schwabe also stressed the importance of defending against implementation attacks, where attackers use side-channel data such as power consumption or electromagnetic radiation to uncover secret keys. Taiwanese researchers are already addressing these vulnerabilities with hardware solutions, a field Schwabe anticipates will see significant growth in the next decade.

"With its expertise in cryptography, chip design, and formal verification, Taiwan is well-positioned to lead in securing the next generation of cryptographic systems," Schwabe concluded.

Schwabe's organization, encouraged by its work with Chelpis, is exploring a long-term collaboration with Taiwan's National Science and Technology Council to advance research and development in post-quantum cryptography.

22. PQShield announces participation in NEDO program to implement post-quantum cryptography across Japan

https://www.design-reuse.com/news/57312/pqshield-nedo-post-quantum-cryptography-japan.html

PQShield, the cybersecurity company specializing in post-quantum cryptography (PQC), has joined the Cyber Research Consortium (CRC) in Japan to participate in its program with the Japanese government's New Energy and Industrial Technology Development Organization (NEDO) to enhance Japan's defense against quantum-enabled cyber attacks. As a supporting member of the CRC, PQShield will design and deliver PQC protocols that can be implemented across Japan's technology supply chain, and contribute to the ongoing global PQC standardization process. NEDO is providing a funding grant to CRC to support this project.

The publication of NIST's finalized PQC standards in August 2024 gave businesses, governments, and institutions globally a defined route to modernizing their cryptography, safeguarding their data, and protecting themselves from future quantum attacks. In July 2024, to kick-start this process in Japan, NEDO announced that research into PQC implementation technologies would take place as part of its

"Enhancement of situational awareness and defense capabilities to counter cyber attacks", a newly-established project within Japan's K Program funded by NEDO and delivered by the CRC. The goal of this research is to achieve advanced functionality in quantum-resistant cryptography, such as ring signatures, threshold signatures, and threshold encryption. The K Program is an R&D initiative that builds on the collaboration between public and private organizations in Japan to investigate critical technologies for civil and defense purposes.

Now, PQShield – the leading PQC company which contributed directly to the development of NIST's cryptographic standards after being founded as an Oxford University spinout in 2018 – has been named a supporting member of the CRC under its NEDO grant, and will be subcontracted to deliver designs and protocols for PQC implementation technologies. PQShield's Lead Cryptography Researcher Dr Shuichi Katsumata, based in Japan, will lead the company's work under the CRC.

As part of the CRC, PQShield is being subcontracted to carry out two PQC projects for NEDO: designing PQC primitives; and, in collaboration with AIST, constructing new protocols to ensure that non-PQC protocols can be updated to align with NIST's latest standards. Both projects will contribute to the ongoing effort to coordinate robust, global standards for PQC. All results will be published in academic papers, the primitives designed by PQShield will be submitted to NIST's standardization call for multi-party threshold cryptography, and the protocols constructed with AIST will be shared with the Internet Engineering Task Force to become public RFCs.

PQShield is working directly with AIST, on the design and standardization of new PQC protocols, while further support for this project is being provided by CRC subcontractors SCU Inc., Mitsubishi Electronics, and The University of Tokyo. The full list of participants in this project is:

- FFRI Security Inc
- Preferred Networks Inc
- Fujitsu
- NTT
- Powder Keg Technologies
- Ricerca Security
- Mitsubishi Electronics
- Japan Electronics
- Hitachi
- Toppan
- PQShield
- Secafy
- SCU Inc
- Yokohama National University
- Waseda University
- Keio University
- The University of Tokyo

- AIST
- Iwasaki Gakuen

Through this collaborative project, PQShield aims to enhance the functionality and security of the technology supply chain across Japan and globally. This includes planned R&D into the difficulty of the lattice problems PQC is based in, opening up avenues to understand the fundamental security of current cryptography standards. PQShield already has a strong presence in Japan, with partners including Mirise Technologies, Sumitomo Electric and NTT Data Group Corporation – the NEDO grant supports the company's growing presence in the market and the expansion of its local team.

Dr Ali El Kaafarani, founder and CEO of PQShield, said: "Securing critical infrastructure from quantum computers requires strong collaboration between governments, universities and the private sector, and this project is an ambitious and necessary step to protect against the quantum threat. Japan is an important market for PQShield and plays a critical role in the global technology supply chain. We are pleased to be working directly with NEDO and the government of Japan to help implement PQC across the country and protect against the cyber threats of the future."

Tsutomu Matsumoto, Director of the Cyber Physical Security Research Center at AIST, said: "The implementation of post-quantum cryptography across Japan is extremely important, and updating existing protocols to support NIST's latest standards will play a significant role in this process. We're pleased to support this vital mission and look forward to collaborating with fellow CRC subcontractors, including PQShield, to design and standardize new protocols which can become public RFCs."

PQShield's project with the CRC and NEDO will run from 2024 to 2026, with the final standardization documents to be delivered in 2026.

23. CAST to Enter the Post-Quantum Cryptography Era with New KiviPQC-KEM IP Core

by Artemis Couroupaki
https://www.cast-inc.com/press-releases/cast-enter-post-quantum-cryptography-era-new-kivipqc-kem-ip-core

CAST, a leading semiconductor intellectual property (IP) core provider, is excited to announce the upcoming release of its new KiviPQC™-KEM IP core and invites early adopters to engage in product evaluations. This new IP core implements the Module-Lattice Key Encapsulation Mechanism (ML-KEM) as specified in the NIST FIPS 203 standard, and is CAST's first product leveraging the power of the NIST-standardized post-quantum cryptography (PQC) algorithms to secure future SoC designs.

Overview of the KiviPQC-KEM IP Core

Designed by cryptographic solutions expert KiviCore, the new core efficiently handles secret key generation, encapsulation, and decapsulation using any of the ML-KEM variants provisioned by the NIST standard. The core's key features are:

- **Secure-by-Design:** Operates as a self-contained engine, with minimal attack surface and optional protection against time-based side-channel attacks (SCA).
- **Configurable Performance:** The hardware accelerated operation can be tuned to meet the performance, latency, and silicon resources needs of different applications.
- **Easy-to-integrate:** Employs industry-standard AMBA® hardware interfaces and provides a comprehensive software API.

The core conforms to CAST's stringent design and verification standards, is supported by CAST's 24/7 support infrastructure with access to the core's developers, and is available with CAST's flexible licensing schemes. It thus delivers PQC cryptography with CAST's promise for a Better IP Experience.

Potential applications of the KiviPQC-KEM IP core include data communication connections with the MACSec and CANSec cores also offered by CAST, as well as IPSec, Transport Layer Security (TLS), and many other protocols.

Ready for Early Adopters

"We have managed to implement the secure key management functions needed for the post-quantum computing era in a high-quality IP core with a focus on resource efficiency, simplicity, and seamless integration," said Frank Deicke, KiviCore co-founder. "One of the earliest – and we believe the most reliable yet flexible – such IP cores available, this first in our KiviPQC series will dramatically simplify cryptographic system development in many fields."

The KiviPQC-KEM IP is expected to meet product-level verification and quality assurance goals and be ready for customer release within the first quarter of 2025. Meanwhile, early adopters are invited to contact CAST (info@cast-inc.com) to evaluate the KiviPQC-KEM core using a readily available FPGA-based reference design.

24. 2025: The year to become Quantum-Ready

by Mitra Azizirad
https://azure.microsoft.com/en-us/blog/quantum/2025/01/14/2025-the-year-to-become-quantum-ready/

We find ourselves in an exciting and pivotal time. We are at the advent of the reliable quantum computing era. This past November, Microsoft successfully created and entangled 24 logical qubits in collaboration with Atom Computing. As our industry looks toward the next 12 months, the pace of quantum research and development is only going to accelerate, making this a critical and catalyzing time for business leaders to act. We're seeing a growing need for business leaders to have the information and tools to understand better the depth of these amazing technical breakthroughs and the business applications and value they open up. In a business decision-maker study, 12% said their organizations were prepared to assess quantum opportunities. Clearly, there is an urgent need for leaders to get more information and better understand how technical advancements in quantum will enable real-world impact.

Leaders in global companies, investment funds, and governments across the world are making multi-billion-dollar investments in quantum computing. Those organizations that are in the throes of planning a comprehensive quantum-ready strategy are creating durable, competitive differentiation for their organizations and positioning themselves to harness the full power of quantum as it scales. Clearly, without strategic readiness, it's a challenging proposition for leaders to assess the risks and returns, or to design effective and responsible quantum strategies that are necessary to create a full-on quantum roadmap for their organization.

This is why at Microsoft we are excited to announce our new Quantum Ready program, designed to address these exact challenges by providing business leaders with the insights and tools needed to:

1. Build practical, high-impact hybrid applications.
2. Invest in strategic skilling and access to reliable quantum computers for experimentation.
3. Embrace quantum safety and focus on cryptographic agility.
4. Prepare for scale such that your investments are future-proofed.

Becoming quantum-ready is both a business and a global imperative. In fact, the United Nations announced 2025 as the International Year of Quantum Science and Technology (IYQ), reflecting the transformative impact quantum mechanics has had in the past century, and setting the stage for the next wave of quantum innovation. As part of this global initiative, Microsoft will be a leading partner with the IYQ, along with the American Physical Society (APS), to celebrate 100 years of quantum innovation. We are so excited to partner with APS and other leading institutions to support the IYQ as it engages with communities from across the world to scale awareness of how quantum science and applications will transform industries.

Hybrid applications: Business value and security for today and tomorrow

Given the rapid pace of innovation, it's critical that organizations start exploring, identifying, and building an application roadmap that sets them up for success in a quantum future. Doing so will clarify where and when quantum will provide tangible business value and guide both how and to what degree you should invest to become quantum-ready today.

Through our Quantum Ready program, leaders will have an opportunity to engage with Microsoft in one-on-one workshops and industry-specific forums to accelerate their strategic readiness and identify high-value use cases. We hope to bring learnings that result from these industry-specific forums to the broader ecosystem to provide practical insights in the form of custom industry outlook reports to help guide your organization's leadership and company strategy.

Additionally, business leaders need to start preparing for a quantum-safe future; not because there is an immediate threat but because a transition to emerging cryptographic standards will take time. Security is a top priority at Microsoft—this is why we established the Microsoft Quantum Safe Program to enable security alignment from both business and technical perspectives.

Cultivating a quantum-ready culture: Skilling and vision for the hybrid era

Cultivating a culture of innovation begins with robust workforce skilling and training, empowering teams with the knowledge and mindset to embrace quantum-enabled possibilities. Putting this mindset into practice requires providing access to a unified hybrid platform integrating resilient quantum computing, classical supercomputing, and AI. Especially when 76% of leaders indicate that a quantum skills crisis is causing a deceleration in innovation, the organizations that can harness the power of these complementary technologies—and who understand their use is not a matter of *either or*, but *when* and *how*—are in a distinct position to stay ahead.

Our Quantum Ready program will offer different skilling and training opportunities to help prepare business and government leaders with resources, frameworks, and tools they need to:

- Understand why quantum technology is positioned to help revolutionize your business operations, talent strategies, and infrastructure.
- Gain an early-mover competitive edge by creating a quantum strategy that aligns the technology's potential with your specific business and innovation goals.
- Explore deep insight and guidance into the impact quantum computing will make in your industry and what it means for your organization.

Acting for success: Preparation for scale with the right partner

So, where and how should organizations start? Navigating the many skilling, strategy, and culture considerations is not easy, and it requires the right partners: those with experience putting state-of-the-art hybrid tools into practice with real-world, impactful applications; those who carefully consider the risks quantum pose and are working to mitigate them with leading security solutions and commitments to safe use; and finally, those with an open ecosystem approach to future-proof your investments.

From envisioning new use cases and identifying co-innovation opportunities to receiving first access to visionary industry insights, outlook reports, skilling, workshops, and other exciting new programs to come, sign up here to join Microsoft's Quantum Ready program. We look forward to connecting with you soon!

25. GlobalSign Announces Strategic Reseller Partnership to Accelerate Customer Post-Quantum Cryptography Solutions

by Amy Krigman
https://www.businesswire.com/news/home/20250114285452/en/GlobalSign-Announces-Strategic-Reseller-Partnership-to-Accelerate-Customer-Post-Quantum-Cryptography-Solutions

GMO GlobalSign, Inc. a global Certificate Authority (CA) and leading provider of identity security, digital signing and IoT solutions, today announced a new strategic partnership with Value Added Reseller Quantum PKI (formerly Acmetek). The collaboration calls for Quantum PKI to resell all GlobalSign products and services to companies in the United States. In addition, with this new relationship, Quantum PKI will provide current and future GlobalSign customers in the U.S. with an opportunity to explore and plan the various pathways to Post-Quantum Cryptography (PQC) solutions.

GlobalSign is renowned for its expertise in Public Key Infrastructure (PKI) products and solutions that span more than two decades. Its digital certificates, digital signatures, IoT identity certificates and Secure/Multipurpose internet Mail Extensions (S/MIME) certificates are utilized by thousands of companies worldwide.

Quantum PKI has a track record of success, in providing trusted PKI solutions from the top PKI brands and Certificate Lifecycle Management (CLM) solutions, specializing in simplifying the complexities of managing digital certificates. With the company's new focus on PQC, Quantum PKI will play a key role in assisting GlobalSign customers as they begin planning their journeys from traditional PKI toward PQC certificates.

"We are very pleased to partner with a PKI industry leader such as GlobalSign. Our relationship is being cemented at a significant time where our organization is expanding its reach to post quantum computing solutions. Given that GlobalSign is a recognized leader for PKI and leader in trusted identities, we feel strongly they are an important partner for us to mutually build new opportunities in this emerging Post-Quantum Computing market," said Kevin Naidoo, Founder and Lead Engineer, Quantum PKI.

The partnership underscores GlobalSign's commitment to delivering top-tier PKI solutions and supporting businesses in their digital transformation journeys. By combining GlobalSign's cutting-edge technology with Quantum PKI's extensive market reach, this collaboration promises to set new standards in the PKI industry.

"GlobalSign is very pleased to partner with a value added reseller like Quantum PKI that shares our vision of advancing security for businesses. Their range of traditional PKI solutions such for digital certificates, digital signatures, email security and IoT & connected devices align well with our offerings," said Frank Romito, Director, North American Service Provider Sales, GMO GlobalSign, Inc. "With their newest focus on PQC, the collaboration between our two organizations will allow us to accelerate the delivery of these solutions and provide even more companies with the tools they need to manage their digital identities effectively. They are the perfect company to partner with as we all look towards the future of our industry."

26. NSA and Others Publish Guidance for Secure OT Product Selection

by NSA Media Relations
https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4027075/nsa-and-others-publish-guidance-for-secure-ot-product-selection/

HThe National Security Agency (NSA) joins the Cybersecurity and Infrastructure Security Agency (CISA) and other organizations to publish guidance helping operational technology (OT) owners and operators integrate security when selecting OT products.

The joint Cybersecurity Information Sheet (CSI), "Secure by Demand: Priority Considerations for Operational Technology Owners and Operators in the Selection of Digital Products," highlights key security elements to consider when purchasing industrial automation and control systems and other OT products, as well as specific questions to ask manufacturers. Many OT products are not designed or developed securely, and they commonly have weaknesses that make them a target for cyber threat actors, including the following: weak authentication, shared software vulnerabilities, limited logging, default settings, default credentials, and default protocols.

"The guidance not only helps owners and operators of critical systems secure their OT procurement lifecycles, it also sends a message to manufacturers to establish a more resilient and flexible cybersecurity foundation in their products," said Dave Luber, NSA's Cybersecurity Director.

The CSI urges OT owners and operators to select products with the following key security elements:

- configuration management,
- logging in the baseline product,
- open standards, ownership,
- protection of data,
- secure by default,
- secure communications,
- secure controls,

- strong authentication,
- threat modeling,
- vulnerability handling, and
- upgrade tooling.

The other agencies co-sealing the CSI are the Federal Bureau of Investigation (FBI), the U.S. Department of Energy, the U.S. Environmental Protection Agency (EPA), the U.S. Transportation Security Administration, the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), Canadian Centre for Cyber Security (CCCS), European Commission, Germany's Federal Office for Information Security (BSI), Netherland's National Cyber Security Centre (NCSC-NL), New Zealand's National Cyber Security Centre (NCSC-NZ), and the United Kingdom's National Cyber Security Centre (NCSC-UK).

27. HancomWITH secures first domestic quantum-resistant cryptography verification

by Lee Kyung-tak
https://biz.chosun.com/en/en-it/2025/01/13/I7U5XTARABDORJ555TGIN62CAE/

HancomWITH announced on the 13th January that its subsidiary, SoftForum's "IQNUS Crypto v1.0" cryptographic module has passed the National Intelligence Service's cryptographic module verification (KCMVP). This cryptographic module is the first unverified cryptographic module in South Korea to include algorithms selected as post-quantum cryptography standards by the National Institute of Standards and Technology (NIST), and through this verification, it has proven its technology and stability.

Post-quantum cryptography is gaining attention as a technology that can proactively respond to the threat that quantum computers pose to current cryptographic systems. This is particularly highlighted by Google's recent announcement regarding its 105-qubit quantum computer chip "Willow," which solved a problem that would take existing supercomputers 10 septillion (10 to the power of 24) years in just 5 minutes. As the arrival of the quantum computing era accelerates, the importance of post-quantum cryptography is becoming even more pronounced.

The government has established a "Post-Quantum Cryptography Master Plan" to transition the current cryptographic system to post-quantum cryptography by 2035, aiming to complete the development and standardization of Korean-style post-quantum cryptography (KpqC) by 2029. In this context, HancomWITH is strengthening cooperation with its subsidiary SoftForum and expanding its projects applying post-quantum cryptography technology, focusing on key industrial sectors such as finance, healthcare, and defense.

HancomWITH has already introduced the communication segment cryptographic solution "Hancom xConnect v4.0" and structured/unstructured data security solution "Hancom xDB v5.0," applying post-quantum cryptography technology across various sectors such as public services, finance, and

insurance. In the future, they plan to introduce post-quantum cryptography into private certification and simple certification solutions to enter the authentication security market.

Song Sang-yeop, CEO of HancomWITH, noted, "I hope that through our subsidiary's cryptographic modules, we can securely protect critical information from future security threats in various areas that require high security, such as national and public institutions, financial sectors, and corporations."

28. Expert Bruce Schneier Says Regulation not AI Is key for Cybersecurity

by Marie-Astrid Langer
https://www.nzz.ch/english/expert-bruce-schneier-says-regulation-not-ai-is-key-for-cybersecurity-ld.1865226

Cybersecurity is facing a tough challenge. Hospitals, schools and companies are constantly falling victim to ransomware attacks. Criminals are draining life savings from unsuspecting citizens through «pig-butchering» attacks. Even American government systems do not seem immune to hackers – Chinese attackers recently penetrated the largest telecommunications networks in the U.S. and tapped into Donald Trump's phone lines.

The future doesn't seem very promising either: Some experts warn that the quantum computers currently under development could crack the encryption safeguarding today's computer systems.

But is computer security really that bad? Few people can answer the question better than Bruce Schneier. The 61-year-old American is regarded as the elder statesman of the cybersecurity industry. As a cryptologist, he has developed important encryption methods himself. Today, he teaches at Harvard University and sits on the board of the civil rights organization Electronic Frontier Foundation.

Whether lecturing at Harvard or attending specialist conferences, Schneier is instantly recognizable: A ponytail, full gray beard and newsboy cap are his trademarks. His approach to answering questions is just as distinctive – concise, direct and provocative.

The monthly newsletter of his blog «Schneier on Security» is read by 250,000 recipients. In his latest book «A Hacker's Mind,» Schneier explains how all areas of society can be cracked with a hacking mentality.

Mr. Schneier, some experts are of the opinion that computer security will soon deteriorate massively when quantum computers arrive and it will be possible to crack any existing encryption. As a cryptologist, how concerned are you about this risk?

Not really very much, for a whole bunch of reasons: One is we don't know how soon this is going to happen, if ever. Quantum computers currently don't exist, and no one knows when – or even if – we'll be able to build one. They seem to always remain «10 years in the future» which means no one has any idea.

And two, the math is well ahead of the physics here. We are creating post-quantum encryption algorithms faster than the quantum people are breaking non-quantum-resistant algorithms. So I think we're fine.

So the current cybersecurity systems won't need any adjustments?

The federal agency in charge, NIST, has a whole set of post-quantum algorithms that they have already released and are continuing to release. So that's good. The people who are panicking are people who don't understand cryptography. A common misperception is that crypto is going to break everything. It's not true. The real importance is crypto agility: It's not enough to implement a single standard; it's vital that our systems be able to easily swap in new algorithms when required. In the face of all that uncertainty, agility is the only way to maintain security.

But progress is certainly being made in the development of quantum computers. Google has just broken the barrier to fault-tolerant quantum computers.

Breakthroughs in error correction is where we need the work, so good for Google for recently reporting breakthroughs in that field. We'll see how much of a leap forward that will be. In the short term, cryptographers are putting considerable effort into designing and analyzing quantum-resistant algorithms, and those are likely to remain secure for decades.

Generative AI is not a dream of the future, but already a reality. What are the most important changes that AI brings to cybersecurity?

If you go to industry conferences, every company has an AI strategy. Most of it is marketing bullshit, but some of it is real. Now we're starting to see AI embedded in things like spam detection, vulnerability scanning and source code analysis. We see more machine learning techniques. They're not revolutions, but they're definitely evolutions.

I've seen AI pen testing technologies. [Pen testing, or penetration testing simulates attacks on computer systems.] So far, they are mediocre like all AI technology, but they're going to get a lot better. I expect this to permeate every aspect of cybersecurity.

Does generative AI benefit the attackers more than the defenders?

In the long term, we have no idea. In the near term, my guess is that AI techniques benefit the defender more. You are already being attacked at computer speeds, so the fact that the defender can do that too now is a big deal. There are a bunch of tools trying to speed up the defense – like intrusion detection systems [that monitor a network for malicious activity or policy violations] for vulnerability scanning. Lots

of companies are working on creating AI cybersecurity products. They are not very good just yet, but they will get a lot better.

But there is little sign of an improved defense today. Ransomware attacks and sophisticated scams are the epidemics of the internet age. Why are cybercriminals so successful?

You are right, it's really, really bad. Some of it is cryptocurrency. The cybercrime industry would not exist without Bitcoin. But scams like «pig butchering» come down to bank regulation. Why aren't the banks liable for this? If they were, they'd fix it. A lot of it is due to the professionalization of the criminal industry. There are some really impressive cybercrime gangs that have become something like global brands. So some of it is getting after them and law enforcement arresting them. But it's really hard because of the geopolitics. Now Russia is going to let them live on their soil.

Let's talk about state-sponsored hacking. Chinese hackers recently penetrated the telecommunications systems in the U.S. Is the U.S. government doing too little to protect its systems?

Of course we are doing too little. But doing a lot is expensive and hard to do. It tells you either we are not the best in the world or being the best is not enough. We're in a world where attack is easier than defense. Defense is hard and expensive and pisses off corporations. I'm not surprised, also not by the extent of [the attacks]. It's a matter of trade-offs of costs and benefits.

Is this an example of how private companies should have used more technology to better protect themselves?

The [cybersecurity] industry is doing great stuff, but it's not the industry, it's the economics of using it. I mean, I go to [trade fairs that are] full of really fantastic products and services – that nobody buys. Companies are more willing to take the chance of an intrusion than to spend the money.

Why is that?

We could blame capitalism. Companies get their quarterly stock price by saving money, not by being secure. And it's probably the lack of regulation that gets companies taking their chances rather than being secure. You don't get rewarded for security, you get rewarded for saving money. It really is the system in which this is all embedded.

In your view, should there be higher fines if companies are unable to keep hackers out of their networks?

It'd be nice. Or maybe we can jail people. You know, the financial penalty is the cost of doing business. In jail, executives suddenly notice. But this is a problem way bigger than cybersecurity. I would like to see incentives change – either liabilities or regulation or something. It would be nice [to make companies] responsible, because right now they're externalities.

These are actually really big problems because, yes, you're right. The Chinese got into the telecom networks. But tell me how the telephone network is going to suffer because of that. Show me where this matters to my stock price or my profit line.

Probably nowhere, you're right. But the Americans, for their part, are masters at monitoring other nations. Do you believe that the surveillance internet makes the world fundamentally safer or less safe?

Much less safe. It would be better if we could actually secure the internet rather than use it for surveillance. This is an actual real problem. It's sheer conceit: The U.S. thinks we're doing all this spying and we don't want to not spy. So we're going to make sure everybody can spy. It is a stupid thing to do. A world where nobody spies is better than a world where everybody spies.

As a cybersecurity expert, what is your advice on how everyone can improve their own internet security?

Some very general, basic advice is: Update your software, keep good backups and have a good bullshit detector – that is, a healthy dose of skepticism. That already covers a lot of ground.

29.Sopra Steria x Thales: Post Quantum Cryptography for Banks

by Marine Lecomte
https://www.soprasteria.be/newsroom/blog/details/sopra-steria-x-thales-post-quantum-cryptography-for-banks

We recently published an article describing the need to upgrade existing cryptography systems with so-called Post-Quantum algorithms, which will be able to resist the potentially huge computation power of quantum computers.

In this article, we would like to focus on the practical solutions which could be offered to the banks in this regard. To this end, we are interviewing Benoît Jouffrey from Thales Digital Identity & Security (DIS), a leading global provider of cybersecurity solutions.

Benoît Jouffrey, would you please tell us about Thales DIS and your role there?

As Chief Technology Officer of Thales Digital Identity & Security, one of my duties is to identify the main technology trends that will impact our customers over the next few years, and start defining the answers we should bring them in order to build, as per the Thales motto, a future we can all trust. One of these trends is Post-Quantum Cryptography (PQC).

In our last article, we described the Q-day risk, ie. a doomsday due to quantum computers breaking all existing cryptography algorithms. At what horizon do you see this coming and what are the actual risks for the banking sector?

There is a diversity of opinions between computer scientists regarding the date at which a first version of a commercial Quantum Computer would be available to "break" the classical cryptosystems. Some experts believe this would be possible within the next 10 years while others are generally targeting 2035 – 2040. The reality is that nobody knows, and at the same time nobody wants to take the risk. The reasoning is the following: we have the vaccine, why not use it?

Regarding the banking sector, one of its peculiarities is that migration times can be long compared to other industries, meaning this threat has to be anticipated now. Three types of major risks need to be taken into account:

- Disclosure of banks' sensitive information with long-term secrecy requirements .
- Loss of integrity of large amount payment orders between banks, that could be undetected if the cryptographic keys used to protect these payment orders are revealed.
- Impersonation of bank customers who are identified using classical electronic signatures, generating fraud and loss of reputation.

We understand that the US has setup a timeline to migrate to post-quantum cryptography, especially through the NIST standards. What is the situation on the market? How have the US banks started preparing?

Indeed in the USA, the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA) and the National Institute of Standards Technology (NIST), have urged organizations to start preparing for the implementation of post-quantum cryptography by doing the following:

- Establish a Quantum-Readiness Roadmap
- Engage with technology vendors to discuss post-quantum roadmaps.
- Conduct an inventory to identify and understand cryptographic systems and assets.
- Create migration plans that prioritize the most sensitive and critical assets.

As a result, the US has decided that its federal public service shall migrate first, although no obligation has been set. The estimated cost of the migration of the prioritized information systems until 2035 shall be more than $7 billion

As of now, no migration schedules have been set neither for the US Administration nor the Financial Sector. NIST takes 2035 as a reference date at which the Quantum Threat will likely become a reality, which can therefore be a reasonable target date for the US Financial Industry to migrate. .

Even though there is limited public visibility regarding the overall positioning of US banks towards the Quantum Threat, we note that Pioneer Quantum US Banks include JP Morgan, Citigroup, Wells Fargo and HSBC according to the American Banker.

And they overall have been considering two different kinds of approaches against the Quantum Risks:

- Direct use of Quantum Technologies to mitigate the Quantum Threat, for instance through Quantum Key Distribution, which requires a dedicated infrastructure.
- Migration to Post-Quantum Cryptography

The first option has been tested by several of those US Pioneers. But I believe that the second option will be privileged, in particular thanks to the availability of the first NIST Post-Quantum Cryptography Standards (FIPS 203,204 and 205) which were released in August 2024.

We should note than on top of preventing "Quantum risks", a Bank having a "Quantum advantage" would get a major competitive breakthrough. As a result, some US Banks have announced funding of different promising Hi-Tech Companies working in the field of Quantum Computers.

In Europe also, the ENISA has started sharing convictions, as well as some local authorities (ANSSI in France is one of them). However, the timeline does not seem to be as precise as in the US. How do you foresee the situation evolving there? Are banks starting to move forward with some initiatives?

We believe that at European Level, the migration to Post-Quantum systems will be ultimately mandated by law and monitored by the Financial Authorities and ENISA. Via a common agreement and possibly after consulting with the Banking industry, they will set migration deadlines.

European Banks such as Credit Agricole and BNP Paribas in France, UK Banks such as Barclays, HSBC and Netherland's ING have already evaluated Quantum Risks and sometimes funded Quantum Start-Ups and/or directly experiencing Quantum Technology.

The first phase of a migration program to PQC is to get a complete understanding of the existing crypto systems. What are the challenges related to this? What is Thales DIS offering in this space ?

Banks must consider their IT systems and Customer Data (Storage, In Transit) for their Post-Quantum migration. Indeed, it's unlikely they are cryptographically protected with an adequate level of robustness. Therefore, for Banks the most urgent task is to create the inventory of these critical data and review their cryptographic protection, against a double criterion: adverse consequences in case they're disclosed, and/or if their integrity is broken. Once the inventory is done, they must focus on the evaluation of the investments required for the PQ migration, establishing a priority for migration depending on the criticality and/or vulnerability of the IT system identified as hosting data at risk.

Thales DIS has comprehensive experience in delivering products and solutions for a safe migration of the Security Controls protecting sensitive IT systems. More importantly, Thales DIS is either having ready-to-use or prototypes of Post-Quantum components for Payment Systems, both at the front-end level (PQ cards and Secure Elements) and for back-end systems (OTA and Cloud-based servers, HSMs, Key Management Servers…).

The second phase is to experiment with concrete algorithms, especially through hybridization. Could you define this concept better and help us understand why it is the right step towards full PQC?

Hybridization consists in the implementation of a cryptographic mechanism which is the combination of a Post-Quantum asymmetric algorithm (e.g., ML-DSA recently standardized by NIST) with a classical asymmetric algorithm (e.g., RSA).

French ANSSI, alongside German BSI, insist that hybridization is needed when a post-quantum algorithm is implemented, at least until 2030 according to its position paper on Post-Quantum Cryptography. The reason is that post-quantum algorithms have not been sufficiently tested yet. As a result, the addition of a classical and robust cryptographic mechanism adds to the security of a " stand-alone " post-quantum implementation.

Another phase is to upgrade towards a new crypto-agile infrastructure. What is this new concept of crypto agility? Why is this necessary? What is Thales DIS offering in this space?

Crypto-agility is a device/system functionality that enables to update the device/system for the execution of stronger cryptographic mechanisms, with no need to replace the system physical components and thus ensuring business continuity. In this respect, we note that the new EU regulation Cyber-Resilience Act (CRA) requires that personal computing devices support patching functionalities.

For instance, a crypto-agile payment card using a classical asymmetric algorithm, such as RSA for card authentication purposes, will be able to switch and execute the same card authentication using ML-DSA (another protocol). Thales DIS will be offering crypto-agile payment cards when established certification processes will be available

How do you see the market evolve in the next 12 – 24 months?

We believe that the recent publication by NIST of the first set of Post-Quantum Crypto-algorithms is going to boost the interest of Banks for prototyping devices supporting crypto-agile and /or hybrid post-quantum cryptography. It sets the basis for more stable standards and a solid base. Migration is still going to take time but the incentive is real and the interest around those topics is going to keep rising. We are just at the beginning of this major transformation.

30. Chinese Scientists Describe the 105 Qubit Zuchongzhi 3.0, a Competitor to Google's Willow

by GQI
https://quantumcomputingreport.com/chinese-scientists-describe-the-105-qubit-zuchongzhi-3-0-a-competitor-to-googles-willow/

In a recent paper posted on arXiv, Chinese scientists have described their latest superconducting quantum processor named Zuchongzhi 3.0, a successor to the earlier Zuchongzhi 2. The device appears to be quite similar to Google's Willow chip and has the same amount of 105 qubits. However, Willow appears to have a slight edge in a few key qubit quality metrics as summarized in the table below. (Additional qubit quality information is available for GQI clients on the GQI portal.)

	Ave. Connectivity	Ave. T_1	Ave. T_{2CPMG}	Ave. 1Q Fidelity	Ave. 2Q Fidelity	Ave. Readout Fidelity	Ave. 1Q Gate Delay	Ave. 2Q Gate Delay
Willow	3.47	98 µsec	89 µsec	99.965 %	99.86%	99.33%	25 nsec.	42 nsec.
Zuchzongzhi 3.0	3.47	72 µsec	58 µsec	99.90%	99.62%	99.18%	28 nsec.	45 nsec.

The Chinese team also published results of a Random Circuit Sampling (RCS) experiment where they used 83-qubits with 32-cycles on Zuchongzhi 3.0 to process one million samples in just a few hundred seconds. The same circuit would take 6.4×10^9 years to complete on the classical Frontier supercomputer. For comparison, Google reported that they had performed a larger RCS experiment on Willow that completed in under five minutes and would require the largest current day classical supercomputer 10^{25} years to finish.

31. Encryption backdoor debate 'done and dusted,' former White House tech advisor says

by Jessica Lyons
https://www.theregister.com/2025/01/04/encryption_backdoor_debate/

In the wake of the Salt Typhoon attacks, which lawmakers and privacy advocates alike have called the worst telecoms security breach in America's history, US government agencies have reversed course on encryption.

After decades of advocating against using this type of secure messaging, "encryption is your friend," Jeff Greene, CISA's executive assistant director for cybersecurity, told journalists last month at a press briefing with a senior FBI official, who also advised us to use "responsibly managed encryption" for phone calls and text messages.

In December, CISA published formal guidance on how to keep Chinese government spies off mobile devices, and "strongly urged" politicians and senior government officials – these are "highly targeted" individuals that are "likely to possess information of interest to these threat actors" – to ditch regular phone calls and messaging apps and instead use only end-to-end encrypted communications.

It's a major about-face from the feds, which have historically demanded law enforcement needs a backdoor to access people's communications – but only for crime-fighting and terrorism-preventing purposes.

"We know that bad guys can walk through the same doors that are supposedly built for the good guys," Virtru CEO and co-founder John Ackerly told *The Register*. "It's one thing to tap hardline wires or voice communication. It's yet another to open up the spigot to all digital communication."

This, of course, is exactly what the Communications Assistance for Law Enforcement Act – better known as CALEA – did 30 years ago. The 1994 law required telecom providers to design their systems to comply with wiretapping requests from law enforcement. In 2006, the FCC expanded this backdoor mandate to cover broadband internet companies.

CALEA also required telcos to lock down their own networks to prevent foreign spies from intercepting Americans' communications. But the FCC never really enforced this piece of the legislation.

And earlier this year Beijing's cyberspies recorded "very senior" US political figures' calls as part of the Salt Typhoon espionage campaign. This breach, which one senior US senator called the "worst telecom hack in our nation's history – by far," has renewed calls to reform CALEA and remove these government-ordered backdoors that can be found and abused by others.

"The debate over end-to-end-encryption is done and dusted," Ackerly said. "It's over substantively, and as a country, we should be embracing encryption without backdoors."

Before Ackerly and his brother Will - who previously worked for the US National Security Agency - co-founded their data encryption startup, John Ackerly worked in the George W Bush White House as a tech advisor and played a role in developing the data privacy language in the 2000 Republican Party's platform, which called for encryption without backdoors into networks.

He was also in the West Wing when September 11 happened, and the terrorist events quickly quashed any pro-encryption messaging from the government.

Ackerly said he heard about the Salt Typhoon hacks almost 10 years to the week that he was in New York talking to the press about the 2014 Sony Pictures breach.

"So it was: Here we go again," he said. "But then it became super clear that this is orders of magnitude more devastating than any single hack to a particular company."

Burrowing this deep into America's telecommunications systems essentially gave Salt Typhoon attackers access to "every company across the country and every American," Ackerly added. "This is the worst breach in our nation's history. So that was my second reaction. And then the third reaction was: okay, maybe people will wake up."

The public and lawmakers should wake up to the need for E2EE, he said, adding that Congress should step in with a legislative fix. "Batten down the hatches, the way Ron Wyden is proposing with security requirements for the telecom companies that have been asleep at the wheel," Ackerly said.

He's referring to the US senator from Oregon's proposed legislation that would require American network operators to implement cybersecurity standards and ensure their systems are not susceptible to hacks by nation-state attackers.

Wyden, in announcing the Secure American Communications Act, blasted the FCC's "failure" to implement security standards already required by CALEA.

"What we have to fight against is complacency and bad policy," Ackerly said. "That's why CALEA needs to be reformed. Keep a Klieg light on this until there's a better answer than just: The Chinese are still there, I don't know what to do. It's just too late, forget it."

32. Quantum Cybersecurity in 2025: Post-Quantum Cryptography Drives Awareness

by Berenice Baker
https://www.iotworldtoday.com/quantum/quantum-cybersecurity-in-2025-post-quantum-cryptography-drives-awareness

Quantum computing is set to enter a new era of capability in 2025, but that means it poses a growing risk to current encryption protocols necessitating the adoption of post-quantum cryptography (PQC).

However, quantum technology can also offer improved security through advancements in quantum networking, quantum key distribution (QKD) and quantum random number generation (QRNG).

Enter Quantum has collected cybersecurity predictions from quantum computing providers and adopters, looking into how they expect the industry to change in the new year, what technologies are set to emerge and how businesses can adapt to meet the changing landscape.

Here are some of the major trends anticipated for 2025, including the migration to PQC, QKD, QRNG and the need for crypto-agility.

Quantinuum head of cybersecurity Duncan Jones

"There are still significant hurdles before we reach the day when quantum computers are able to break classical encryption. According to the majority of scientists and academics, we are still about five to 10 years away from such an event. Gartner's latest prediction is that advances in quantum computing will make most conventional asymmetric cryptography unsafe to use far sooner, by 2029.

While there is no set formula for assessing the risk and timing of the quantum threat, organizations can rely on progress in the following three areas as indicators: hardware progression, error correction and algorithm development. For instance, Quantinuum accelerated its roadmap for fully fault-tolerant quantum computing to 2030.

Given where we stand today, the need to complete migration to PQC to effectively protect sensitive data needs to be prioritized, as technological developments could necessitate such quantum secure solutions sooner than 2035.

In 2024, there was a groundswell of reports detailing concern over the potential impacts of a post-quantum cyberattack on U.S. financial systems. One focused on the Federal Reserve and its Fedwire network that facilitates bank-to-bank transactions. The report by the Hudson Institute suggested that a hack executed by a powerful quantum computer in the future on macroeconomic financial institutions could render an indirect GDP loss between $2 trillion and $3.3 trillion. Another Hudson Institute report estimated that the overall cost of a major hack and devaluation of Bitcoin alone would equal $3 trillion in direct and indirect losses.

The quantum industry will likely see continued incremental advances in 2025, including hardware improvements in error correction and qubit scaling, expanded practical adoption of quantum key distribution and quantum random number generation (QRNG). There will also be ongoing research into quantum algorithms to break cryptography, though claims of dramatic breakthroughs should be treated with appropriate skepticism.

Organizations implementing quantum-safe strategies today should focus on PQC migration while ensuring their cryptographic foundations are as strong as possible through the use of QRNG. This approach provides immediate security benefits while preparing for future quantum-safe technologies."

Florian Neukart, chief product officer, Terra Quantum

"The increasing urgency to address cybersecurity challenges will drive the adoption of quantum-safe cryptographic solutions like QKD and post-quantum algorithms in 2025. Advancements in quantum networking, particularly quantum key distribution for securing critical infrastructure, will also accelerate.

At Terra Quantum we are scaling our cryptography solutions, leveraging our leadership in QKD and post-quantum cryptography to secure next-gen communications.

The increasing urgency to address cybersecurity challenges will drive the adoption of quantum-safe cryptographic solutions like QKD and post-quantum algorithms and is one of the factors that will drive industry growth in the coming year."

Michele Mosca, founder, EvolutionQ

"Organizations will rapidly adopt post-quantum cryptography, balancing security needs with compliance challenges.

The cybersecurity landscape is shifting dramatically, with enterprises recognizing the critical need to transition to quantum-resistant encryption. This migration represents a proactive approach to mitigating potential quantum computing threats, though implementing these solutions will require careful strategic planning.

Emerging threats drive demand for cryptographic diversity and agile defense strategies. Recent research, particularly from Chinese cybersecurity experts, underscores the complexity of modern cyber threats. Organizations must develop multi-layered, adaptable cryptographic approaches that can quickly respond to evolving technological risks.

Quantum threats will become a top agenda item for enterprise boards, with cryptographic resilience as a key business requirement. Chief information security officers (CISOs) are facing unprecedented pressure to demonstrate quantum readiness. As cloud and SaaS dependencies grow, understanding and mitigating quantum risks has become a critical leadership responsibility.

Nation-state cyberattacks and global instability will drive demand for stronger cryptographic systems and region-specific standards. Increasing geopolitical tensions are directly influencing cybersecurity strategies. Nations are developing region-specific cryptographic standards, recognizing that technological sovereignty is now as crucial as traditional defensive measures."

Ben Packman, chief security officer, PQShield

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

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

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

Todd Moore, vice president, of data security products, Thales

"Earlier this year, NIST released its first sets of post-quantum encryption algorithms. Before these standards were released, many enterprises needed help grasping the need for PQC. NIST's standards have brought urgency to address the impact of quantum advancements and the need to address these threats.

Even though the TLS and SSH protocols have been updated to meet NIST's new standards, NIST is already working on its next set of algorithms, meaning that the algorithms implemented today will be different by the time the threat of quantum computing arrives. This points to the importance of crypto agility in adapting to these evolving security recommendations.

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

33. Quantum Computing 2025 – Is it Turning the Corner?

by John Russell
https://www.hpcwire.com/2025/01/01/quantum-computing-2025-is-it-turning-the-corner/

It's time to stop doubting quantum information technology.

Are we there yet? No. Not by a long shot. But the progress on a number of key challenges, the sheer number of organizations fighting to succeed (and make a buck), the no-turning-back public investment, and nasty international rivalry are all good guarantors.

It feels like quantum computing is turning an important corner, maybe not the corner leading to the home stretch, but likely the corner beyond the turning back point. We now have quantum computers able to perform tasks beyond the reach of classical systems. Google's latest break-through benchmark demonstrated that. These aren't error corrected machines yet, but progress in error correction is one of 2024's highlights.

Quantum pioneer John Preskill recently suggested we change our mindset and language and stop talking about NISQ (noisy intermediate scale quantum) versus FASQ (fault-tolerant application scale quantum) systems and start talking about Mega/Gigaquop (million/billion quantum operations) systems – basically systems able to do some levels of productive "work."

That feels right. We're rapidly developing the features (hardware and software) that will make Mega/Gigaquop possible. We're entering the next phase of quantum computing development. Not the end game but a significant change, let's call it the middle game, where winning hardware and software strategies will emerge and lesser ones will fade.

This year, HPCwire published roughly 90 feature articles on quantum computing writ large. Last year we published roughly 80. What just a few years ago was a small fraction of HPCwire's coverage has grown steadily. Today, AI, traditional HPC, and quantum makeup the bulk of our coverage.

But back to quantum computing – it's happening, and maybe sooner than many expect. Here are six key trends and nine notables worth watching in 2025.

Let's get started.

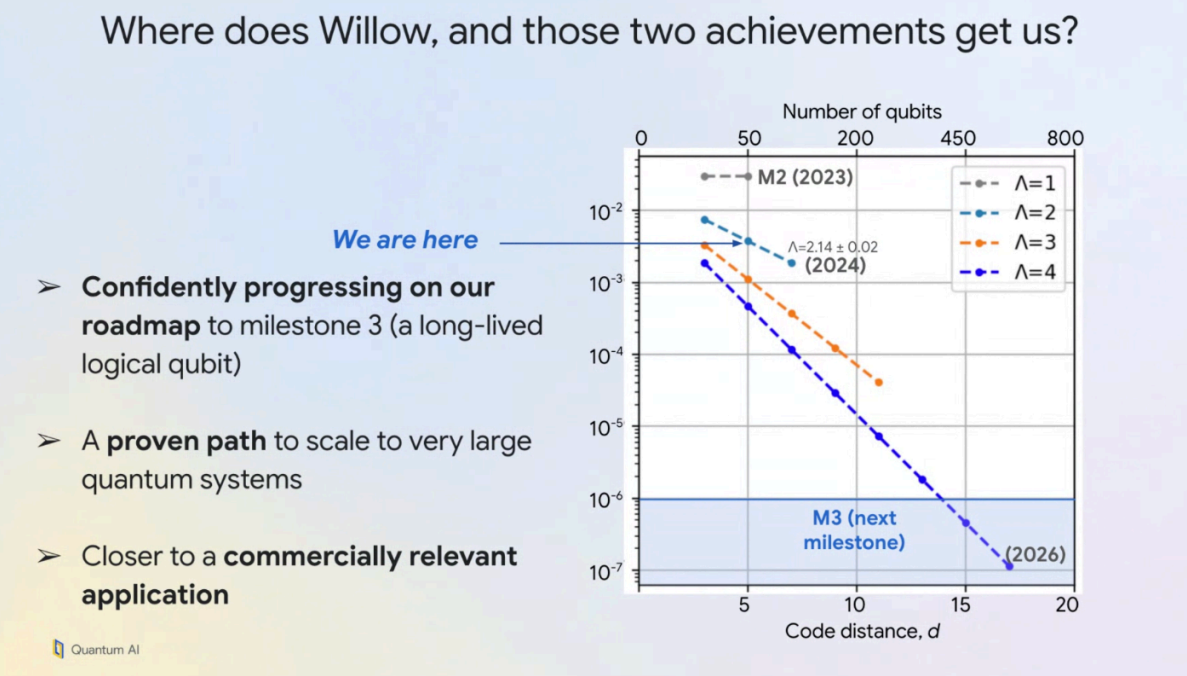
1. Great Strides in Error Correction

Last year, led by Google's breaking of the QEC Threshold on Google's new chip (Willow), there was an impressive wave of quantum error correction advances. More efficient surface codes. Improved alternate approaches (Cat Qubits). Impressive collaborations such as Microsoft and Quantinuuum's development of qubit virtualization technique using quantum and classical resources.

Physics World, the membership magazine of the Institute of Physics (U.K.), one of the largest physical societies in the world, selected Quantum Error Correction as its breakthrough of the year with two groups sharing the honor: 1) Google for Willow and breaking the QEC Threshold barrier and 2) MIT, Harvard, and QuEra for work demonstrating quantum error correction on an atomic processor with 48 logical qubits.

Physics World wrote, "Errors caused by interactions with the environment – noise – are the Achilles heel of every quantum computer, and correcting them has been called a "defining challenge" for the technology. These two teams, working with very different quantum systems, took significant steps towards overcoming this challenge. In doing so, they made it far more likely that quantum computers will become practical problem-solving machines, not just noisy, intermediate-scale tools for scientific research."

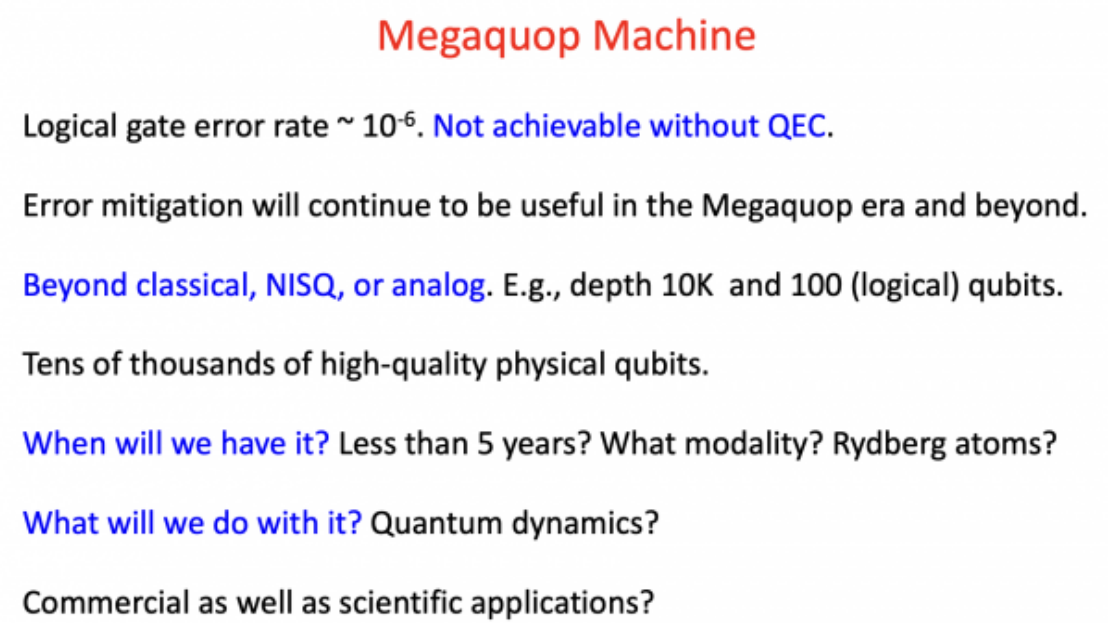
It seems every possible QEC avenue is being explored with progress on many fronts. (Google slide is below)



Not only is attention being paid to QEC structures but it's also being focused on QEC decoder capabilities. Error decoding is done by co-located classical systems. Google's error decoder (classical) takes about 63 microseconds to perform and another ten second to be transmitted by ethernet*. "Not bad," said John Preskill, recently, but it will need to improve as the code grows in size.

"Riverlane and Rigetti have demonstrated in small experiments that the decoding latency can be reduced by running the decoding algorithm on FPGAs rather than CPUs, and by integrating the decoder into the control stack to reduce communication time. Adopting such methods may become increasingly important as we scale further," said Preskill. "Google DeepMind has shown that a decoder trained by reinforcement learning can achieve a lower logical error rate than a decoder constructed by humans, but it's unclear whether that will work at scale because the cost of training rises steeply with code distance. Also, the Harvard / QuEra team has emphasized that performing correlated decoding across multiple code blocks can reduce the depth of fault-tolerant constructions, but this also increases the complexity of decoding, raising concern about whether such a scheme will be scalable."

The industry goal, or thereabouts, is to create a physical million-qubit system with on the order of 100 reliable qubits able to run circuit depths of 10,000. While most observers think it will still be a decade to get there, some (me) think the time-line may shrink. There are just so many people working on the problem, producing results, and building on each other's work.



2. The Rise of Regional Hot Spots

Call it Silicon Valley-itis (SVI). At least a dozen (or more) cities and municipalities around the world are scrambling to become hotspots for quantum development and commerce. The memory of Silicon Valley's ride to riches while driving the electronics revolution has folks salivating.

Think that's an exaggeration? Here are just a few of the regional efforts in the U.S.: Illinois (Chicago Quantum Exchange), Colorado (Elevate Quantum), Tennessee (Chattanooga Quantum Collaborative), Maryland (The Quantum Stater), Connecticut (QuantumCT), Massachusetts (Quantum Complex). No doubt there are more. Many are being designated TechHubs as part of the U.S. Commerce program.

It's a similar story in Europe. In Germany, there's a well-established effort called the Munich Quantum Valley that can rival pretty much any other regional effort. Just last month Hamburg jumped into the fray with a new consortium touting the Hamburg Full Stack Initiative. SVI efforts are springing up around the globe. There are, of course, many national efforts around the world.

They all see riches and influence flowing from the expected quantum technology revolution. They are crafting a mix of tax breaks, land-use provisions, government funding, academic center affiliations, and government lab associations as enticements. Close collaboration with industry is generally a de rigueur element.

Aspirations are sky high as shown here by the U.S.-based Elevate Quantum effort:

- **Elevate Quantum (a multi-western state effort – Colorado, New Mexico, and Wyoming)** says it will deliver 15,000 jobs, $2 billion in funding for startups, and $150 million in revenue by 2030. Its website says: "The consortium of 120 organizations works to ensure that the region remains the global epicenter for Quantum by helping turn cutting-edge research into world-changing companies, facilitating a vibrant startup and scale-up ecosystem and building a diverse and inclusive workforce."

- **Elevate Quantum's stated mission is simple:** "Secure the Mountain West's position as the global epicenter for QIT development and enhance U.S. economic and national security."

Currently, the Chicago Quantum Exchange/Illinois effort and the Munich Quantum Valley efforts seem the most advanced and are tackling the widest scope of quantum activities.

Illinois is building Illinois Quantum and Microelectronics Park (IQMP), a multibillion-dollar quantum campus on Chicago's southeast side. It will include the multimillion-dollar Illinois-DARPA Quantum Proving Ground and be anchored by PsiQuantum. Last month IBM announced plans to establish a National Quantum Algorithm Center at IQMP and locate one of its Quantum Systems Two there. The Chicago Quantum Exchange, which has been around since 2017, boasts core members such as the University of Chicago, Fermi National Laboratories, and Argonne National Lab.

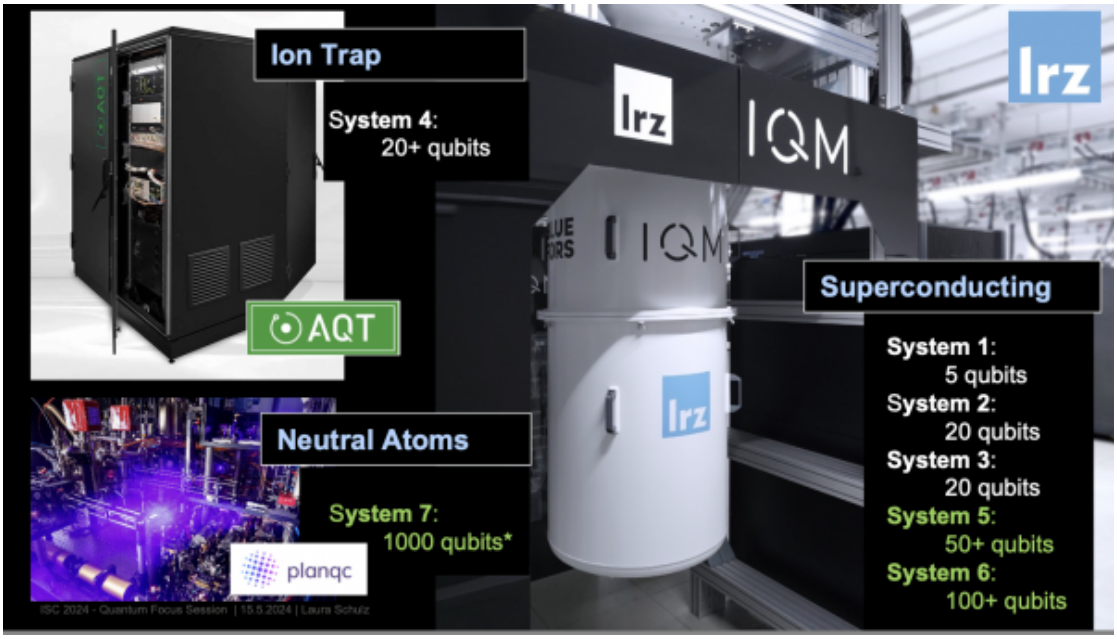
In Germany, the Munich Quantum Valley effort is also steamrolling along. At SC24, at a roundtable on integrating quantum computing with HPC, Laura Shultz, head of quantum at LRZ, a core Munich Quantum Valley noted:

> *"We currently have four quantum systems that are installed in our facility, three superconducting and one ion trap. Our mission is not only to install these systems, to make them available for the users, but we're also focused on making sure that multi modality type quantum systems can be integrated into the HPC workflow and operational system. We've been working on this now for about three years. This includes bringing up the systems, integrating them into the facility, and then also making sure that they are connected with an open source hybrid software stack that we call*

the [Munich quantum software stack.](#) So we've been working on this for a couple of years now, and envision for hybrid HPC use cases what we call tight integration.

"So we want to not just have systems, HPC systems, quantum systems, working separately over different different networks, different spaces, which is absolutely fine, we think, for some applications, but we want to really focus on very tightly-integrated, which means that we have it on the same network. We have it co-located on prem, we have these together, so that we're really able to to reduce down the latency, maximize the communication and the computation between the two, and really treat these as accelerators to the overall HPC framework."

That's impressive work.



How serious these regional efforts are isn't always easy to tell, but many are moving quickly to establish strong footholds. It's too early to pick winners and it will be interesting to see how/if these efforts payoff. No one wants to be left behind.

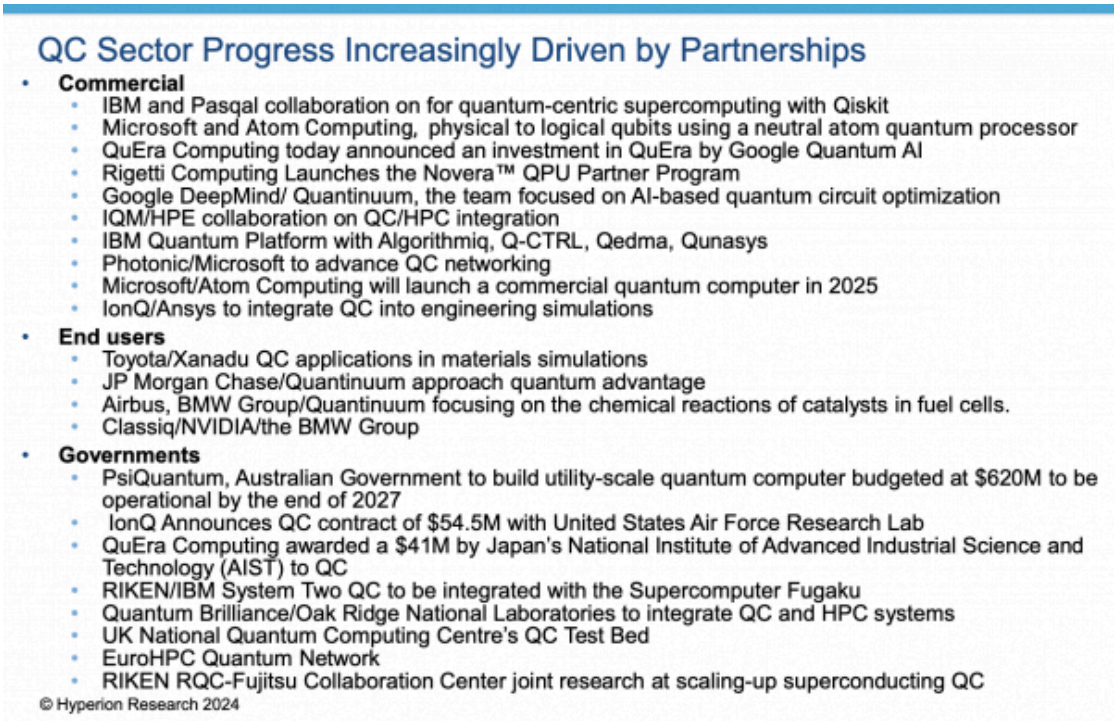
Interestingly, the ongoing AI boom, which hangs over all-things-technology these days, hasn't seemed to slow the quantum technology land rush though it may have slowed funding. Also interesting some states with plentiful quantum companies – California comes to mind – don't seem to have a single concentrated effort.

3. The Soaring Value of Collaboration

The go-it-alone crowd in quantum computing is shrinking. To be fair, it's always been a small community with lots of conversations and paper-sharing/reading within it. That said, the number and depth of

collaborations is mushrooming, many around common concerns such as error correction, but really these partnerships now encompass virtually every phase QC develop and commercialization.

Take a look at Bob Sorensen's terrific slide below. It's from his talk at Q2B last month. Yes, it's a test for the eye, but it captures the range of partnerships and collaborations in quantum science today. As he would no doubt agree, it's incomplete as many more collaborations exist, but its value as an exemplar is significant.



Sorensen, chief quantum watcher for Hyperion Research, says, "The rapid increase in QC partnerships at every level is a clear indicator that the sector has entered the next critical stage of evolution. Just as Boeing doesn't make jet engines, Goodyear doesn't build cars, and McDonalds doesn't raise cattle, smart QC vendors will increasingly seek to hone their specific value-added capabilities while partnering within a maturing ecosystem to ultimately provide a better total solution to end users."

While many companies still profess the full-stack-company mantra, the practical truth is even they are engaging in meaningful collaborations. It turns out, there's really no other way.

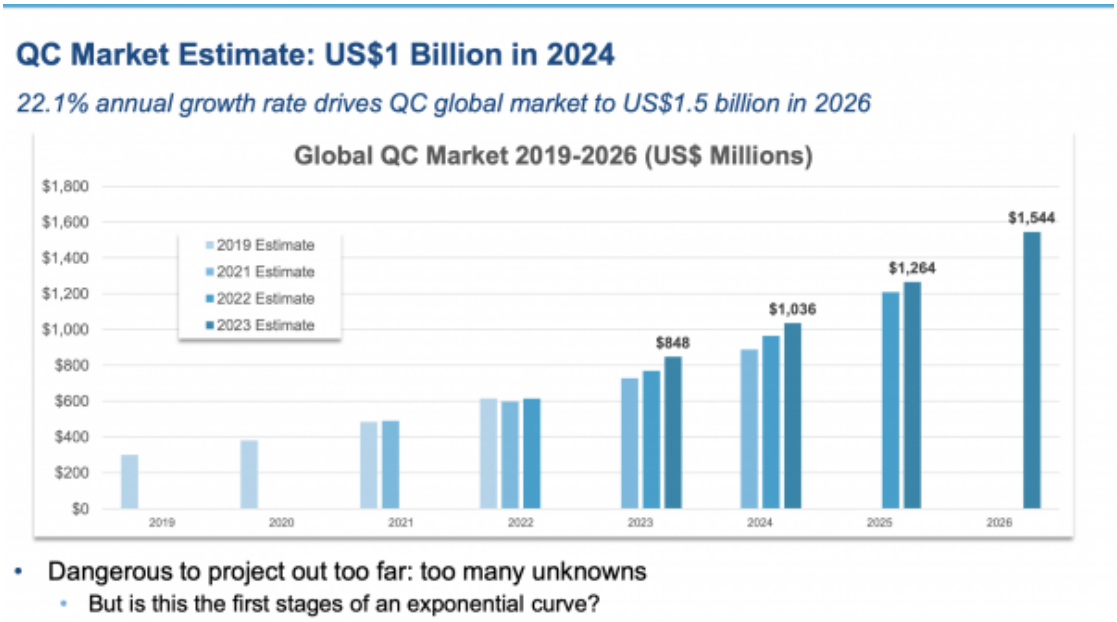
4. Stock Market Swings, 2 Casualties, but Signs of Hope

Despite the growing optimism, quantum computing remains a risky endeavor.

Zapata Computing, which started in 2017 as a pure-play QC software company, pivoted to an AI emphasis, and went public through a SPAC with Andretti Acquisition Corp, then ceased operations in

October. The Harvard spinout's fate is a cautionary tale about uncertainties in weak user demands. Norwegian company Nordic Quantum Computing also shut down. Alibaba and Baidu dumped their quantum business in 2023. Clearly 'user-based' revenue is scarce.

The worldwide market (aside from funding rounds and government contracts which amount to the same thing) is still small; it will finish this year at around $1 billion headed to about $1.544 billion in 2026, according to Hyperion Research. That's a nice roughly 22% annual growth but still not a big market. Yet.



D-Wave likes to point out it is open for business and has customers. And indeed, it is open for business and has product offerings and has a few customers with applications being used in production. No small achievement and real congratulations are due. But we'll need to see more active customers – let's say 10-to-a-dozen – with applications being used in production and corresponding growth in revenue before calling an active market happening.

There are signs the financial markets may be starting to think that time isn't so far off.
D-Wave and Rigetti Computing are among the few pure-play quantum computing to go public and both were punished early and faced delisting more than once. As of this writing they are surging. Another early player IonQ has fared well for some time. Whether the current surge is a sign of confidence or momentary blips is up for debate.

Rumors of planned IPOs have swirled around other early quantum pioneers – Quantinuum, for example. In Quantinuum's instance, going public would provide an exit for Honeywell from which Quantinuum was spun out. There's been speculation that Honeywell is investigating disaggregating itself into several pieces.

5. NQIA 2.0 – What's in The Reauthorization Act (MAYBE)

It's starting to look like the National Quantum Initiative Act of 2018 may actually get reauthorized. In December a formal bill was submitted to the Senate that authorizes $2.7 billion over five years. The original Act set in motion the U.S. national quantum effort; it established, among other things, the five National Quantum Information Science research centers and also direct NIST to help establish the Quantum Economic Development Consortium (QED-Q).

The latest bill's sponsors – Sen. Maria Cantwell (D-Wash.), Chair of the Senate Committee on Commerce, Science and Transportation, Sen. Todd Young (R-Ind.), member of the Committee, Sen. Dick Durbin (D-Ill.) and Sen. Steve Daines (R-Mont.) – say the reauthorization will shift focus from basic science to fostering commercial development.

Here are a few bullets from the bill:

- Establishes up to three new NIST quantum centers to advance research in quantum sensing, measurement and engineering.
- Creates five new NSF Multidisciplinary Centers for Quantum Research and Education, a quantum workforce coordination hub and quantum testbeds at the NSF's Technology, Innovations, and Partnerships Directorate.
- Authorizes NASA quantum R&D activities, including quantum satellite communications and quantum sensing research initiatives.
- Creates prize challenges to accelerate the development of quantum applications and algorithms through public-private collaboration.
- Requires the White House Office of Science and Technology Policy (OSTP) to develop an international quantum cooperation strategy to coordinate R&D activities with allies of the United States.

Industry is throwing its weight behind the bill as noted in these two statements in support:

"QED-C wholeheartedly supports the bipartisan NQI Reauthorization Act being introduced in the Senate by the Committee on Commerce, Science and Transportation. The Act will ensure US leadership by supporting a broad portfolio of basic research, promoting engagement with industry and international partners, and building a quantum-ready workforce," said Celia Merzbacher, Executive Director of the Quantum Economic Development Consortium.

"IonQ applauds Senator Maria Cantwell in her efforts to reauthorize the National Quantum Initiative Act (NQI). The NQI is instrumental in driving the U.S. national quantum strategy and demonstrates how policy can support technology leadership. Now is the time for the U.S. government to employ quantum computing and networking technologies to help address many of society's complex challenges in areas such as security, finance, manufacturing and life sciences. We encourage a swift passage of this necessary legislation," said Peter Chapman, President and CEO of IonQ.

Things seemed gloomier about NQIA's prospects last year (See HPCwire coverage). This year the mood is upbeat. (BTW – As required by law the NQI supplement to the U.S. budget was released in December which pertains to the existing program.)

6. NIST Pushes Post Quantum Security Adoption

No one believes quantum computers able to decrypt current (RSA-dominated) encryption methods are going to fire up soon. But they are coming. In August, NIST issued its first formal standards for Post Quantum Cryptography standards. Already there's a steady stream of new tools moving to market. NIST doesn't expect the transition to be fast and has issued guidance (Transition to Post-Quantum Cryptography Standard). Eventually all government agencies and most contractors will be required to meet the new standards.

As noted in the report, "National Security Memorandum 10 (NSM-10) establishes the year 2035 as the primary target for completing the migration to PQC across Federal systems [NSM10]: "Any digital system that uses existing public standards for public-key cryptography, or that is planning to transition to such cryptography, could be vulnerable to an attack by a Cryptographically Relevant Quantum Computer (CRQC). To mitigate this risk, the United States must prioritize the timely and equitable transition of cryptographic systems to quantum-resistant cryptography, with the goal of mitigating as much of the quantum risk as is feasible by 2035."

The report goes into considerable detail. Here are two sample tables.

Table 1: Post-Quantum Security Categories

Security Category	Attack Type	Example
1	Key search on a block cipher with a 128-bit key	AES-128
2	Collision search on a 256-bit hash function	SHA-256
3	Key search on a block cipher with a 192-bit key	AES-192
4	Collision search on a 384-bit hash function	SHA3-384
5	Key search on a block cipher with a 256-bit key	AES-256

Table 2: Quantum-vulnerable digital signature algorithms

Digital Signature Algorithm Family	Parameters	Transition
ECDSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
EdDSA [FIPS186]	≥ 128 bits of security strength	***Disallowed*** after 2035
RSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035

Making the transition to PQC is expected to be difficult and costly. Dustin Moody, a NIST PQC leader and one of the authors of the draft transition document told HPCwire back in June, "Very often, you're going to need to use sophisticated tools that are being developed to assist with that. Also talk to your vendors, your CIOs, your CEOs to make sure they're aware and that they're planning for budgets to do this. Just because a quantum computer [able to decrypt] isn't going to be built for, who knows, maybe 15 years, they may think I can just put this off, but understanding that threat is coming sooner than you realize is important."

34. Company Claims Quantum Algorithm Implements FULL Adder Operations On Quantum Gate Computers

by Matt Swayne
https://thequantuminsider.com/2025/01/01/company-claims-quantum-algorithm-implements-full-adder-operations-on-quantum-gate-computers/

MicroAlgo Inc. has announced the development of a quantum algorithm it claims significantly enhances the efficiency and accuracy of quantum computing operations. According to a company press release, this advance focuses on implementing a FULL adder operation – an essential arithmetic unit – using CPU registers in quantum gate computers.

The company says this achievement could open new pathways for the design and practical application of quantum gate computing systems. However, it's important to point out that the company did not cite supporting research papers or third-party validations in the announcement.

QUANTUM GATES SIMULATE FULL ADDER OPERATIONS

Quantum gate computers operate by applying quantum gates to qubits, which are the basic units of quantum information. Unlike classical bits that represent data as either "0" or "1," qubits can exist in a superposition of probabilistic states, theoretically enabling quantum systems to process specific tasks more efficiently than classical computers. According to the press release, MicroAlgo's innovation leverages quantum gates and the properties of qubits, including superposition and entanglement, to simulate and perform FULL adder operations.

The FULL adder, a basic building block in classical digital circuits, is relatively straightforward to implement in classical computing systems. Its adaptation to quantum computing, however, is more complex due to the unique behaviors of qubits. MicroAlgo claims its implementation enhances computation speed and accuracy, benefiting applications such as large-scale data processing, cryptography, and optimization problems.

TECHNICAL DETAILS BASED ON THE BERNSTEIN-VAZIRANI ALGORITHM

MicroAlgo's approach reportedly builds on the Bernstein-Vazirani algorithm, a well-known method in quantum computing. The algorithm determines a hidden bit string using a single quantum query, contrasting with multiple queries required in classical computing. The company says it adapted this algorithm to demonstrate a quantum register – a temporary storage system – capable of efficiently handling qubits.

In classical computing, registers are used to temporarily store and process data. MicroAlgo claims its quantum registers expand on this functionality by relying on the quantum properties of superposition and entanglement. The company states this enables higher parallelism and computational efficiency in addition operations. It further claims that the design offers practical access to quantum registers, a critical step for integrating quantum computers into real-world applications.

NO INDEPENDENT VALIDATION PROVIDED

While the press release outlines the purported benefits of the technology, it does not provide supporting documentation, such as peer-reviewed publications or independent expert evaluations. Claims about the potential performance advantages of MicroAlgo's quantum algorithm remain unverified.

The absence of such validation is important because independent verification is a standard practice in the quantum computing industry to substantiate claims of significant advances. Without this, the implications of the claimed development it is difficult to fully assess the claims.

POTENTIAL APPLICATIONS AND CHALLENGES

In the release, MicroAlgo highlights several areas where its quantum algorithm could have applications. The company reports that its technology may improve computational efficiency in fields like cryptography, optimization and large-scale data processing. It also suggests that the design could inspire new strategies for integrating classical computing concepts, such as FULL adders and registers, into quantum computing architectures.

However, the system would likely face significant challenges before it realizes the practical benefits of quantum computing. As noted in the press release, issues such as qubit stability, error rates and the complexities of managing quantum entanglement and superposition are persistent barriers to broader adoption. The development of more robust quantum algorithms is another critical area requiring attention.

35. Top 5 Companies Leading the Race of Quantum Computing Revolution

by Kumar Priyadarshi
https://techovedas.com/top-5-companies-leading-the-race-of-quantum-computing-revolution/

Introduction

Quantum computing is no longer a futuristic concept – it's a rapidly advancing technology poised to transform industries and redefine computational limits. Harnessing the principles of quantum mechanics, quantum computers can solve problems that classical computers would take centuries to process. As this field matures, tech giants and innovative startups are racing to lead the quantum revolution. Here's a closer look at quantum computing, the challenges it faces, and the companies spearheading its progress.

Understanding Quantum Computing

Quantum computing relies on quantum mechanics, a branch of physics that governs particles at the atomic and subatomic levels. Unlike classical computers that use binary bits (0 or 1), quantum computers operate with qubits.

These qubits can exist in multiple states simultaneously, thanks to quantum phenomena like superposition and entanglement.

This capability allows quantum computers to perform parallel computations, enabling them to tackle complex problems far faster than their classical counterparts.

Five Key Points About Quantum Computing

1. **Unprecedented Speed:** Quantum computers solve complex problems faster than classical systems.

2. **Revolutionary Applications:** They offer breakthroughs in cryptography, drug discovery, and logistics optimization.

3. **Challenges Persist:** Building stable, scalable quantum systems remains difficult.

4. **Industry Race:** Major tech companies and startups are driving advancements.

5. **Complementary Technology:** Quantum computers will enhance, not replace, classical systems.

The Challenges of Building Quantum Computers

Creating a functional quantum computer is an engineering marvel that faces numerous challenges:

- **Stability:** Qubits are extremely sensitive to noise and environmental factors. Maintaining their coherence for computations is crucial.
- **Error Rates:** Quantum error correction is essential to ensure reliable outputs, given the susceptibility of qubits to errors.
- **Scalability:** Developing quantum systems with thousands or millions of qubits is a significant hurdle.
- **Material Innovation:** Advanced materials and architectures are required to support qubit functionality.

Despite these obstacles, companies are investing heavily in research and development to overcome them.

The Evolution of Quantum Computing

The concept of quantum computing dates back to 1982 when physicist Richard Feynman proposed machines capable of simulating quantum systems.

Classical computers struggle to model quantum mechanics due to the exponential complexity of quantum phenomena. Feynman's vision inspired decades of research, leading to today's experimental quantum systems.

Industry Leaders Driving Quantum Advancements

The race to quantum supremacy has attracted tech giants and startups alike. Here are some of the key players making strides:

1. IBM

IBM has been at the forefront of quantum computing innovation. Its **Condor processor**, featuring 1,121 qubits, is among the most advanced in the industry. The company aims to build a 100,000-qubit system by 2033. IBM's modular **Quantum System Two** is another milestone, designed for scalable quantum computing solutions.

2. Google Quantum AI

Google achieved a major breakthrough with its **Sycamore processor**, which demonstrated quantum supremacy by solving a problem that classical computers could not. The company is now focusing on developing quantum machine learning algorithms and aims to construct a million-qubit quantum computer.

3. Intel

Intel applies its semiconductor expertise to quantum computing. Its **Tunnel Falls chip**, featuring 12 qubits, is a step toward scalable quantum systems.

Intel's focus on silicon-based spin qubits highlights its commitment to building stable and efficient quantum processors.

4. Microsoft Azure Quantum

Microsoft provides a full-stack quantum platform through **Azure Quantum**, combining hardware and tools like the Q# programming language. This ecosystem supports developers in experimenting with quantum applications.

5. Amazon Web Services (AWS)

AWS's **Braket platform** offers access to quantum hardware and hybrid quantum-classical systems. Its partnerships with various quantum hardware providers ensure versatility for researchers and developers.

Emerging Startups in Quantum Computing

While tech giants dominate the headlines, several startups are making significant contributions:

- **Quantinuum:** A merger of Honeywell Quantum Solutions and Cambridge Quantum, this company develops hardware-agnostic quantum software, including the **TKET programming toolkit**.
- **Rigetti Computing:** Known for its superconducting qubits, Rigetti focuses on integrating quantum systems with classical infrastructure for machine learning and chemistry applications.
- **IonQ:** Specializing in trapped-ion technology, IonQ's systems offer long coherence times and precision, ideal for quantum chemistry and financial modeling.
- **Xanadu:** This Canadian startup leverages photonic quantum computing, using light-based qubits to address temperature and scalability challenges.
- **D-Wave Systems:** A pioneer in quantum annealing, D-Wave focuses on solving optimization problems and has collaborated with organizations like Google and NASA.

Quantum Computing Applications

Quantum computers have the potential to revolutionize various fields:

Cryptography: Quantum systems can break traditional encryption methods, driving the need for quantum-safe cryptographic protocols.
Drug Discovery: Quantum simulations can model molecular interactions, accelerating pharmaceutical innovation.
Climate Modeling: Complex climate systems can be better understood through quantum computations.
Logistics Optimization: Quantum algorithms can optimize supply chains and transportation networks.
Artificial Intelligence: Quantum computing enhances machine learning by solving high-dimensional optimization problems.

The Road Ahead

Quantum computing remains in its early stages, with practical, large-scale systems still years away. However, the progress made by companies like IBM, Google, and Intel signals a promising future. The focus now is on improving stability, scalability, and error correction to make quantum systems commercially viable.

As quantum computing evolves, it will complement classical systems, handling specialized tasks requiring extraordinary computational power. The potential for breakthroughs in science, technology, and industry is immense.

Conclusion

The quantum computing race is heating up, with leading tech companies and startups pushing the boundaries of what's possible. From tackling complex scientific problems to transforming companies,

quantum computing holds the promise of a new era in technology. As investments pour in and innovations continue, the future of quantum computing looks brighter than ever.